MME Administration Guide, StarOS Release 21.1

First Published: 2017-01-26

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

About this Guide

This preface describes the *MME Administration Guide*, how it is organized and its document conventions.

Mobility Management Entity (MME) is a StarOS application that runs on Cisco® ASR 5x00 and virtualized platforms.

About this Guide

This preface describes the *MME Administration Guide*, how it is organized and its document conventions.

Mobility Management Entity (MME) is a StarOS application that runs on Cisco® ASR 5x00 and virtualized platforms.

Conventions Used

The following tables describe the conventions used throughout this documentation.

Notice Type	Description
Information Note	Provides information about important features or instructions.
Caution	Alerts you of potential damage to a program, device, or system.
Warning	Alerts you of potential personal injury or fatality. May also alert you of potential electrical hazards.

Typeface Conventions	Description
Text represented as a `screen display`	This typeface represents displays that appear on your terminal screen, for example: `Login:`
Text represented as **commands**	This typeface represents commands that you enter, for example: **show ip access-list** This document always gives the full form of a command in lowercase letters. Commands are not case sensitive.
Text represented as a **command** *variable*	This typeface represents a variable that is part of a command, for example: **show card** *slot_number* *slot_number* is a variable representing the desired chassis slot number.
Text represented as menu or sub-menu names	This typeface represents menus and sub-menus that you access within a software application, for example: Click the **File** menu, then click **New**

Supported Documents and Resources

Related Common Documentation

The most up-to-date information for this product is available in the product Release Notes provided with each product release.

The following common documents are available:

- *AAA Interface Administration Guide and Reference*
- *Command Line Interface Reference*
- *GTPP Interface Administration Guide and Reference*
- *Installation Guide* (platform dependent)
- *Release Change Reference*
- *SNMP MIB Reference*
- *Statistics and Counters Reference*
- *System Administration Guide* (platform dependent)
- *Thresholding Configuration Guide*

Related Product Documentation

The following product documents are also available and work in conjunction with the MME:

- *ePDG Administration Guide*
- *IPSec Reference*
- *P-GW Administation Guide*
- *S-GW Administration Guide*
- *SAEGW Administration Guide*
- *SGSN Administration Guide*

Obtaining Documentation

The most current Cisco documentation is available on the following website:

http://www.cisco.com/cisco/web/psa/default.html

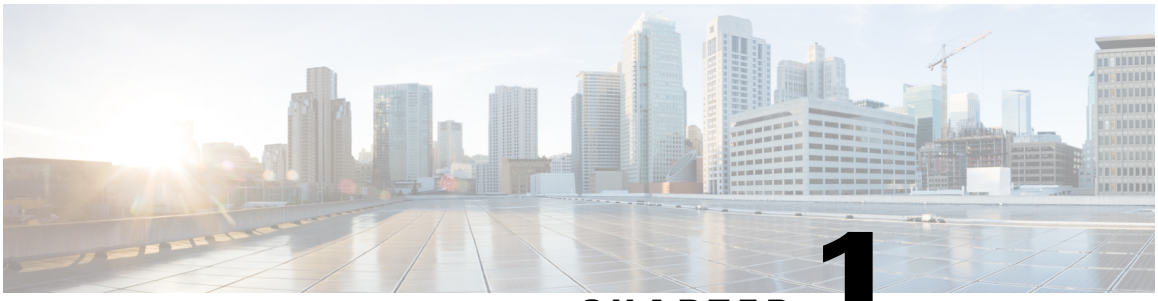
Use the following path selections to access the MME documentation:

Products > Wireless > Mobile Internet> Network Functions > Cisco MME Mobility Management Entity

Contacting Customer Support

Use the information in this section to contact customer support.

Refer to the support area of http://www.cisco.com for up-to-date product documentation or to submit a service request. A valid username and password are required to access this site. Please contact your Cisco sales or service representative for additional information.



CHAPTER 1

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

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 conjunction 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).

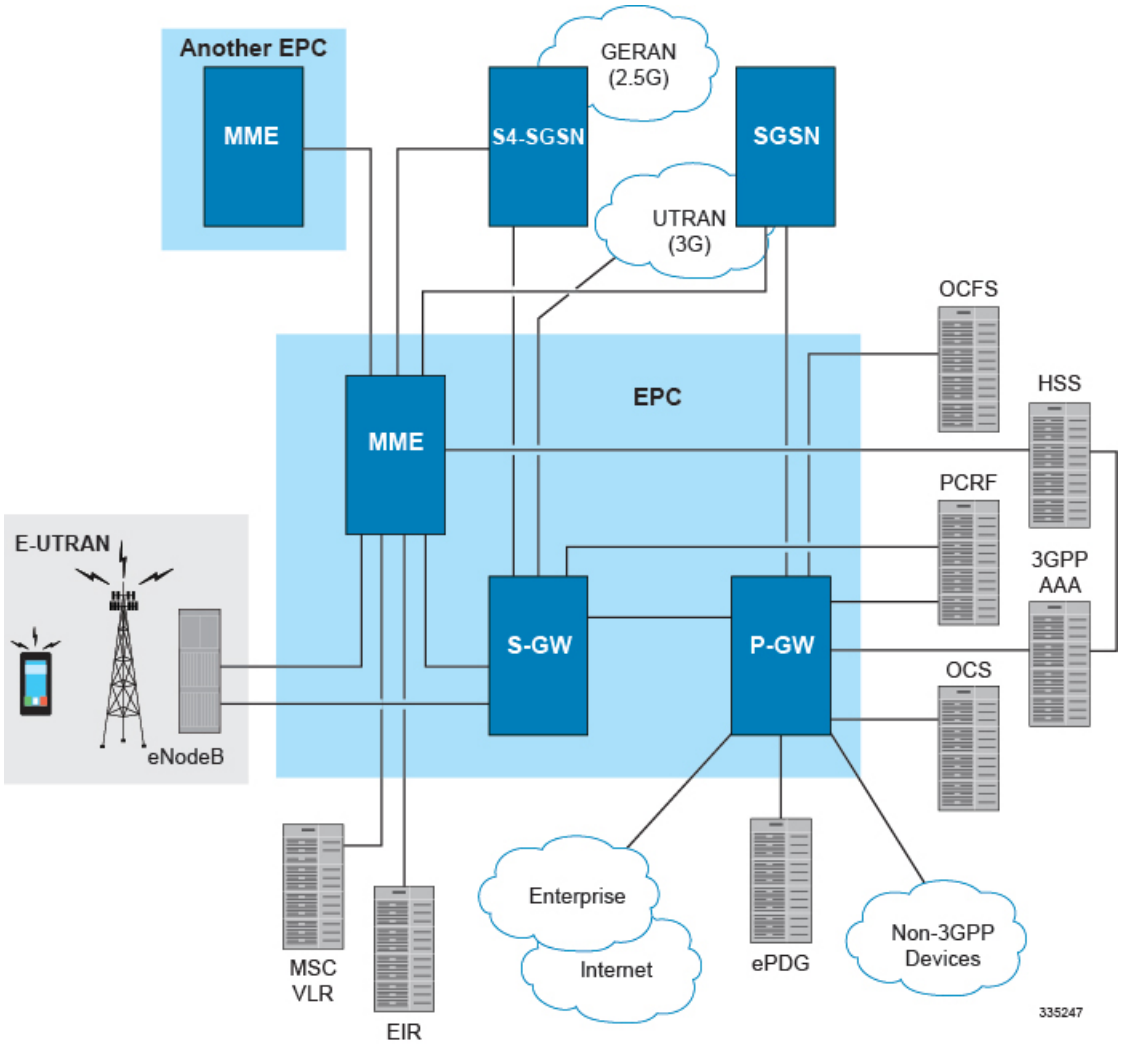
- Works as termination point for Non-Access Stratum (NAS) signaling.
- Responsible for generation and allocation of temporary identities to UEs.
- Checks the authorization of the UE to camp on the service provider's Public Land Mobile Network (PLMN) and enforces UE roaming restrictions.
- The MME is the termination point in the network for ciphering/integrity protection for NAS signaling and handles the security key management.
- Communicates with MMEs in same PLMN or on different PLMNs. The S10 interface is used for MME relocation and MME-to-MME information transfer or handoff.

Besides the above mentioned functions, the lawful interception of signaling is also 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 terminating 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 towards the home HSS for roaming UEs.

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



In accordance with 3GPP standard, the MME provides 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 towards 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 5x00 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*.

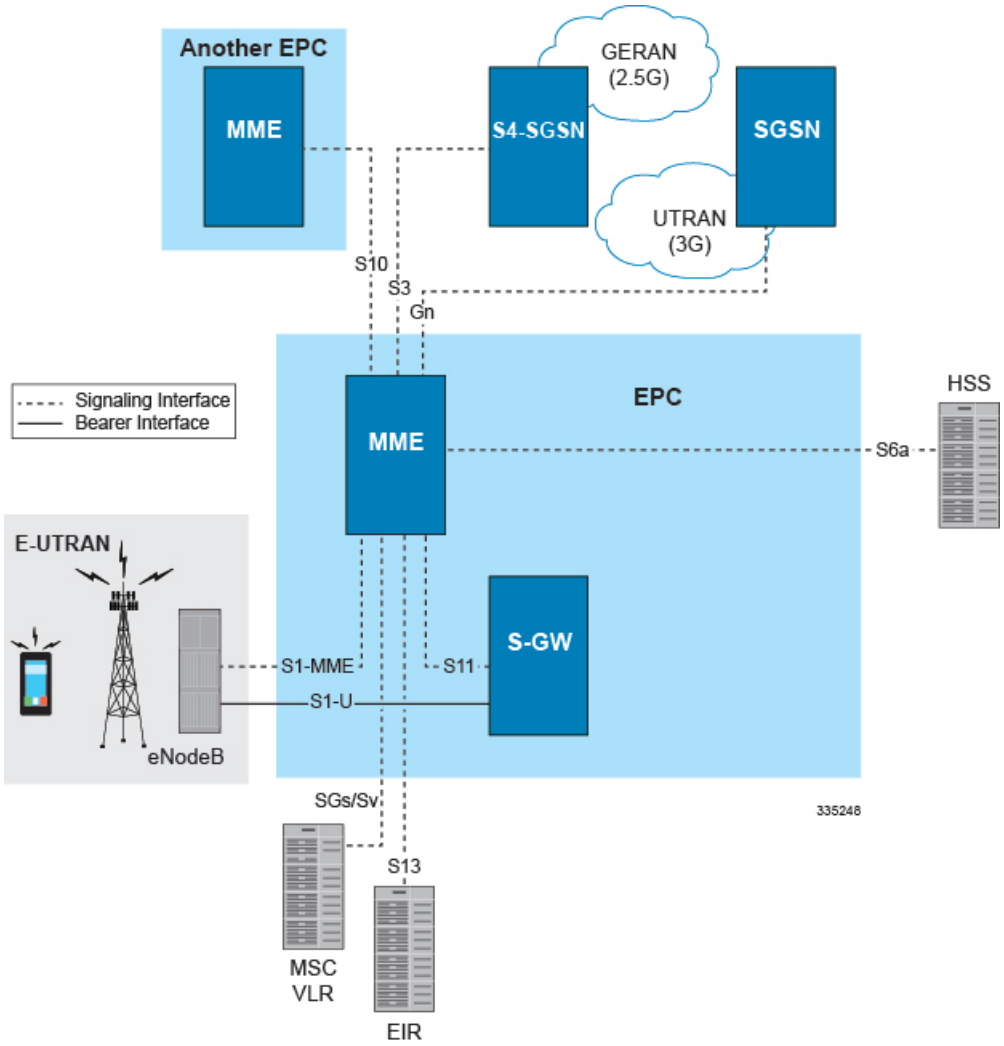
Network Deployment and Interfaces

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

MME in the E-UTRAN/EPC Network

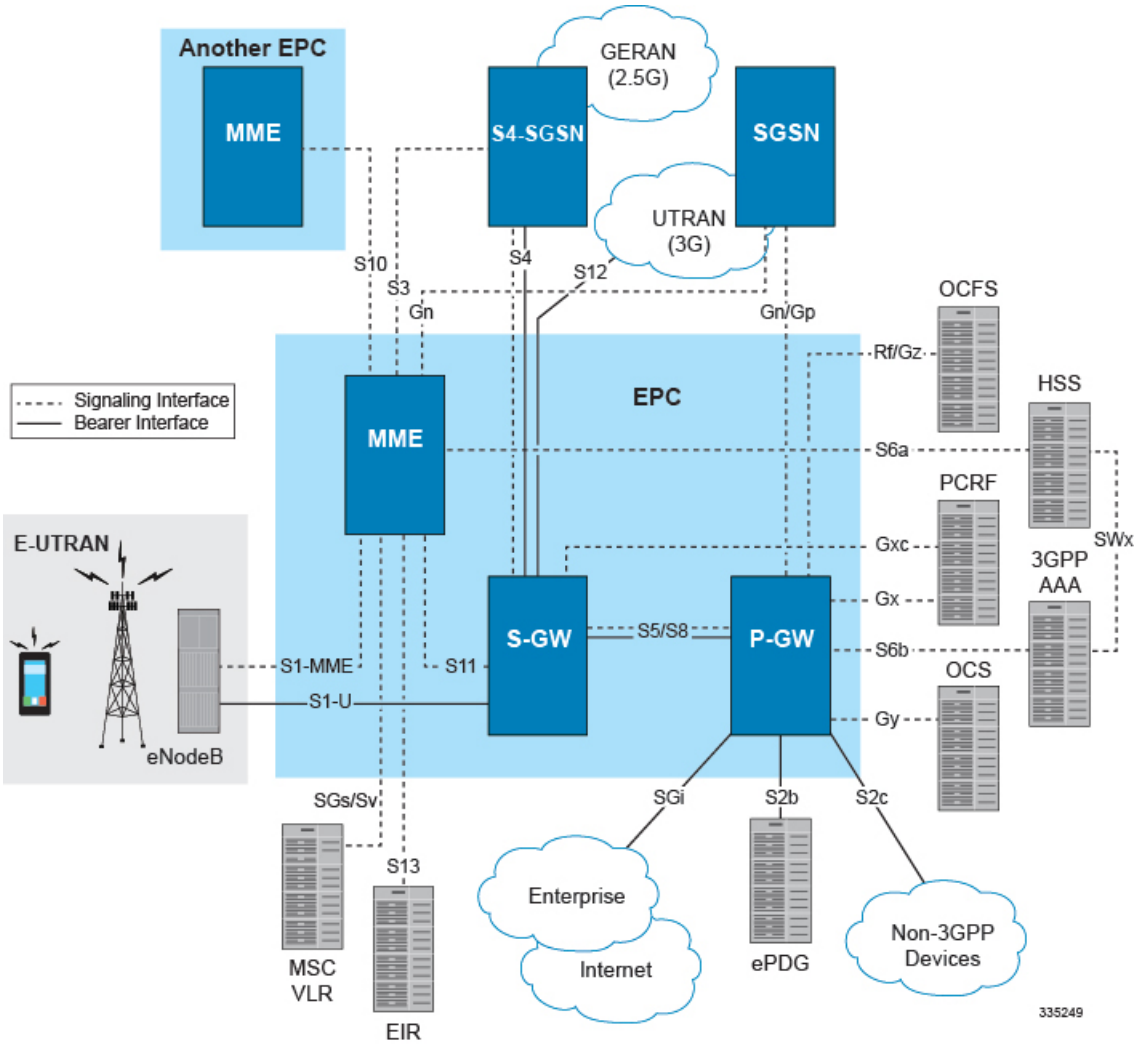
The following figure illustrates the specific network interfaces supported by the MME. Refer to the following section *Supported Logical Network Interfaces (Reference Points)* for detailed information about each interface illustrated in these figures..

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

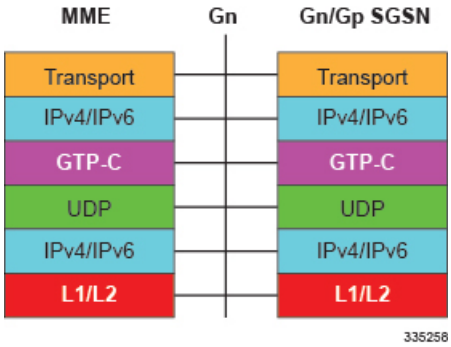
Gn interfaces facilitate user mobility between 2G/3G 3GPP networks. The Gn interface is used for intra-PLMN handovers. The MME supports pre-Release-8 Gn interfaces to allow inter-operation between EPS networks and 2G/3G 3GPP networks.

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.

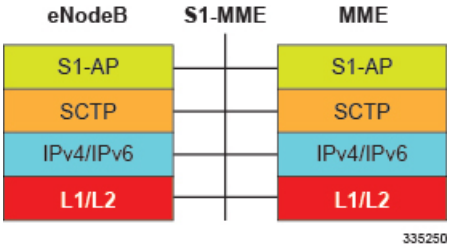
The S1-MME interface supports IPv4, IPv6, IPSec, and multi-homing.

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 From release 20.0 onwards the S1-AP stack in 3GPP R12 complaint.



S3 Interface

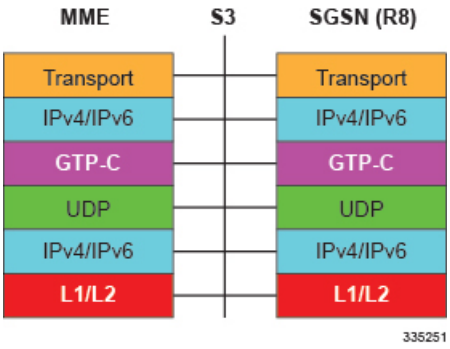
This is the interface used by the MME to communicate with S4-SGSNs on the same Public PLMN for interworking between GPRS/UMTS and LTE network access technologies. This interface serves as the signaling path for establishing and maintaining subscriber UE contexts.

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



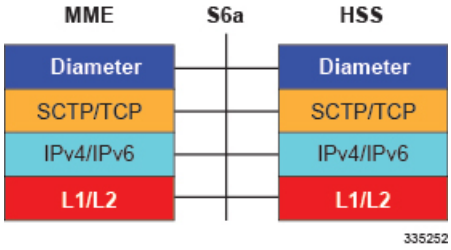
S6a Interface

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



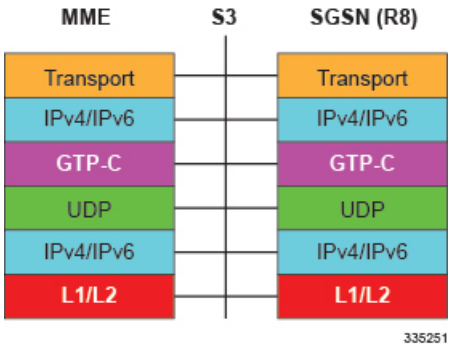
S10 Interface

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



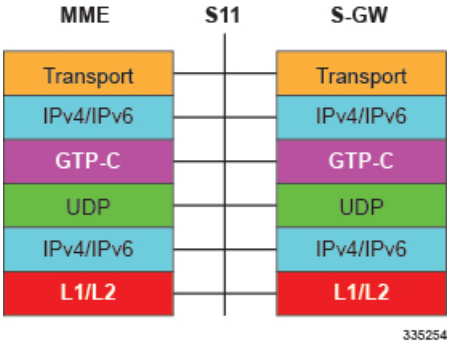
S11 Interface

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



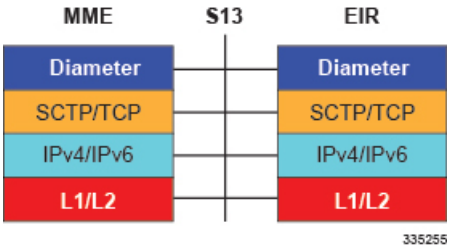
S13 Interface

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

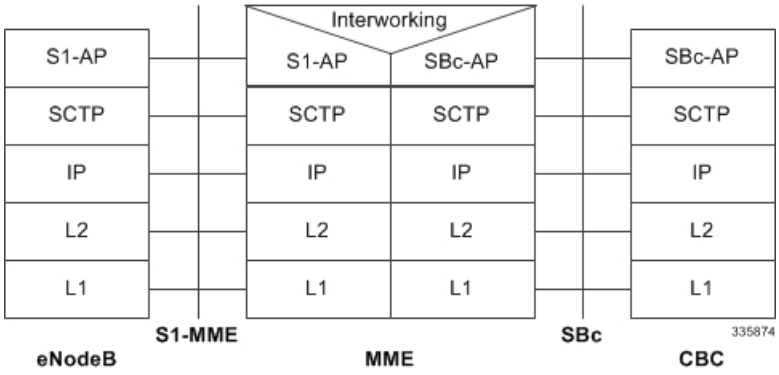


SBc Interface

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

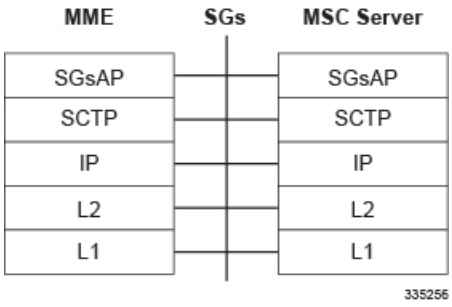


SGs Interface

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

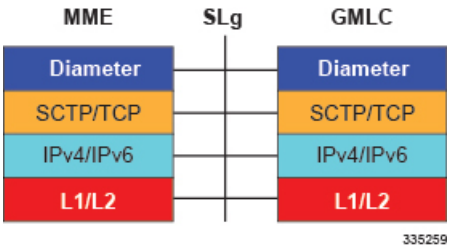


SLg Interface

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

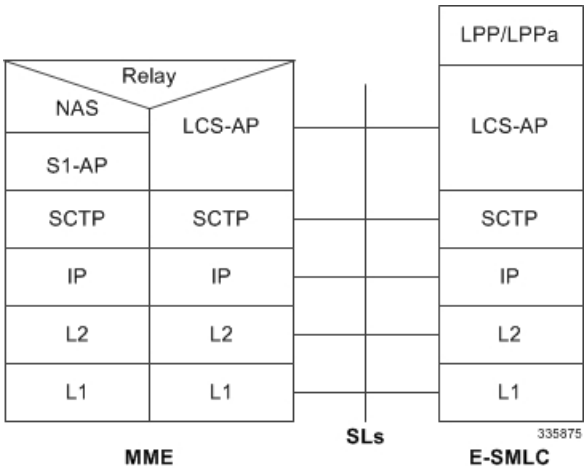


Important MME Software also supports additional interfaces. For more information on additional interfaces, refer to the *Features and Functionality - Licensed Enhanced Feature Software* section.

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

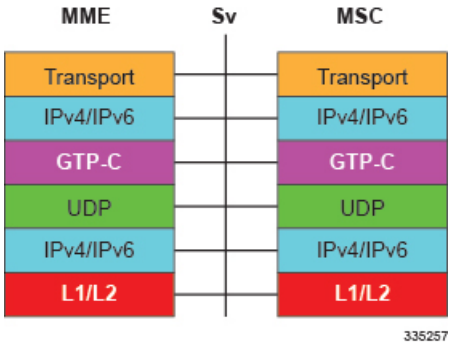


Sv Interface

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.

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 *Cisco ASR 5x00 Series 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.

Define Same TAI in Multiple TAI Lists

Prior to 17.0, 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.

With this enhancement, 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.

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*.

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.

IMSI Manager Scaling

In Release 18.0, with support for the expanded capacities of the VPC-DI and ASR5500 platforms, the IMSIMgr has become a bottleneck. The IMSIMgr Scaling feature increases the number of IMSI managers that can be made available on the MME. - from 1 (ASR5000) to a maximum of 4. The number is configurable.

The IMSIMgr is the de-multiplexing 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 calls 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 (e.g., 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).

As a result of IMSIMgr Scaling, a second behavior change has been implemented. Now all IMSIMgr instances will send the current count of sessions per MME service to the MMEMgr via existing response messaging. The MMEMgr shall send the same data received from multiple IMSIMgr instances back to the IMSIMgr in existing request messaging. As a result, each IMSIMgr shall 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.

Customers will notice the following changes when the number of IMSI managers is set for 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 visualized 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 IMSI Mgr instance.

Important The Exec mode **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.

This feature does not require a special license.

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 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*.

MMEMgr Scaling to Support VPC-DI

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, 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
- Increase in number of MMEMgrs
    - maximum of 12 MMEMgrs in an ASR5K platform
    - maximum of 24 MMEMgrs in either an ASR5500 and a VPC
- Two models of configuration, normal density and high density

For more information about the VPC platform, ask 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.

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

It 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.

The MME implements UEs algorithm (128-EEA1 and 128-EEA2) for NAS Signaling ciphering and SNOW 3G algorithm (128-EIA1 and 128-EIA2) for NAS Signaling integrity protection.

- 128-EIA1= SNOW 3G
- 128-EIA2= UES

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.

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. In previous releases multiple SCTP connections from a VLR were hosted on the same MME manager. 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.

Important In Release 18, this functionality is available as Trial Quality and should only be used in a test environment. In Release 19, this functionality is available as Deploy Quality.

The MME already supports circuit switched fallback (CSFB) and single radio voice call continuity (SRVCC) for E-UTRAN. With release 19.0, 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:

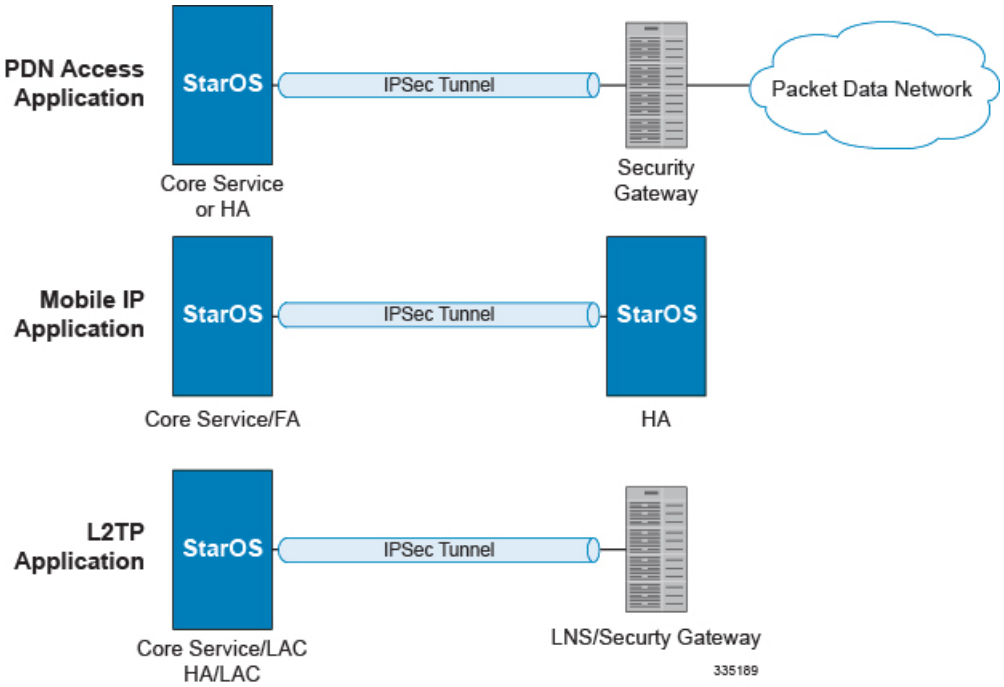
- **PDN Access**: Subscriber IP traffic is routed over an IPSec tunnel from the system to a secure gateway on the packet data network (PDN) as determined by access control list (ACL) criteria.
- **Mobile IP**: Mobile IP control signals and subscriber data is encapsulated in IPSec tunnels that are established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

In this release, 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. Beginning with Release 17.4, 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.

In this release, 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. Beginning with Release 17, 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 now allows configuration of the T3396 back-off timer value.

With this feature, 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, nor store the SM back-off timer expiry time. If an SM request is received and if congestion exists, the request would be rejected based 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 to 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.

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.

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.

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.

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

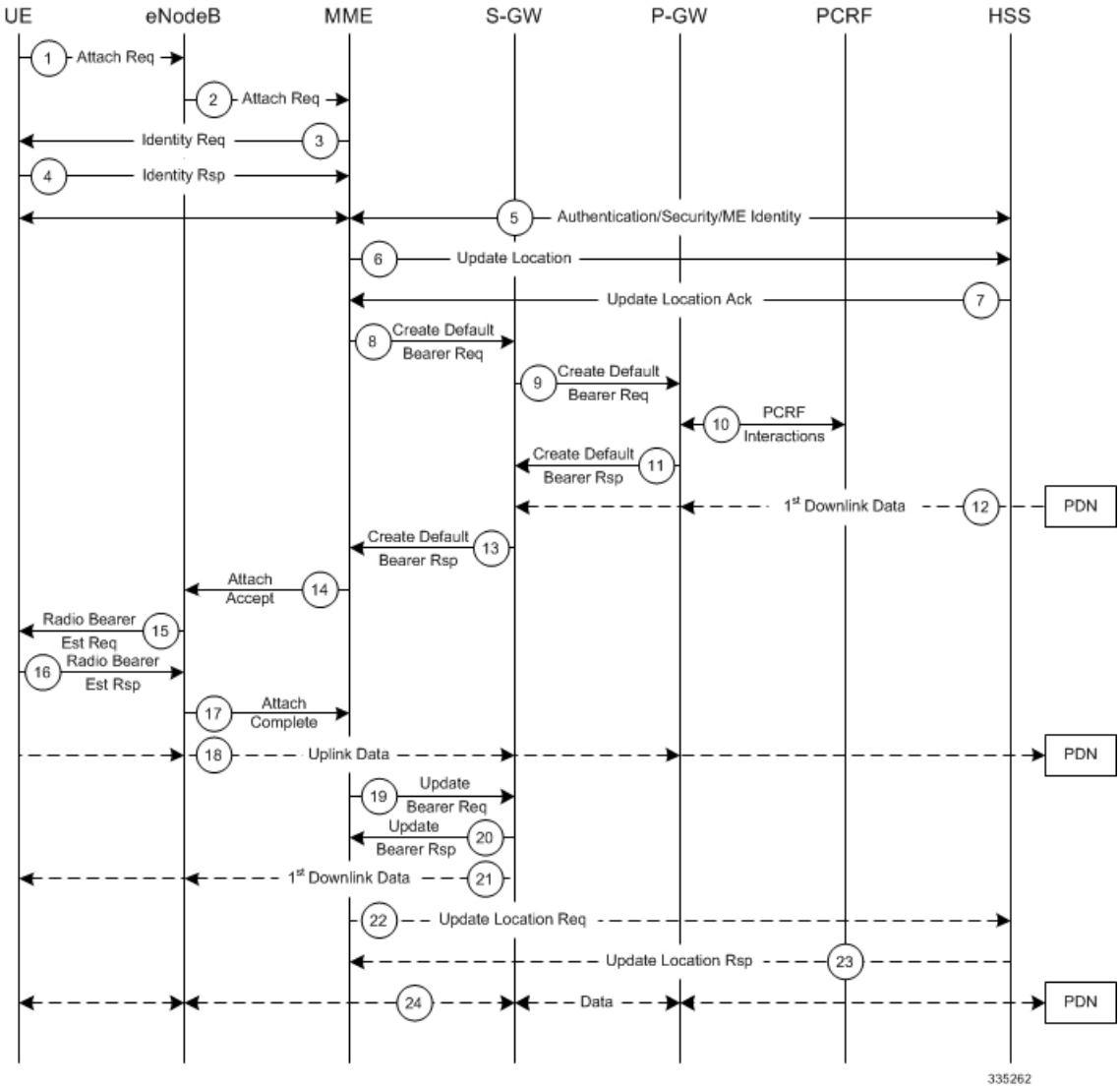


Table 1: Subscriber-initiated Attach (initial) Call Flow Description

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.
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.

Step	Description
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.
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

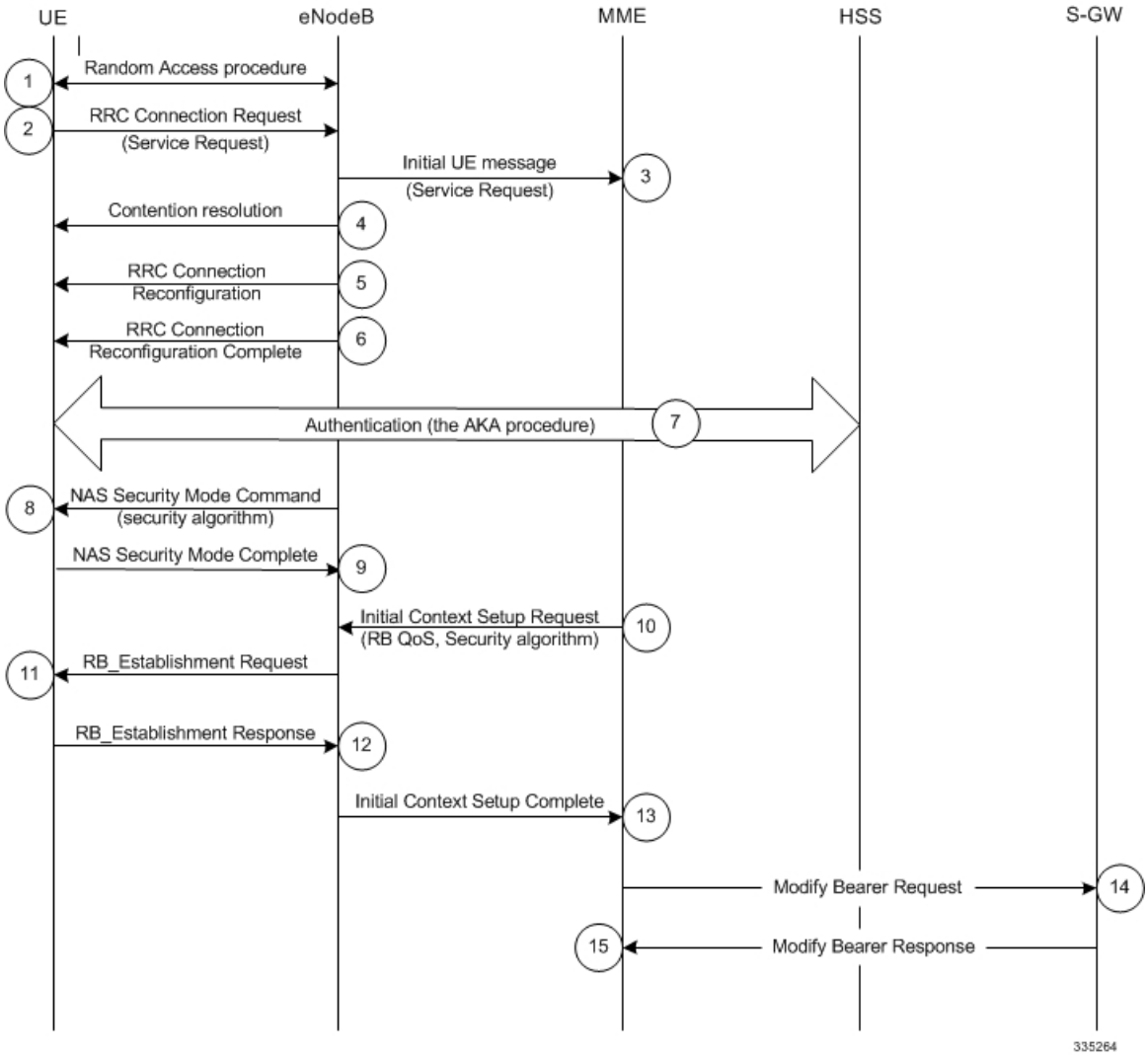


Table 3: UE-initiated Service Request Message Flow Description

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.

Step	Description
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

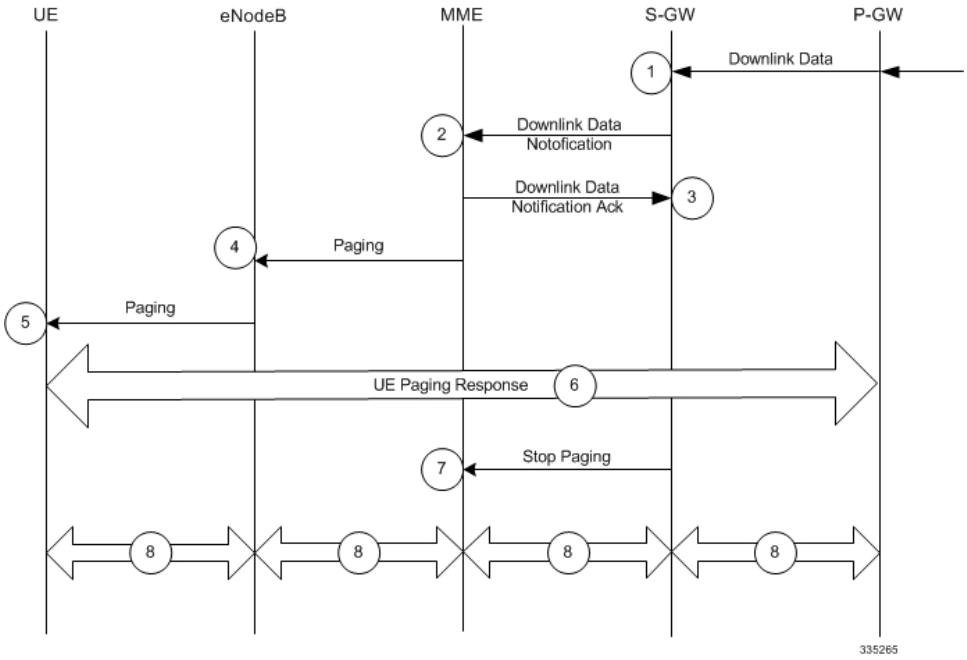


Table 4: Network-initiated Service Request Message Flow Description

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. **Note** Steps 4 and 5 are skipped if the MME has a signaling connection over the S1-MME towards the UE.

Step	Description
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. 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.
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 V12.8.0: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 23.272 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 V12.8.0: General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access
- 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 24.080, 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 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 V10.4.0: 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 V11.6.0: 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

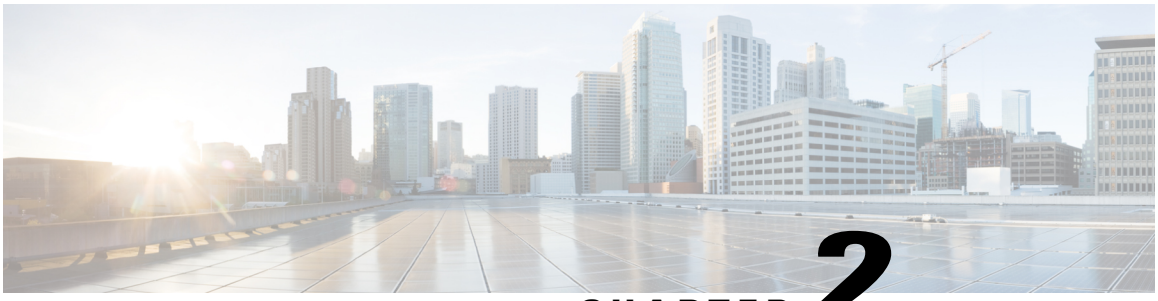
- RFC-1212, Concise MIB Definitions, March 1991
- RFC-1213, Management Information Base for Network Management of TCP/IP-based Internets: MIB-II, March 1991
- RFC-1215, A Convention for Defining Traps for use with the SNMP, March 1991
- RFC-1224, Techniques for managing asynchronously generated alerts, 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



CHAPTER 2

Mobility Management Entity Configuration

This chapter provides configuration information for the Mobility Management Entity (MME).

Because each wireless network is unique, the system is designed with a variety of parameters allowing it to perform in various wireless network environments. In this chapter, only the minimum set of parameters are provided to make the system operational. Optional configuration commands specific to the MME product are located in the *Command Line Interface Reference*.

Important At least one packet processing card must be made active prior to service configuration. Information and instructions for configuring a packet processing card to be active can be found in the *System Settings* chapter of the *System Administration Guide*.

Important Before you plan or modify your MME's configuration, we recommend that you review *Appendix A: Engineering Rules* for the engineering rules and configuration limits hardcoded into the system.

Caution While configuring any base-service or enhanced feature, it is highly recommended to avoid conflicting or blocked IP addresses and port numbers when binding or assigning these to your configuration. In association with some service steering or access control features, the use of inappropriate port numbers may result in communication loss. Refer to the respective feature configuration document carefully before assigning any port number or IP address for communication with internal or external networks.

Important Information about all commands in this chapter can be found in the *Command Line Interface Reference*.

Configuring the System as a Standalone MME (base configuration)

This section provides a high-level series of steps and associated configuration file examples for configuring the system to perform as an MME in a test environment. This section also includes suggestions about the types of information that are needed to be able to configure the MME, as well as information about how the MME works based on some of the possible configurations.

The configurations in this section assume the following:

- A single context (other than the Local context) for all interfaces and services
- Static S-GW/P-GW selection (MME Policy configuration)

Information Required

The following sections describe the minimum amount of information required to configure and make the MME operational on the network. To make the process more efficient, it is recommended that this information be available prior to configuring the system.

There are additional configuration parameters that are not described in this section. These parameters deal mostly with fine-tuning the operation of the S-GW in the network. Information on these parameters can be found in the appropriate sections of the *Command Line Interface Reference*.

Required MME Context Configuration Information

The following table lists the information that is required to configure the MME context.

Table 5: Required Information for MME Context Configuration

Required Information	Description
MME context name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the MME context is recognized by the system.
S1-MME Interface Configuration (To/from eNodeB)	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv4 or IPv6 address assigned to the S1-MME interface. This address will be used for binding the SCTP (local bind address(es)) to communicate with the eNodeBs using S1-AP. Multiple addresses and subnets are needed if multiple interfaces will be configured.

Required Information	Description
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
S11 Interface Configuration (To/from S-GW)	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv4 address assigned to the S11 interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
S6a Interface Configuration (To/from HSS)	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv4 or IPv6 addresses assigned to the S6a interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
S6a Diameter Endpoint Configuration	
End point name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the S6a Diameter endpoint configuration is recognized by the system.

Required Information	Description
Origin realm name	An identification string between 1 through 127 characters. The realm is the Diameter identity. The originator's realm is present in all Diameter messages and is typically the company or service name.
Origin host name	An identification string from 1 to 255 characters (alpha and/or numeric) by which the S6a origin host is recognized by the system.
Origin host address	The IP address of the S6a interface.
Peer name	The S6a endpoint name described above.
Peer realm name	The S6a origin realm name described above.
Peer address and port number	The IP address and port number of the HSS.
Route-entry peer	The S6a endpoint name described above.
S13 Interface Configuration (To/from EIR)	
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv4 or IPv6 addresses assigned to the S13 interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
S13 Diameter Endpoint Configuration	
End point name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the S13 Diameter endpoint configuration is recognized by the system.
Origin realm name	An identification string between 1 through 127 characters. The realm is the Diameter identity. The originator's realm is present in all Diameter messages and is typically the company or service name.
Origin host name	An identification string from 1 to 255 characters (alpha and/or numeric) by which the S13 origin host is recognized by the system.

Required Information	Description
Origin host address	The IP address of the S13 interface.
Peer name	The S13 endpoint name described above.
Peer realm name	The S13 origin realm name described above.
Peer address and port number	The IP address and port number of the EIR.
Route-entry peer	The S13 endpoint name described above.
MME Service Configuration	
MME service name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the MME service can be identified on the system. It is configured in the Context configuration mode. Multiple names are needed if multiple MME services will be configured.
PLMN identifier	The identifier of Public Land Mobile Network (PLMN) of which MME belongs to. PLMN identifier is consisting of MCC and MNC.
MME identifier	The identifier of MME node. The MME Id is consisting of MME group and MME code.
TAI management database name	An identification string from 1 to 64 characters (alpha and/or numeric) by which the TAI management database service can be associated with the MME service. This is required for static S-GW selection. Refer to the *Required MME Policy Configuration Information* section below.
P-GW IP address	IPv4 or IPv6 address of a PDN Gateway (P-GW). This is required for static S-GW/P-GW selection.
eGTP Service Configuration	
eGTP service name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the eGTP service can be associated with MME system. Multiple names are needed if multiple eGTP services will be used.
Interface type	Identifies the type of interface to which the eGTP service is bound. This interface type is "interface-mme".
GTP-C binding IP address	The IPv4 address of the S11 interface.
HSS Peer Service Configuration	

Required Information	Description
HSS peer service name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the HSS peer service is recognized by the system. Multiple names are needed if multiple HSS peer services will be used.
Diameter HSS peer	The name for a pre-configured Diameter endpoint, configured on system to associate with this MME service to access an HSS and an EIR. This is the S6a Diameter endpoint name.

Required MME Policy Configuration Information

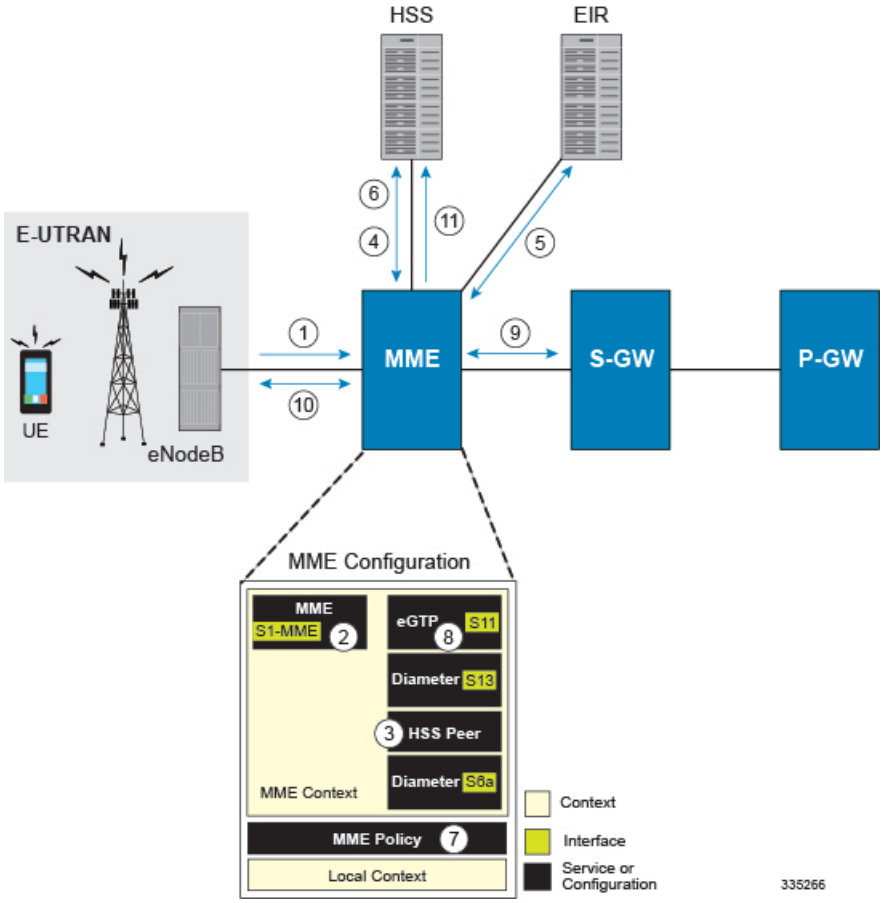
The following table lists the information that is required to configure the MME Policy on an MME.

Table 6: Required Information for MME Policy Configuration

Required Information	Description
Tracking Area Identifier (TAI) management database name	An identification string from 1 to 64 characters (alpha and/or numeric) by which the TAI management database is recognized by the system.
Tracking Area Identifier (TAI) management object name	An identification string from 1 to 64 characters (alpha and/or numeric) by which the TAI management object is recognized by the system.
MCC, MNC, and TAC	The Mobile Country Code, Mobile Network Code, and Tracking Area Code for the S-GW this management object represents.
S-GW IP address	The IPv4 or IPv6 address of the S-GW this management object represents.

How This Configuration Works

The following figure and supporting text describe how this configuration with a single context is used by the system to process a subscriber call originating from the GTP LTE network.



1. The eNodeB forwards an Attach Request message from the UE to the MME containing the IMSI, last visited TAI (if available), the UE's core network capability, the PDN Type, and the Attach Type.
2. The MME service receives the Attach Request message and references the HSS peer service for authentication and location resolution.
3. The HSS peer service configuration specifies the Diameter configuration and S6a interface to use to communicate with the HSS and the Diameter configuration and S13 interface to use to communicate with the Equipment Identity Register (EIR).
4. Assuming that the MME has no previous security context, it sends an S6a Authentication Request to the HSS and uses the authentication vectors received in the response to complete the authentication procedure with UE.
5. After authentication, the MME proceeds to do a security setup with the UE. During this procedure, the ME identity is transferred to the MME which then queries the EIR.
6. The MME then sends an Update Location Request to the HSS and obtains relevant subscription data for the IMSI in the response.
7. The MME policy is accessed to determine the S-GW and P-GW to which the UE should be attached.
8. The MME uses the S11 interface bound to the eGTP service to communicate with the S-GW specified by the MME policy configuration.

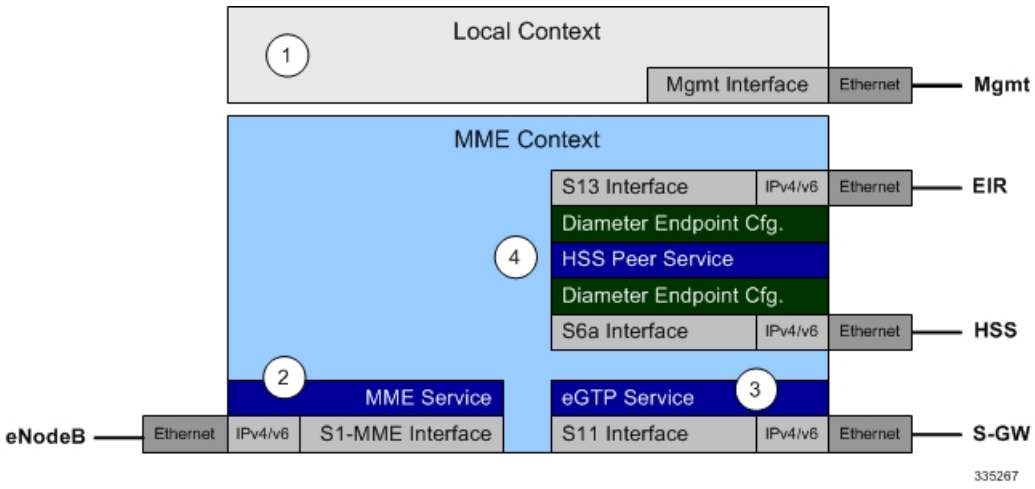
9 The MME then sends a Create Session Request to S-GW which is also forwarded to the specified P-GW (assuming GTP-S5/S8) P-GW establishes the S5/S8 GTPU bearers and then responds with a Create-Session-response which is forwarded to the MME by the S-GW. The S-GW includes the relevant S1-U bearer information.

10 The MME then sends a NAS Attach Accept embedded in the S1 Init Ctxt Setup request to the eNodeB. The Attach Accept contains the IP address allocated to the PDN and the temporary identifier (GUTI) assigned to the UE. The MME waits for positive acknowledgment from both the eNodeB (Init Ctxt Setup response) and UE (Attach Complete). The Init Ctxt Setup Response contains the S1-U bearer endpoint information. The MME then uses the S11 Modify Bearer Request to update the eNodeB endpoints with the S-GW. The receipt of the S11 Modify Bearer Response completes the end-to-end bearer setup.

11 The MME then uses the S6a Notify Request to update the HSS with the APN and P-GW identity.

MME Configuration

To configure the system to perform as a standalone eGTP S-GW, review the following graphic and subsequent steps.



Step 1 Set system configuration parameters such as activating PSCs by applying the example configurations found in the *System Administration Guide*.

Step 2 Create the MME context, service, and all interfaces, and bind the S1-MME interface to an IP address by applying the example configuration in the section.

Step 3 Create the eGTP service and associate it with the S11 interface by applying the example configuration in the section.

Step 4 Create the HSS peer service and associate it with the S6a interface and S13 interface by applying the example configuration in the section.

Step 5 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Creating and Configuring the MME Context and Service

Use the following example to configure the MME context and all supported interfaces:

```
configure
    context mme_context_name -noconfirm
        interface s1-mme_intf_name
            ip address ipv4_address
            exit
        interface s11_intf_name
            ip address ipv4_address
            exit
        interface s6a_intf_name
            ip address ipv4_address
            exit
        interface s13_intf_name
            ip address ipv4_address
            exit
        mme-service mme_svc_name -noconfirm
            mme-id group-id grp_id mme-code mme_code
            plmn-id mcc mcc_value mnc mnc_value
            network-sharing plmnid mcc mcc_value mnc mnc_value mme-id group-id id mme-code
code
            associate egtp-service egtp-service_name context mme_context_name
            associate hss-peer-service hss_peer_service_name context mme_context_name
            policy attach imei-query-type imei-sv verify-equipment-identity
            pgw-address pgw_ip_address
            bind s1-mme ipv4-address ip_address
            exit
        exit
    port ethernet slot_number/port_number
        no shutdown
        bind interface s1-mme_intf_name mme_context_name
        end
```

Notes:

- All interfaces in this configuration can also be specified as IPv6 addresses using the **ipv6 address** command.
- Multi-homing is supported on the S1-MME and S6a interfaces. For more information on configuring multi-homing for the S1-MME and/or S6a interface(s), refer to Configuring SCTP Multi-homing Support, on page 91.
- A maximum of 256 services (regardless of type) can be configured per system.
- The **bind s1-mme** command can also be specified as an IPv6 address using the **ipv6-address** keyword.
- The **network-sharing** command is used to configure an additional PLMN ID for this MME service.
- The eGTP service is configured in the following section.
- The HSS peer service is configured in the configuration sequence for Creating and Configuring the HSS Peer Service and Interface Associations, on page 78.

- In the above example, the mobile equipment identity (IMEI) is checked during the attach procedure. This is configured in the **policy attach** command. Another option is to check IMEI during the tracking area update (TAU). This can be accomplished instead of, or, in addition to, the EIR query during the attach procedure. To check during the TAU, use the **policy tau** command.
- The **pgw-address** command is used to statically configure P-GW discovery.

Creating and Configuring the eGTP Service and Interface Association

Use the following example to create an eGTP service and associate it with the S11 interface.

```
configure
    context mme_context_name
        egtp-service egtp_service_name
            interface-type interface-mme
             gtpc bind ipv4-address s11_infc_ip_address
            exit
        exit
    port ethernet slot_number/port_number
        no shutdown
        bind interface s11_interface_name mme_context_name
        end
```

Notes:

- The **gtpc bind** command can be specified as an IPv6 address using the **ipv6-address** keyword. The interface specified for S11 communication must also be the same IPv6 address.

Creating and Configuring the HSS Peer Service and Interface Associations

Use the following example to create and configure the HSS peer service:

```
configure
    context mme_context_name
        hss-peer-service hss_peer_service_name
            diameter hss-endpoint hss_endpoint_name eir-endpoint eir-endpoint_name
            exit
        exit
        diameter endpoint hss-endpoint_name
                origin realm realm_name
                origin host name address S6a_interface_address
                peer peer_name realm realm_name address hss_ip_address
                route-entry realm realm_name peer peer_name
                exit
        diameter endpoint eir-endpoint_name
                origin realm realm_name
                origin host name address S13_interface_address
                peer peer_name realm realm_name address eir_ip_address
                route-entry realm realm_name peer peer_name
                exit
        port ethernet slot_number/port_number
                no shutdown
                bind interface s6a_interface_name mme_context_name
                exit
        port ethernet slot_number/port_number
```

```
no shutdown
bind interface s13_interface_name mme_context_name
end
```

Notes:

- The **origin host** and **peer** commands can accept multiple IP addresses supporting multi-homing on each endpoint. For information on configuring SCTP multi-homing for the S6a interface, refer to Configuring SCTP Multi-homing Support, on page 91.

Caution On a PSC2 setup, all diamproxy tasks might go in to a warning state if the number of hss-peer-services configured are more than 64 since the memory usage may exceed the allocated value.

Configuring Dynamic Destination Realm Construction for Foreign Subscribers

For a foreign subscriber, the MME does not know the HSS nodes in all the foreign PLMNs. In this case the MME routes S6a/S6d requests directed to foreign PLMNs via a Diameter Routing Agent (DRA) using only the destination realm. The DRA in turn routes the request to the correct HSS based on the destination realm. In order to accomplish this, the MME needs to dynamically construct requests to the DRA/HSS with a Destination Realm representing the foreign PLMN of the UE.

The MME can be configured to derive the EPC Home Network Realm/Domain based on the user's IMSI (MNC and MCC values) and use it as the Destination Realm in all diameter messages.

For home subscribers, the MME will always use the configured peer realm as destination-realm, regardless if dynamic-destination-realm is enabled.

Because MNCs can be 2 or 3 digits long, to provide the ability for an operator to configure the MCC and MNC of foreign PLMNs, the operator policy of the subscriber map is used to determine the MNC value and the length of the MNC. The following steps outline how this configuration can be implemented.

First, enable the dynamic destination realm functionality for the HSS Peer Service:

```
configure
  context ctxt_name
    hss-peer-service HSS1
      dynamic-destination-realm
      end
```

Then configure the foreign PLMNs in the LTE subscriber map. For example:

```
configure
  lte-policy
    subscriber map SM1
      precedence 10 match-criteria imsi mcc 232 mnc 11 operator-policy-name OP.HOME
      precedence 20 match-criteria imsi mcc 374 mnc 130 msin first 700000000 last 800000000
operator-policy-name OP.ROAMING
      end
```

Then associate the subscriber map to the MME Service. For example:

```
configure
  context ingress
    mme-service mmesvc
      associate subscriber-map SM1
      end
```

A static route entry must also be added in the diameter endpoint configuration for each foreign realm. For example:

```
configure
    context ingress
        diameter endpoint s6a1
            peer HSS1 realm HSS-Realm1 address ip-address sctp
            route-entry realm epc.mnc045.mcc123.3gppnetwork.org peer HSS1
            end
```

With this sample configuration, an MNC of length 2 and value of 11 is matched with first operator policy (OP.HOME), and an MNC length of 3 and value of 130 is matched with the second operator policy (OP.ROAMING). With this configuration, the MME will find the MNC based on the operator policy for the foreign subscriber.

If there is no matching entry present in the operator policy, the MME will use the global static table to decide the MNC length and pass that information to Diameter layer to construct the dynamic realm. The following list of MCCs are all considered as 3 digit MNCs. All other MCCs are considered 2 digit MNCs.

302	334	354	405
310	338	356	708
311	342	358	722
312	344	360	732
316	346	365	
	348	376	

The **show hss-peer-service service name** command displays this configuration in the **Destination Realm** field, either **Configured Peer Realm** (default), or **Dynamic Realm**.

```
Request Auth-vectors            : 1
Notify Request Message          : Enable
Destination Realm               : Dynamic Realm
```

Configuring Optional Features on the MME

The configuration examples in this section are optional and provided to cover the most common uses of the MME in a live network. The intent of these examples is to provide a base configuration for testing.

Configuring Differentiation Between HeNB-GW and eNodeBs

The MME can be configured to distinguish the Home eNodeB Gateway (HeNB-GW) from other eNodeBs. This is required to support S1 handovers to Home eNodeBs connected via a HeNB-GW.

As per 3GPP TS 36.300, section 4.6.2, the TAI used in a HeNB-GW should not be reused in another HeNB-GW. The global eNodeB id of the HeNB-GW can now be configured within the lte-policy configuration mode.

In case of S1-based handovers to Home eNodeBs served by a HeNB-GW, the lookup at MME for the target eNodeB based on global ENB id will fail, as MME is aware of only the HeNB-GW. In those cases additional lookup needs to be done based on TAI to find the HeNB-GW serving the Home eNodeB.

This feature allows operators to configure the global eNodeB ids of HeNB-GWs in the MME service. The MME uses this information to perform HeNB-GW related functions.

The following steps create an HeNB-GW management database, configures a single Global eNodeB ID and TAI within the management database, and associates the HeNB-GW management database with the MME service:

```
configure
    lte-policy
        mme henbgw mgmt-db db_name
            henbgw-global-enbid mcc mcc_value mnc mnc_value enbid enbid_value
            end
configure
    context ctxt_name
        mme-service svc_name
            associate henbgw-mgmt-db db_name
            end
```

Notes:

- A maximum of 8 HeNB-GWs can be configured within the HeNB-GW management database.
- The **show lte-policy henbgw-mgmt-db name** *db_name* command displays configuration information about the specified HeNB-GW management database.
- The **show mme-service enodeb-association full** command displays whether the eNodeB is an HeNB-GW by including "(HeNB-GW)" in the output of the **eNodeB Type** field.

Configuring Dual Address Bearers

This example configures support for IPv4/v6 PDNs.

Use the following configuration example to enable support on the MME for dual-address bearers:

```
configure
    context mme_context_name -noconfirm
        mme-service mme_svc_name
            policy network dual-addressing-support
            end
```

Configuring Dynamic Peer Selection

The configuration in this section replaces static configurations on the MME for the following peer components: MME, P-GW, S-GW, SGSN.

Use the following example to configure dynamic P-GW, S-GW, and peer MME selection through a DNS interface:

```
configure
    context mme_context_name -noconfirm
        interface dns_intf_name
            ip address ipv4_address
            exit
        ip domain-lookup
        ip name-servers dns_ip_address
        dns-client name
```

```
        bind address dns_intf_ip_address
        exit
    mme-service mme_svc_name
        dns pgw
        dns sgw
        dns peer-mme
        dns peer-sgsn
        end
```

Notes:

- For the **dns pgw**, **dns sgw**, **dns peer-mme**, and **dns peer-sgsn** commands, the DNS client service must exist in the same context as the MME service. If the DNS client resides in a different context, the **context** command and *ctx_name* variable must be added to the command(s).
- If you have associated a tai-mgmt-db with a call-control-profile, and DNS is to be used for S-GW lookups, the DNS configuration must be configured within the same call-control-profile using the **dns-sgw** command present within the call-control-profile configuration mode.

Configuring Emergency Session Support

The configuration example in this section enables emergency bearer session support on the MME.

Use the following configuration example to enable emergency bearer services on the MME:

```
configure
  lte-policy
    lte-emergency-profile profile_name
      ambr max-ul bitrate max-dl bitrate
      apn apn_name pdn-type type
      pgw ip-address address protocol type weight value
      qos qci qci arp arp_value preemption-capability capability vulnerability type
      ue-validation-level type
      exit
    mme-service mme_svc_name
      associate lte-emergency-profile profile_name
      end
```

Notes:

- A maximum of four LTE emergency profiles can be configured on the system.
- In the **apn** command, the valid PDN types are: **ipv4**, **ipv4v6**, and **ipv6**.
- In the **pgw** command, the valid protocol types are: **both**, **gtp**, and **pmip**. A maximum of four P-GW IP addresses can be configured per profile. An FQDN can also be configured in place of the IP addresses but only one P-GW FQDN can be configured per profile.
- In the **qos** command, the valid preemption capabilities are: **may** and **shall not**. The valid vulnerability types are: **not-preemptable** and **preemptable**.
- The **ue-validation-level** types are: **auth-only**, **full**, **imsi**, and **none**.
- To configure the MME to ignore the IMEI validation of the equipment during the attach procedure in emergency cases, use the following command in the **mme-service** configuration mode:
  policy attach imei-query-type imei | imei-sv | none verify-equipment-identity verify-emergency

- To configure the MME to ignore the IMEI validation of the equipment during TAU procedures in emergency cases, use the following command in the **mme-service** configuration mode:
  policy tau imei-query-type imei | imei-sv | none verify-equipment-identity verify-emergency

Configuring Gn/Gp Handover Capability

The example configuration in this section provides 3G to 4G handover capabilities between the MME and a Gn/Gp SGSN. The configuration creates the Gn interface used for control signaling during the handover.

Use the following configuration example to create a Gn interface and configure the control interface on the MME for Gn/Gp handovers:

```
configure
   context mme_context_name -noconfirm
      interface Gn_intf_name
         ip address ipv4_address
         exit
      sgtp-service sgtp_svc_name
         gtpc bind address Gn_intf_ip_address
         exit
      mme-service mme_svc_name
         associate sgtpc-service sgtp_svc_name
         peer-sgsn rai mcc mcc_value mnc mnc_value rac value lac value address ip_address
capability gn
         nri length length plmn-id mcc mcc_value mnc mnc_value
         end
```

Notes:

- The **peer-sgsn** command is used to statically configure a peer SGSN. SGSN selection can also be performed dynamically through the DNS client. For more information about dynamic peer selection, refer to the Configuring Dynamic Peer Selection, on page 81 in this chapter.
- If dynamic peer-SGSN selection is configured, an additional **gtpc** command must be added to the SGTP service: **gtpc dns-sgsn context** *cntxt_name*
- In the absence of an NRI length configuration, the MME treats the NRI as invalid. The MME will use a plain RAI-based FQDN (and not an NRI-based FQDN) for DNS queries made to resolve the source SGSN.

Configuring Inter-MME Handover Support

Use the following example to configure inter-MME handover support:

```
configure
   context mme_context_name -noconfirm
      interface s10_intf_name
         ip address ipv4_address
         exit
      egtp-service egtp_service_name
         interface-type interface-mme
         gtpc bind ipv4-address s10_infc_ip_address
         exit
      exit
```

```
        mme-service mme_svc_name
            peer-mme gummei mcc number mnc number group-id id mme-code code address
ipv4_address
            exit
        exit
    port ethernet slot_number/port_number
        no shutdown
        bind interface s10_interface_name mme_context_name
        end
```

Notes:

- The S10 IP address can also be specified as an IPv6 address. To support this, the **ip address** command can be changed to the **ipv6 address** command.
- The **peer-mme** command can also be configured to acquire a peer MME through the use of a TAI match as shown in this command example:
  peer-mme tai-match priority *value* **mcc** *number* **mnc** *number* **tac any address** *ipv4_address*
- The **peer-mme** command is used to statically configure a peer MME. MME selection can also be performed dynamically through the DNS client. For more information about dynamic peer selection, refer to the Configuring Dynamic Peer Selection, on page 81 in this chapter.
- The peer MME IP address can also be specified as an IPv6 address.

Configuring X.509 Certificate-based Peer Authentication

The configuration example in this section enables X.509 certificate-based peer authentication, which can be used as the authentication method for IP Security on the MME.

Important Use of the IP Security feature requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

The following configuration example enables X.509 certificate-based peer authentication on the MME.

In Global Configuration Mode, specify the name of the X.509 certificate and CA certificate, as follows:

```
configure
    certificate name cert_name pem url cert_pem_url private-key pprivate-keyem url private_key_url
    ca-certificate name ca_cert_name pem url ca_cert_url
    end
```

Notes:

- The **certificate name** and **ca-certificate list ca-cert-name** commands specify the X.509 certificate and CA certificate to be used.
- The PEM-formatted data for the certificate and CA certificate can be specified, or the information can be read from a file via a specified URL as shown in this example.

When creating the crypto template for IPSec in the Context Configuration Mode, bind the X.509 certificate and CA certificate to the crypto template and enable X.509 certificate-based peer authentication for the local and remote nodes, as follows:

```
configure
    context mme_context_name
```

```
crypto template crypto_template_name ikev2-dynamic
    certificate name cert_name
    ca-certificate list ca-cert-name ca_cert_name
    authentication local certificate
    authentication remote certificate
    end
```

Notes:

- A maximum of sixteen certificates and sixteen CA certificates are supported per system. One certificate is supported per service, and a maximum of four CA certificates can be bound to one crypto template.
- The **certificate name** and **ca-certificate list ca-cert-name** commands bind the certificate and CA certificate to the crypto template.
- The **authentication local certificate** and **authentication remote certificate** commands enable X.509 certificate-based peer authentication for the local and remote nodes.

Configuring Dynamic Node-to-Node IP Security on the S1-MME Interface

The configuration example in this section creates an IKEv2/IPSec dynamic node-to-node tunnel endpoint on the S1-MME interface.

Important Use of the IP Security feature requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

Creating and Configuring an IPSec Transform Set

The following example configures an IPSec transform set which is used to define the security association that determines the protocols used to protect the data on the interface:

```
configure
    context <mme_context_name>
        ipsec transform-set <ipsec_transform-set_name>
            encryption aes-cbc-128
            group none
            hmac sha1-96
            mode tunnel
            end
```

Notes:

- The encryption algorithm, **aes-cbc-128**, or Advanced Encryption Standard Cipher Block Chaining, is the default algorithm for IPSec transform sets configured on the system.
- The **group none** command specifies that no crypto strength is included and that Perfect Forward Secrecy is disabled. This is the default setting for IPSec transform sets configured on the system.
- The **hmac** command configures the Encapsulating Security Payload (ESP) integrity algorithm. The **sha1-96** keyword uses a 160-bit secret key to produce a 160-bit authenticator value. This is the default setting for IPSec transform sets configured on the system.
- The **mode tunnel** command specifies that the entire packet is to be encapsulated by the IPSec header including the IP header. This is the default setting for IPSec transform sets configured on the system.

Creating and Configuring an IKEv2 Transform Set

The following example configures an IKEv2 transform set:

```
configure
    context <mme_context_name>
        ikev2-ikesa transform-set <ikev2_transform-set_name>
            encryption aes-cbc-128
            group 2
            hmac sha1-96
            lifetime <sec>
            prf sha1
            end
```

Notes:

- The encryption algorithm, **aes-cbc-128**, or Advanced Encryption Standard Cipher Block Chaining, is the default algorithm for IKEv2 transform sets configured on the system.
- The **group 2** command specifies the Diffie-Hellman algorithm as Group 2, indicating medium security. The Diffie-Hellman algorithm controls the strength of the crypto exponentials. This is the default setting for IKEv2 transform sets configured on the system.
- The **hmac** command configures the Encapsulating Security Payload (ESP) integrity algorithm. The **sha1-96** keyword uses a 160-bit secret key to produce a 160-bit authenticator value. This is the default setting for IKEv2 transform sets configured on the system.
- The **lifetime** command configures the time the security key is allowed to exist, in seconds.
- The **prf** command configures the IKE Pseudo-random Function, which produces a string of bits that cannot be distinguished from a random bit string without knowledge of the secret key. The **sha1** keyword uses a 160-bit secret key to produce a 160-bit authenticator value. This is the default setting for IKEv2 transform sets configured on the system.

Creating and Configuring a Crypto Template

The following example configures an IKEv2 crypto template:

```
configure
    context <mme_context_name>
        crypto template <crypto_template_name> ikev2-dynamic
            authentication local pre-shared-key key <text>
            authentication remote pre-shared-key key <text>
            ikev2-ikesa transform-set list <name1> . . . <name6>
            ikevs-ikesa rekey
            payload <name> match childsa match ipv4
                ipsec transform-set list <name1> . . . <name4>
                rekey
                end
```

Notes:

- The **ikev2-ikesa transform-set list** command specifies up to six IKEv2 transform sets.
- The **ipsec transform-set list** command specifies up to four IPSec transform sets.

Binding the S1-MME IP Address to the Crypto Template

The following example configures the binding of the S1-MME interface to the crypto template:

configure
context *<mme_context_name>*
mme-service *<mme_svc_name>*
bind s1-mme ipv4-address *<address>* **ipv4-address** *<address>* **crypto-template** *<enodeb_crypto_template>*
end

Notes:

- The **bind** command in the MME service configuration can also be specified as an IPv6 address using the **ipv6-address** command.
- This example shows the **bind** command using multi-homed addresses. The multi-homing feature also supports the use of IPv6 addresses.

Configuring ACL-based Node-to-Node IP Security on the S1-MME Interface

The configuration example in this section creates an IKEv2/IPSec ACL-based node-to-node tunnel endpoint on the S1-MME interface.

Important Use of the IP Security feature requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

Creating and Configuring a Crypto Access Control List

The following example configures a crypto ACL (Access Control List), which defines the matching criteria used for routing subscriber data packets over an IPSec tunnel:

configure
context *<mme_context_name>*
ip access-list *<acl_name>*
permit tcp host *<source_host_address>* **host** *<dest_host_address>*
end

Notes:

- The **permit** command in this example routes IPv4 traffic from the server with the specified source host IPv4 address to the server with the specified destination host IPv4 address.

Creating and Configuring an IPSec Transform Set

The following example configures an IPSec transform set which is used to define the security association that determines the protocols used to protect the data on the interface:

configure
context *<mme_context_name>*
ipsec transform-set *<ipsec_transform-set_name>*

```
encryption aes-cbc-128
group none
hmac sha1-96
mode tunnel
end
```

Notes:

- The encryption algorithm, **aes-cbc-128**, or Advanced Encryption Standard Cipher Block Chaining, is the default algorithm for IPSec transform sets configured on the system.
- The **group none** command specifies that no crypto strength is included and that Perfect Forward Secrecy is disabled. This is the default setting for IPSec transform sets configured on the system.
- The **hmac** command configures the Encapsulating Security Payload (ESP) integrity algorithm. The **sha1-96** keyword uses a 160-bit secret key to produce a 160-bit authenticator value. This is the default setting for IPSec transform sets configured on the system.
- The **mode tunnel** command specifies that the entire packet is to be encapsulated by the IPSec header including the IP header. This is the default setting for IPSec transform sets configured on the system.

Creating and Configuring an IKEv2 Transform Set

The following example configures an IKEv2 transform set:

```
configure
    context <mme_context_name>
        ikev2-ikesa transform-set <ikev2_transform-set_name>
            encryption aes-cbc-128
            group 2
            hmac sha1-96
            lifetime <sec>
            prf sha1
            end
```

Notes:

- The encryption algorithm, **aes-cbc-128**, or Advanced Encryption Standard Cipher Block Chaining, is the default algorithm for IKEv2 transform sets configured on the system.
- The **group 2** command specifies the Diffie-Hellman algorithm as Group 2, indicating medium security. The Diffie-Hellman algorithm controls the strength of the crypto exponentials. This is the default setting for IKEv2 transform sets configured on the system.
- The **hmac** command configures the Encapsulating Security Payload (ESP) integrity algorithm. The **sha1-96** keyword uses a 160-bit secret key to produce a 160-bit authenticator value. This is the default setting for IKEv2 transform sets configured on the system.
- The **lifetime** command configures the time the security key is allowed to exist, in seconds.
- The **prf** command configures the IKE Pseudo-random Function which produces a string of bits that cannot be distinguished from a random bit string without knowledge of the secret key. The **sha1** keyword uses a 160-bit secret key to produce a 160-bit authenticator value. This is the default setting for IKEv2 transform sets configured on the system.

Creating and Configuring a Crypto Map

The following example configures an IKEv2 crypto map:

```
configure
    context <mme_context_name>
        crypto map <crypto_map_name> ikev2-ipv4
            match address <acl_name>
            peer <ipv4_address>
            authentication local pre-shared-key key <text>
            authentication remote pre-shared-key key <text>
            ikev2-ikesa transform-set list <name1> . . . <name6>
            payload <name> match ipv4
                lifetime <seconds>
                ipsec transform-set list <name1> . . . <name4>
                exit
            exit
        interface <s1-mme_intf_name>
            ip address <ipv4_address>
            crypto-map <crypto_map_name>
            exit
        exit
    port ethernet <slot_number/port_number>
        no shutdown
        bind interface <s1-mme_intf_name> <mme_context_name>
        end
```

Notes:

- The type of crypto map used in this example is IKEv2-IPv4 for IPv4 addressing. An IKEv2-IPv6 crypto map can also be used for IPv6 addressing.
- The **ipsec transform-set list** command specifies up to four IPSec transform sets.

Configuring Mobility Restriction Support

Mobility or handover restriction is performed by handover restriction lists configured on the MME. These lists restrict inter-RAT, 3G location area, and/or 4G tracking area handovers based on the configuration in the Handover Restriction List Configuration Mode.

Important Mobility restriction support is only available through the operator policy configuration. For more information on operator policy, refer to the *Operator Policy* chapter in this guide.

Configuring Inter-RAT Handover Restrictions on the MME

Inter-RAT handover restriction configurations on the MME restrict subscribers from participating in handovers to defined radio access network types.

Use the following example to configure this feature:

```
configure
    lte-policy
```

```
ho-restrict-list <name>
    forbidden inter-rat cdma2000
    end
```

Notes:

- Other forbidden inter-RAT choices are: all, GERAN, and UNTRAN.
- This configuration will only become operational when it is associated with a call control profile. Only one handover restriction list can be associated with a call control profile.

Configuring Location Area Handover Restrictions on the MME

Location area handover restriction lists on the MME restrict subscribers from participating in handovers to specific 3G location area codes.

Use the following example to configure this feature:

```
configure
  lte-policy
    ho-restrict-list name
      forbidden location-area plmnid id
        lac area_code area_code area_code +
        end
```

Notes:

- Up to 16 forbidden location areas can be configured per handover restriction list.
- Up to 128 location area codes can be entered in a single **lac** command line.
- This configuration will only become operational when it is associated with a call control profile. Only one handover restriction list can be associated with a call control profile.

Configuring Tracking Area Handover Restrictions on the MME

Tracking area handover restriction lists on the MME restrict subscribers from participating in handovers to specific 4G tracking area codes.

Use the following example to configure this feature:

```
configure
  lte-policy
    ho-restrict-list name
      forbidden tracking-area plmnid id
        tac area_code [ area_code + ]
        end
```

Notes:

- Up to 16 forbidden tracking areas can be configured per handover restriction list.
- Up to 128 tracking area codes can be entered in a single **tac** command line.
- This configuration will only become operational when it is associated with a call control profile. Only one handover restriction list can be associated with a call control profile.

Configuring S4-SGSN Handover Capability

This configuration example configures an S3 interface supporting inter-RAT handovers between the MME and an S4-SGSN.

Use the following example to configure this feature:

```
configure
    context mme_context_name -noconfirm
        interface s3_interface_name
            ip address ipv4_address
            exit
        mme-service mme_svc_name
            peer-sgsn rai mcc mcc_value mnc mnc_value rac value lac value address ip_address
capability s3
            nri length length plmn-id mcc mcc_value mnc mnc_value
            exit
        exit
    port ethernet slot_number/port_number
        no shutdown
        bind interface s3_interface_name mme_context_name
        end
```

Notes:

- The S3 IP address can also be specified as an IPv6 address. To support this, the **ip address** command can be changed to the **ipv6 address** command.
- The **peer-sgsn** command is used to statically configure a peer SGSN. SGSN selection can also be performed dynamically through the DNS client. For more information about dynamic peer selection, refer to the Configuring Dynamic Peer Selection, on page 81 section in this chapter.
- In the absence of an NRI length configuration, the MME treats the NRI as invalid. The MME will use a plain RAI-based FQDN (and not an NRI-based FQDN) for DNS queries made to resolve the source SGSN.

Configuring SCTP Multi-homing Support

SCTP multi-homing can be configured on the S1-MME interface (to/from eNodeB), the S6a interface (to/from HLR/HSS), and the SGs interface (to/from the MSC/VLR).

Configuring SCTP Multi-homing on the S1-MME Interface

Up to two IPv4 or IPv6 addresses for the S1-MME interface can be entered to allow for SCTP multi-homing.

The configuration example in this section is intended as a replacement for the S1-MME interface configuration located in the section for Creating and Configuring the MME Context and Service, on page 77. Use the following example to configure S1-MME multi-homing between the MME and the eNodeB:

```
configure
    context mme_context_name -noconfirm
        interface s1-mme_intf_name
            ip address ipv4_address
            ip address secondary_ipv4_address
```

```
        exit
    mme-service mme_svc_name
        bind s1-mme ipv4-address ipv4_address ipv4-address secondary_ipv4_address
        exit
    exit
port ethernet slot_number/port_number
    no shutdown
    bind interface s1-mme_intf_name mme_context_name
    end
```

Notes:

- The S1-MME IP addresses can also be specified as IPv6 addresses using the **ipv6 address** keyword.
- The IP addresses in the **bind s1-mme ipv4-address** command can also be specified as IPv6 addresses using the **ipv6-address** keyword.

Configuring SCTP Multi-homing on the S6a Interface

Up to four IPv4 or IPv6 addresses for the S6a interface can be configured to allow for SCTP multi-homing.

The configuration example in this section is intended as a replacement for the S6a interface configuration located in Creating and Configuring the MME Context and Service, on page 77 section and the Diameter configuration for the S6a interface located in Creating and Configuring the HSS Peer Service and Interface Associations, on page 78 . Use the following example to configure S6a multi-homing between the MME and the HLR/HSS:

```
configure
    context mme_context_name
        interface s6a_intf_name
            ip address s6a_intf_primary_ip_addr ip_mask
            ip address s6a_intf_secondary_ip_addr2 ip_mask secondary
            ip address s6a_intf_secondary_ip_addr3 ip_mask secondary
            exit
        exit
    diameter endpoint hss-endpoint_name
        origin realm realm_name
        origin host name address s6a_intf_primary_ip_addr port number address
s6a_intf_secondary_ip_addr2 port number address s6a_intf_secondary_ip_addr3 port number
        peer peer_name realm realm_name address hss_ip_addr1 port number address hss_ip_addr2
 port number sctp
        route-entry realm realm_name peer peer_name
        exit
    port ethernet slot_number/port_number
        no shutdown
        bind interface s6a_intf_name mme_context_name
        exit
```

Notes:

- The S6a IP addresses can also be specified as IPv6 addresses using the **ipv6 address** keyword.

Configuring S6a SCTP and Application Timers for Multi-homing

In the event of a path failure, the SCTP multi-homing feature requires time to activate the alternate path. Timers associated with the SCTP heartbeat and the application in this instance, a Diameter watchdog request,

must be tuned properly to ensure that the application does not timeout before the redundant SCTP path can be activated. The required calculation is based on the two paths configured between the MME and the HSS, the maximum retransmission configuration for the SCTP paths, and the SCTP heartbeat timeout configuration. The configuration of the timers must be identical on both peers.

The recommended SCTP timer values are provided below in the first row for the Diameter application default values that follow the typical case of two paths between the MME and HSS SCTP peers. SCTP HB interval can be in the range of 1 to 10 seconds, since (10 sec x 1 retx x 2 paths = 20 seconds) (30 sec watchdog timeout x 1 retry).

The second row displays the recommended configuration using the same Diameter defaults but providing a SCTP heartbeat timer that reduces heartbeat traffic.

Table 7: SCTP/Application Timer Configuration Values

SCTP Heartbeat Timeout	SCTP Path Max Retransmissions	Diameter Device Watchdog Timeout	Diameter Watchdog Request Max Retries
1-10 range	1	30 (default)	1 (default)
5	1	30 (default)	1 (default)

The following example configures the SCTP and application timers for the S6a SCTP interface supporting multi-homing:

```
configure
    sctp-param-template name
        sctp-max-path-retx value
        timeout sctp-heart-beat value
        exit
    context name
        diameter endpoint endpoint_name
            associate sctp-parameter-template template_name
            device-watchdog-request max-retries retry_count
            watchdog-timeout timeout
            end
```

Notes:

- When no SCTP parameter template is associated with the Diameter endpoint, the following default values are used:

  sctp-max-path-retx *10* (default in the parameter template is 5)

  timeout sctp-heart-beat *30* (default for the parameter template as well)

Configuring SCTP Multi-homing on the SGs Interface

Up to two IPv4 or IPv6 addresses for the SGs interface can be entered to allow for SCTP multi-homing.

Use the following example to configure SGs multi-homing between the MME and the MSC/VLR:

```
configure
    context mme_context_name -noconfirm
        interface s1-mme_intf_name
            ip address ipv4_address
```

```
        ip address secondary_ipv4_address
        exit
    sgs-service mme_svc_name
        bind ipv4-address ipv4_address ipv4-address secondary_ipv4_address
        exit
    exit
port ethernet slot_number/port_number
    no shutdown
    bind interface sgs_intf_name mme_context_name
    end
```

Notes:

- The SGs IP addresses can also be specified as IPv6 addresses using the **ipv6 address** keyword.
- The IP addresses in the **bind ipv4-address** command can also be specified as IPv6 addresses using the **ipv6-address** keyword.

SCTP Parameters for MME

The details on the configurable values for SCTP parameters are provided in the table given below:

Parameter	Minimum value	Maximum value	Granularity
RTO.min	10ms	5s	10ms
RTO.max	500ms	120s	10ms
RTO.initial	RTO.min	RTO.max	10ms
RTO.alpha	1/8	1/8	-
RTO.beta	1/4	1/4	-
Valid.Cookie.Life	5s	120s	1s
HB.interval	1s	300s	1s
SACK period	0ms	500ms	10ms
SACK frequency	1	5	1
MTU size	508 bytes	65535 bytes	1 byte

The details on the default values for SCTP parameters are provided in the table given below:

Parameter	Default value
RTO Alpha	5
RTO Beta	10

Parameter	Default value
Valid Cookie Life	600
Max. associate retransmission value	10
Max. number of outgoing streams	16
Max. number of incoming streams	16
Max. retransmission initiations	5
Max. MTU size	1500
Min. MTU size	508
Start MTU	1500
Max. path retransmission	5
RTO Initital	30
RTO Max	600
RTO Min	10
HB interval	30
HB enable	True
SACK period	2
SACK frequency	2
Bundle valid	True
Bundle enable	False

Configuring Static S-GW Pools

The MME supports static TAI list configuration which allows for the mapping of TAIs, TACs, and S-GWs to facilitate S-GW pooling for UEs moving between TAIs in their TAI lists.

Creating and Configuring a TAI Management Database and Object

This section provides configuration examples for creating and configuring the TAI/S-GW associations for S-GW pooling.

Use the following example to configure this feature on the MME:

```
configure
    lte-policy
        tai-mgmt-db db_name
            tai-mgmt-obj object_name
            tai mcc number mnc number tac value
            sgw-address ipv4_address s5-s8-protocol gtp weight number
            end
```

Notes:

- Up to four databases can be configured on the system.
- Up to 500 management objects can be configured per database.
- Up to 16 TAIs can be configured per management object.
- Up to 16 TACs can be configured per TAI.
- The **sgw-address** variable can also be specified as an IPv6 address.
- Up to 32 S-GW IP addresses can be configured per management object.
- Weights for IPv4 addresses are ignored if IPv6 addresses are present meaning only IPv6 addresses are load-balanced if present.
- The s5-s8-protocol can also be specified as **pmip** or **both** (GTP and PMIP).

Associating a TAI Management Database with an MME Service

In order for an MME service to use a statically configured S-GW pool, it must be associated with the TAI Management Database.

Use the following example to configure the TAI Management Database-to-MME service association:

```
configure
    context mme_context_name
        mme-service mme_svc_name
            associate tai-mgmt-db database_name
            end
```

Notes:

- Only one TAI Management Database can be configured per MME service.
- This association can also be performed in the Call Control Profile Configuration Mode supporting Operator Policy. If both associations are configured, the Operator Policy association is preferred by the system.

Associating a TAI Management Database with a Call Control Profile

MME service can access a statically configured S-GW pool through an Operator Policy instance, specifically through the Call Control Profile.

Use the following example to configure the TAI Management Database-to-MME service association:

```
configure
    call-control-profile name
```

```
    associate tai-mgmt-db database_name
    end
```

Notes:

- Only one TAI Management Database can be configured per Call Control Profile.
- This association can also be performed in the MME Service Configuration Mode. If both associations are configured, the Operator Policy association is preferred by the system.
- If the tai-mgmt-db is associated with a call-control-profile, and DNS is to be used for S-GW lookups, the DNS configuration must be configured within the same call-control-profile using the **dns-sgw** command within the call-control-profile configuration mode.

Configuring UMTS to LTE ID Mapping

UMTS networks are configured with LACs allocated from the reserved space of 32K to 64K. In LTE networks, this space is typically reserved for MME group IDs. To overcome this issue during inter-RAT handovers, the MME can be configured with mappings between LACs and MME group IDs.

Use the following configuration example to map PLMN IDs to MME group IDs:

```
configure
  lte-policy
    network-global-mme-id-mgmt-db
      plmn mcc mcc_value mnc mnc_value mme-group-id-range first id last id
      exit
    exit
  context mme_service_context
    mme-service service_name
      associate network-global-mme-id-mgmt-db
      end
```

Notes:

- Up to 32 mappings can be configured on the system.
- Overlapping ranges can be identified in the output of the **show configuration errors** command.

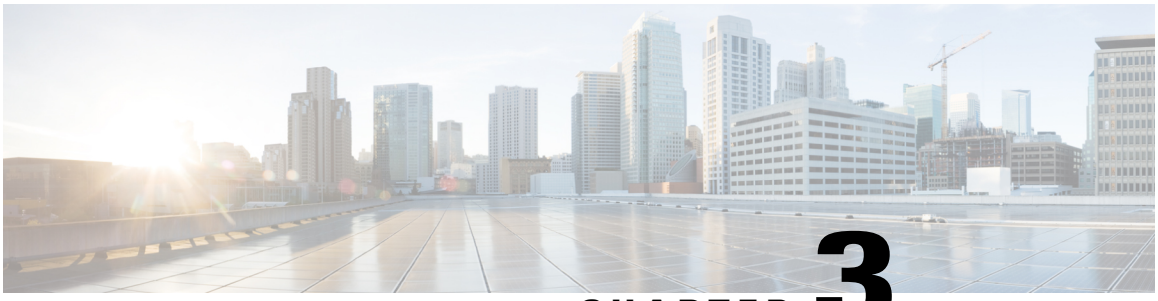
Configuring User Location Information Reporting Support

This feature allows the MME to query and receive UE location reports from an eNodeB.

Note User Location Information Reporting is a licensed feature and requires the purchase of the ULI Reporting feature license to enable it.

Use the following example to configure User Location Information (ULI) reporting support on the MME:

```
configure
  context mme_context_name
    mme-service mme_svc_name
      location-reporting
      end
```



CHAPTER 3

128K eNodeB Connections

The MME supports 128K eNodeB connections for VPC-DI and ASR5500-DPC2 platforms, previously only 64k eNodeB connections were supported.

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. In previous releases multiple SCTP connections from a VLR were hosted on the same MME manager. 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.

Configuring Rate Limit for S1 SCTP Connections from eNodeB

The **task facility mmedemux** command is updated to include option to configure a rate limit for incoming S1 SCTP connections in MME per chassis.

configure
task facility mmedemux { mmemgr-startup-percentage *percent_value* **[mmemgr-startup-wait-time** *wait_time* **] | s1-sctp rate-limit** *value* **}**
default task facility mmedemux mmemgr-startup-percentage mmemgr-startup-wait-time
no task facility mmedemux { mmemgr-startup-percentage mmemgr-startup-wait-time | s1-sctp rate-limit}
exit

- By default rate limiting is not imposed on incoming SCTP connections at the MME. Configuring the rate limit is an optional configuration, to prevent overload of MME from surge/burst of S1 SCTP connections from eNodeBs.
- The keyword **s1-sctp** identifies the MME SCTP interface type.
- The keyword **rate-limit** is used to configure the rate limit for incoming S1 SCTP connections from eNodeB. The value of the rate limit that can be configured is an integer from 1 up to 65535. Once the rate of incoming S1 SCTP connections exceed the configured value, the SCTP cookie echo packets are dropped by the MME on exceeding the rate limit. The SCTP connection with eNodeB is eventually be established after retries/retransmission by the eNodeB. The statistics of the dropped S1 SCTP packets are collected and displayed as part of MME Demux subsystem statistics.

Example:

The following CLI command configures rate-limit of 100 S1 SCTP connections per second for a chassis:

task facility mmedemux s1-sctp rate-limit 100

Verifying the Configuration

The configuration of this feature can be verified using the following show commands. Execute the **show configuration** command to verify the configuration, the output displays the following parameters based on the configuration:

- **task facility mmedemux s1-sctp rate-limit** *value*

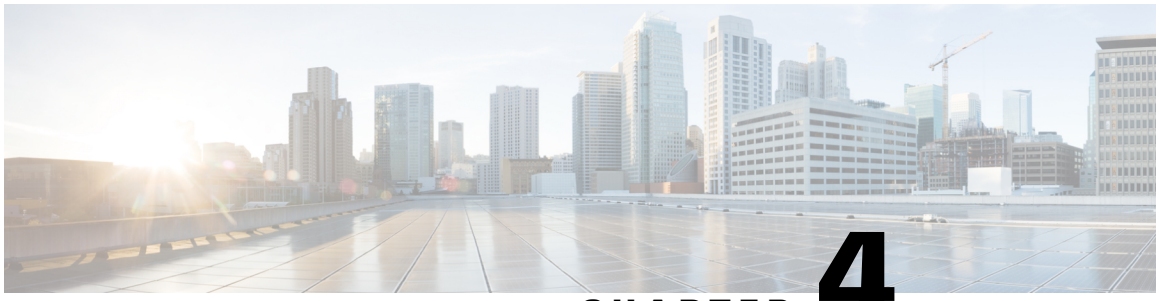
Monitoring and Troubleshooting

This section provides information on the show commands available to support this feature.

Show Command(s) and/or Outputs

The following parameter is added to the output generated by the **show session subsystem facility mmedemux all** command to display statistics for this feature.

- **Total number of S1 sctp packets dropped (rate-limit)** - This counter displays the number of SCTP packets dropped due to the configured rate limit for incoming S1 SCTP connections to the MME on a per chassis basis.



CHAPTER 4

A-MSISDN Functionality

It is possible to configure the MME to support the Additional Mobile Subscriber ISDN (A-MSISDN) flag in the Features List AVP of the Update Location Request (ULR) messages.

This chapter looks at the MME's A-MSISDN functionality.

Feature Description

The MME includes the Additional Mobile Subscriber ISDN (A-MSISDN) flag in the Features List AVP of the Update Location Request (ULR) messages that are sent over the S6a interface to the Home Subscriber Server (HSS) at the time a UE Attaches. In response, if an A-MSISDN is available then the HSS sends a provisioned A-MSISDN and an MSISDN in the Subscription Data AVP in Update Location Answer (ULA) and IDR messages.

How It Works

When A-MSISDN is configured to enable this functionality, then the MME will advertise support for A-MSISDN in S6a ULR messages by setting bit 31 in the Feature List Id 1 AVP. Upon receiving s6a ULA/IDR messages from the HSS, the MME will

- store received A-MSISDN value from the Subscription Data AVP in the UE context.
- use A-MSISDN as C-MSISDN in "SRVCC PS to CS Request" and "Forward Relocation Request" messages.
- store received C-MSISDN as A-MSISDN in the UE context.

Support for A-MSISDN functionality enables the MME to use the A-MSISDN as a Correlation MSISDN (C-MSISDN) during SRVCC PS-to-CS handovers. For information on the purpose of the C-MSISDN, refer to 3GPP TS 23.003.

If the MME sends an A-MSISDN flag in the ULR, then the MME

- can receive only one or both MSISDN and A-MSISDN in ULA/IDR messages.
- can send MSISDN or A-MSISDN as C-MSISDN.

The MME's A-MSISDN functionality is applicable for ULR/ULA, IDR/IDA, and DSR/DSA command pairs sent over S6a interface.

The MME also supports the A-MSISDN withdrawal bit received in DSR Flags AVP. Receipt of this bit triggers the MME to delete an A-MSISDN from the UE context.

Limitations

A-MSISDN support is not present for the S6d interface. This means that A-MSISDN will not be available to the MME when SGSN/MME-combo optimization is enabled and subscription data received by the SGSN is re-used by the MME.

Location services using A-MSISDN are not supported (PLR/LRR).

Lawful Intercept (LI) and Monitor Subscriber functions based on A-MSISDN as the identifier are not supported.

Standards Compliance

The MME's support of A-MSISDN complies with 3GPP 29.274 v11.10.0.

Configuring A-MSISDN Functionality

Enabling A-MSISDN is a two step process:

- First, configure A-MSISDN support on the MME.
- Second, configure the MME to support 3GPP Release 11 AVPs.

Both configuration steps are described below and both must be completed to fully enable A-MSISDN functionality.

Configuring A-MSISDN Support

By default, A-MSISDN is not supported. Use the following configuration sequence to enable the MME to support A-MSISDN functionality and to advertise that support to the HSS.

configure
call-control-profile *profile_name*
a-msisdn
remove a-msisdn
end

Notes:

- **a-msisdn** Enables the MME to notify the HSS of support for Additional-MSISDN for the PLMN associated with this call-control profile.

- **remove** Disables support for A-MSISDN functionality and returns the MME to default state.
- Configure the 3GPP R11 support with the **diameter update-dictionary-avps** command in the HSS Peer Service configuration mode to complete the configuration required to support A-MSISDN.

Verifying the A-MSISDN Support Configuration

Use the output generated by the **show call-control-profile full all** command to verify the configuration status of the A-MSISDN functionality:

```
Call Control Profile Name = cp1
  SAMOG Web-Authorization Mutiple Device Support : NO
  ...
    Super Charger                              : Disabled
    P-CSCF Restoration                         : Enabled
    A-MSISDN                                   : Enabled
    Sending Radio Access Technology (RAT) IE   : Enabled
```

Configuring 3GPP Release 11 AVP Support

The following configuration sequence enables the MME to support AVPs available in Release 11 3GPP 29.272.

configure
context *context_name*
hss-peer-service *service_name*
diameter update-dictionary-avps { 3gpp-r10 | 3gpp-r11 | 3gpp-r9 }
no diameter update-dictionary-avps
end

Notes:

- **3gpp-r11** Configures the MME to support signaling additional AVPs to an HSS in support of Release 11 of 3GPP 29.272. Using this keyword is necessary to enable the MME to fully support inclusion of the Additional Mobile Station ISDN (A-MSISDN) flag of the Feature List AVP in Update Location Request (ULR) messages sent over the S6a interface to the HSS at the time a UE Attaches.
- **no** Sets the command to the default value where Release 8 (standard) dictionary is used for backward compatibility of previous releases.

Monitoring and Troubleshooting the A-MSISDN Functionality

Show Command(s) and/or Outputs

The show commands in this section are available in support of the MME's A-MSISDN functionality.

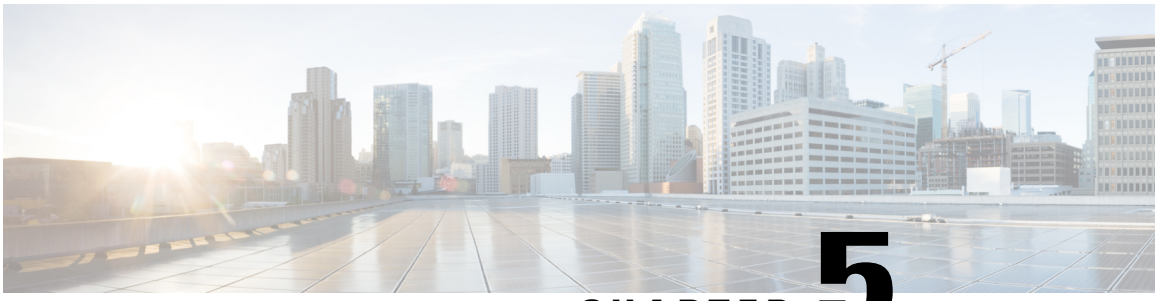
show mme-service session full all

The A-MSISDN field in the generated output indicates an A-MSISDN value if the A-MSISDN is received from the HSS. If no value is received from the HSS, then the value displayed will be **n/a**.

```
[local]asr5000 show mme-service session full all
  SessMgr Instance: 1          ImsiMgr Instance: 1
  MSID: 123456789012345         Callid: 00004e21
  MME Service: mmesvc
  MME HSS Service: mme1
  SGTPC Service: sgtp1
  EGTP S11 Service: egtp_mme
  MME S1 Address: 192.80.80.2
  EGTP S11 Address: 192.80.80.16
  ME Identity: n/a   GUTI: 123:456:32777:2:3221225473
  MSISDN: 888012345679001
  A-MSISDN : 988012345679002
```

The following show commands will also generate outputs that display the A-MSISDN value if it has been received from the HSS. If nothing is received, then the value will be **n/a**:

- show mme-service db record call-id *call-id*
- show mme-service db record imsi *imsi*
- show mme-service db record guti plmn *plmn* group-id *group-id* code *code* m-tmsi *m-tmsi*



CHAPTER 5

Access Restriction based on Regional Zone Code

This chapter describes access restrictions based on regional zone codes, which are configured under a TAI-Object.

Feature Description

Zone codes are used to identify the group of Tracking Area Identities (mcc-mnc-tac), and to further restrict or allow services under those TAI, based on Call Control and/or Operator policies. The scope of zone code is defined as a set of TAIs. This is configurable under LTE TAI Management Object.

Until release 21.0, only one zone code value was configurable under each TAI-Object. Due to this limitation, configuring and managing different access restrictions per TAI-Object separately for each PLMN required a complex configuration or a separate TAI-DB for each PLMN.

To overcome this limitation, in release 21.1, this feature is modified to configure multiple zone code values under the same TAI-Object. It allows specific zone codes to be managed based on call-control-profile / HSS (per roaming partner). Also, this feature supports overlapping of zones by allowing multiple zone code values to which a TAI-Object belongs.

How It Works

Regional Zone Code Identity

A PLMN-specific regional subscription unambiguously defines the region in which roaming is allowed, for the entire PLMN. It consists of one or more regional subscription zones. The regional subscription zone is identified by a Regional Subscription Zone Identity (RSZI).

The RSZI elements are defined below:

- Country Code (CC): This defines the country in which the PLMN is located.

- National Destination Code (NDC): Identifies the PLMN in that country.
- Zone Code (ZC) identifies a regional subscription zone as a pattern of "allowed" and "not allowed" location areas uniquely within that PLMN. ZC has a fixed length of two octets and is coded in full hexadecimal representation.

RSZIs, including ZCs, are assigned by the VPLMN operator.

Information Storage

If a mobile subscriber has a regional subscription, the HSS stores a list - up to 10 Regional Subscription Zone Identities (RSZIs), for each PLMN involved. This is sufficient to store the Zone Code List per CC NDC. On updating the MME, HSS identifies the VPLMN and NDC given by the MME and transfers the corresponding Zone Code List to the MME. The UE is allowed access to all zone codes provided in the subscription data received from the HSS. The Zone Code List maintained by the MME, consists of Zone Codes without CC and NDC.

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 attach/connect only in those zones. Support for Regional Zone Code restriction based on HSS subscription data allows operators to offer zone based EPC subscriptions to home subscribers.

Note Regional subscription zone codes are populated only when HSS returns the zone codes configured in the subscription profile (as shown below). HSS returned zone codes are only configured as Allowed, not as Restricted.

```
Subscription Profile
  Regional Subscription Zone Codes
    Zone Code: 1
    Zone Code: 12
    Zone Code: 234
    Zone Code: 4567
    Zone Code: 890
```

- 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.
- Call-Control-Profile based restriction:
  - In the call-control-profile, the operator can configure zone codes as a list of allowed zone codes for a TAI-list.

    ```
    config
    call-control-profile ccp
    lte-zone-code allow zone-code-list 100 147 170
    ```

    If the "allow" zone code configured in the call-control-profile matches with a zone code from the TAI-Object list, the operation succeeds, else fails.

- In the call-control-profile, the operator can configure zone codes as a list of restricted zone codes for a TAI-list.

```
config
call-control-profile ccp
lte-zone-code restrict zone-code-list 100 147 170
```

If the “restrict” zone codes configured under Call Control Profile matches with any one zone code from TAI-Object then the zone code validation fails, else it succeeds.

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

When zone code validation fails (either with HSS or call-control-profile), the EMM Cause Code to be sent in the reject message can be configured in the call-control-profile.

- On failure, if no EMM Cause Codes is configured, the default EMM Cause Code is sent in reject message is #13, 'roaming-not-allowed-in-this-tracking-area' for roaming subscribers and #12, 'tracking-area-not-allowed' for home subscribers.
- The other EMM Cause Codes are: 'no-suitable-cell-in-tracking-area', 'eps-service-not-allowed-in-this-plmn', and 'plmn-not-allowed'.
- When a UE is rejected either because the zone code was not in the allowed list or because it was not in the restricted list, the above mentioned EMM Cause Codes can be configured.

Use the following CLI commands to configure EMM Cause Codes during a zone code validation failure:

config
call-control-profile *profile_name*
local-cause-code-mapping restricted-zone-code emm-cause-code [eps-service-not-allowed-in-this-plmn | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed]
[remove] local-cause-code-mapping restricted-zone-code
end

Notes:

- The **local-cause-code-mapping restricted-zone-code** command configures the reject cause code to send to a UE when a UE requests access to a restricted zone.
- The **emm-cause-code** command specifies the EPS Mobility Management (EMM) cause code to return when a UE requests access to a restricted zone. The emm-cause-code value must be one of the following options:
  - eps-service-not-allowed-in-this-plmn
  - no-suitable-cell-in-tracking-area - Default.
  - plmn-not-allowed
  - roaming-not-allowed-in-this-tracking-area
  - tracking-area-not-allowed
- The **remove local-cause-code-mapping restricted-zone-code** command removes the configured cause code mapping.

Standards Compliance

The Access Restrictions based on Regional Zone Codes feature complies with the following standards:

- 3GPP TS 24.301 V9.5.0 (2010-12), 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3 (Release 9)
- 3GPP TS 29.272 V9.5.0 (2010-12), 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 9)
- 3GPP TS 29.274 V9.4.0 (2010-09), 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 (Release 9)
- 3GPP TS 29.002 V9.4.0 (2010-09), 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; 3GPP Evolved Packet System (EPS); Mobile Application Part (MAP); (Release 9)
- 3GPP TS 23.008 V9.4.0 (2010-09), 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; 3GPP Evolved Packet System (EPS); Organization of Subscription Data; (Release 9)
- 3GPP TS 23.003 V9.4.0 (2010-09), 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; 3GPP Evolved Packet System (EPS); Numbering, Addressing and Identification; (Release 9)

Limitations

The Access Restriction based on Regional Zone Code feature have the following limitations:

- If an ISDR is received from the HSS for an attached subscriber, the MME does not detach the subscriber, rejects the next TAU request.
- If both call control policy based restrictions and HSS subscription based zone code restrictions are present during a call, only HSS based restrictions will be processed. For a zone code in a HSS accept list, the call will be progressed, and for a zone code that is not in the HSS accept list, the message will be rejected, regardless of any call control profile being active for the call.
- Changes to zone code mapping or call control profile mapping will not detach the currently attached subscribers. The call control profile changes, and also, the changes to mapping of TAI to Zone codes affects the processing of any incoming messages after the change.

Note This feature should be configured with either a HSS provided zone-code policy or a locally configured zone-code policy, but not together. If both are configured, the MME selects the HSS provided zone-code policy leading to an unexpected behavior.

Configuring Access Restriction based on Regional Zone Code

In release 21.1, the CLI command to configure zone code under a TAI-Object is extended to configure multiple zone code values under the same TAI-Object. A maximum of 10 zone codes is configurable under each TAI-Object.

During the configuration, the operator should be mindful of the following:

- Zone codes can be configured as single zone code per configuration line or multiple zone codes per configuration line. It is recommended to enter multiple zone codes per configuration line to reduce the configuration load time.
- Duplicate zone codes are not allowed under the same TAI-Object. However, duplicate zone code can be configured in a different TAI-Object.
- If multiple zone codes are entered in a single line configuration - duplicate zone codes and unique zone codes, only the duplicate zone codes will be rejected whereas the unique zone codes are accepted.
- If number of zone codes entered in single configuration line is greater than 10, then only 10 minus the initial configured zone codes will be accepted and configured.
- During the configuration, if all the 10 slots are configured, the extra configured zone code values are rejected with a suitable error.
- If the zone codes are configured when the subscribers are already attached, the currently attached subscribers are not detached. Changes to the mapping of TAI to Zone codes affect the processing of any incoming messages. So, if the mapping of TAI to zone codes is changed after an initial attach, the next TAU message zone code validation with a HSS/call-control-profile is processed with the newly updated zone code configuration. The initial attach message for new subscribers uses the updated zone code configuration.

  The session manager instance, as displayed in the log, must be reloaded to push the correct configuration to the respective session manager after session manager recovery. This will ensure that the configuration in the session manager and the SCT are in sync.

Use the following CLI commands to enable Access Restriction based on Regional Zone Codes:

```
configure
  lte-policy
    tai-mgmt-db database_name
      tai-mgmt-obj object_name
        [ no ] zone-code zonecode_value  [ zonecode_value2 [...[ zonecode_value10 ] ] ]
       end
```

Notes:

- The **zone-code** command configures zone code values under a TAI object. In release 21.1, the number of zone codes values configurable in a single line configuration is extended to 10 values under a TAI-list. For example, **zone-code 10 11 12 13 14 15 16 17 18 19**
- By default, the **zone-code** command is not enabled.
- The **no zone-code** <*zonecode_value2*>…<*zonecode_value10*>, removes the selected zone code values entered from the TAI-list. For example, in the following configuration: **no zone-code 10 11 12**, only the zone code value 10 11 12 is removed from the existing TAI-list, whereas the other zone code values remain configured in the TAI-list.

Example Configuration

The following is an example configuration to allow access to TAIs for PLMN with a specific value of mcc/mnc, and a configuration to restrict access to specific TAI values for a different PLMN.

```
config
   operator-policy name Partner-1-policy
      associate call-control-profile CCP1
   #exit
   operator-policy name Partner-2-policy
      associate call-control-profile CCP2
   #exit
   lte-policy
      subscriber-map sm1
         precedence 100 match-criteria imsi mcc 111 mnc 222 operator-policy-name
Partner-1-policy
         precedence 101 match-criteria imsi mcc 111 mnc 333 operator-policy-name
Partner-2-policy
      exit
      tai-mgmt-db TMD
         tai-mgmt-obj OBJ1
            zone-code 11 21
            tai mcc 123 mnc 456 tac 1234
            tai mcc 123 mnc 456 tac 1235
            tai mcc 123 mnc 456 tac 1236
            tai mcc 123 mnc 456 tac 1237
         #exit
         tai-mgmt-obj OBJ2
            zone-code 12
            tai mcc 123 mnc 456 tac 2234
            tai mcc 123 mnc 456 tac 2235
            tai mcc 123 mnc 456 tac 2236
         #exit
         tai-mgmt-obj OBJ3
            zone-code 13 22
            tai mcc 321 mnc 456 tac 1244
            tai mcc 321 mnc 456 tac 1245
            tai mcc 321 mnc 456 tac 1248
            tai mcc 321 mnc 456 tac 1249
         #exit
         tai-mgmt-obj OBJ4
            zone-code 23
            tai mcc 321 mnc 456 tac 2244
            tai mcc 321 mnc 456 tac 2245
            tai mcc 321 mnc 456 tac 2247
            tai mcc 321 mnc 456 tac 2248
         #exit
      #exit
   #exit
   call-control-profile CCP1
      lte-zone-code allow zone-code-list 11 12 13
      associate tai-mgmt-db TMD
   #exit
   call-control-profile CCP2
      lte-zone-code restrict zone-code-list 21 22 23
      associate tai-mgmt-db TMD
   #exit
end
```

Configuration Description

In the above configurations, UEs are mapped to separate zone code numbers. Each zone code can be associated to TAIs independent of each other.

From the example above, for “allow” access:

UEs from PLMN – with mcc = 111 and mnc = 222, operator policy = Partner-1-policy and call-control-profile = CCP1 applies. With reference to CCP1, zone codes 11, 12 and 13 are allowed from the associated tai-mgmt-db

= TMD. UEs from this PLMN will be allowed with access to TAI values in tai-mgmt-obj = OBJ1, OBJ3 and OBJ2 (For example, **tai mcc 123 mnc 456 tac 1234**).

From the above example, for "restrict" access:

UEs from PLMN – with mcc = 111 and mnc = 333, operator policy = Partner-2-policy and call-control-profile = CCP2 applies. With reference to CCP2, zone codes 11, 12 and 13 are restricted from the associated tai-mgmt-db = TMD. UEs from this PLMN will be restricted from access to TAI values in tai-mgmt-obj = OBJ1, OBJ3 and OBJ2 (For example, **tai mcc 123 mnc 456 tac 1234**).

Verifying Access Restriction based on Regional Zone Codes

Use the following command to verify Access Restriction based on Regional Zone Codes configuration on the MME.

show lte-policy tai-mgmt-db name *database_name*

```
TAI Management DB: db_test
   TAI Management Object: obj_test
      Zone Code: 103 104 105 106 107 108 109
```

Notes:

- **TAI Management DB:** Denotes the name of the database object.
- **TAI Management Object:** Identifies the TAI-Object list where the zone codes are configured.
- **Zone Code:** Displays the configured zone code values under a specified TAI-Object.

Monitoring and Troubleshooting Access Restriction based on Regional Zone Codes

This section provides information on how to monitor Access Restriction based on Regional Zone Codes.

Show Command(s) and/or Outputs

This section provides information regarding show commands and/or their outputs in support of Access Restriction based on Regional Zone Codes feature.

show mme-service statistics

On running this command, the following fields are displayed for this feature:

- Roaming restricted TA
- PLMN Not allowed
- TA not allowed
- No suitable cells in TA
- No EPS Service in PLMN

Field	Description
Roaming restricted TA	The total number of EMM Attach Reject messages sent with the cause code #13: "Roaming restricted in TA".
PLMN Not allowed	The total number of EMM Attach Reject messages sent with the cause code #11: "PLMN not allowed".
TA not allowed	The total number of EMM Attach Reject messages sent with the cause code 12: "Tracking Area not allowed".
No suitable cells in TA	The total number of EMM Attach Reject messages sent with the cause code #15: "No suitable cells in TA".
No EPS Service in PLMN	The total number of EMM Attach Reject messages sent with the cause code #14: "EPS service not allowed in this plmn".

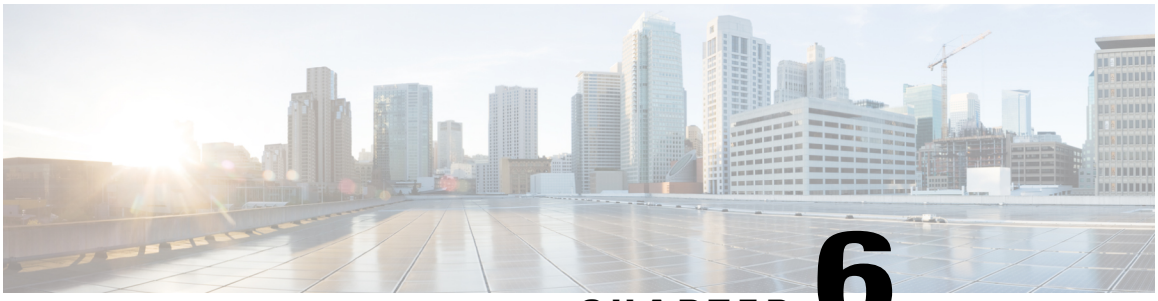
show mme-service db record imsi *imsi_value*

On running this command, zone codes allowed for a particular UE are displayed. The following field is displayed for this feature:

- Regional Subscription Zone Codes

Field	Description
Regional Subscription Zone Codes	This field displays all the Zone Code values (up to 10 zone code values), returned by the HSS in the Update Location Answer message or Insert Subscriber Data message for a UE, based on the values configured in its subscription profile.

Note If zone code restriction is applied under the call-control-profile, then the Regional Subscription Zone Codes field will not be captured in any of the show CLI output.



CHAPTER 6

APN Override

Access Point Name (APN) Override is a set of features which enable the operator to override the APN requested by the UE. The functionality to provide configurable remapping provides the operator flexible options with APN handling locally rather than requiring changes in the external systems.

Feature Description

In many situations the APN provided in the Activation Request is unacceptable. Either it does not match any of the subscribed APNs or could be misspelled, resulting in the SGSN/MME rejecting the Activation Request. The APN Override feature enables the operator to override an incoming APN specified by a subscriber or provided during the APN selection procedure.

There are three methods of performing apn-overriding.

- Network Identifier (NI) based overriding
- Operator Identifier (OI) based overriding
- Charging-characteristic based overriding

A valid license key is required to enable APN Override. Contact your Cisco Account or Support representative for information on how to obtain a license.

MME sends remapped APN to the UE in the ATTACH_ACCEPT or ACTIVATE_DEFAULT_BEARER_REQ messages when APN Remapping feature is enabled. In release 19.5, this behavior is modified so that MME can control to send either the UE requested APN or remapped APN in these messages. This behavior is controlled through adding a new optional keyword **orig-apn** in the existing **apn-remap** CLI command in the APN Remap Table configuration mode.

Additional configuration control is provided at the MME service level to reject or accept UE sessions with APN containing non-3GPP standard characters. The following are considered as standard 3GPP characters:

- A - Z, a - z (alphabets)
- 0 – 9 (numeric)
- - (hyphen)
- * (asterisk)
- . (period)

All other characters are considered as non-3GPP standard.

New CLI configuration is also introduced in the APN Remap Table configuration mode to allow remapping of APNs with non-3GPP characters.

How it Works

The following sections describe the three methods for overriding a UE requested APN. These options enable the operator to overwrite incorrect APNs or apply an APN when not provisioned for the subscriber in the HLR.

Network Identifier (NI) Overriding

Network Identifier (NI) Overriding is done before validating the UE requested APN with HSS subscriber data.

Operator Identifier (OI) Overriding

Operator Identifier (OI) Overriding is done after Network Identifier is validated against HSS subscriber data. After the FQDN is constructed for DNS query, OI overriding is applied on the constructed FQDN to form a new FQDN based on OI remapping.

Charging Characteristics Overriding

Charging characteristics based overriding is performed if the apn-charging-characteristic/subscriber-charging-characteristic from the HSS matches the configured APN and charging-characteristic in the remap entry.

Configuring APN Override

Configuration for all of the functions of the APN Override feature is accomplished in the APN Remap Table configuration mode of the Operator Policy Feature. In order to enable apn-overriding, an apn-remap-table must be configured and associated to the mme-service through the operator-policy.

Before You Begin

APN Override is configured with the commands in the APN Remap Table configuration mode. This mode generates a table that is a key component of the Operator Policy feature and the table is not valid unless it is associated with an operator policy.

Before entering the APN Remap Table configuration mode to configure specific APN override settings, you must first create and associate the various related objects as follows:

Step 1 Create an APN Remap Table instance from the Global configuration mode.

Step 2 Associate the APN Remap Table with an operator policy in the Operator Policy configuration mode.

Step 3 Define which subscribers should have this operator policy applied.
Refer to the following example to complete these steps.

```
configure
    apn-remap-table table_name -noconfirm
        exit
    operator-policy name policy_name -noconfirm
        associate apn-remap-table table_name
        exit
    lte-policy
        subscriber-map map_name -noconfirm
            precedence 1 match-criteria all operator-policy-name policy_name
            exit
        exit
    context ingress -noconfirm
        mme-service srvc_name -noconfirm
            associate subscriber-map map_name
            end
```

Configuring Network Identifier Override

Network Identifier (NI) Overriding is done before validating the UE requested APN with HSS subscriber data.

```
configure
  apn-remap-table table_name
    apn-remap network-identifier company.com new-ni internet.com
    end
```

Notes:

- The **apn-remap** command above remaps the UE requested APN "company.com" to "internet.com".
- Wildcards characters (*) can be used in the existing network identifier.

Configuring Operator Identifier Override

Operator Identifier (OI) Overriding is done after Network Identifier is validated against HSS subscriber data. After the FQDN is constructed for the DNS query, Operator Identifier overriding is applied on the constructed FQDN to construct the new FQDN based on OI remapping.

configure
  apn-remap-table *table_name*
    apn-remap operator-identifier *mnc456.mcc123.gprs* **new-oi** *mnc987.mcc654.gprs*
    apn-remap operator-identifier *mnc456.mcc123.gprs* **value-for-oi-mcc** *543* **value-for-oi-mnc** *234*
    end

Notes:

- The first **apn-remap** command above remaps "company.com.apn.epc.mnc456.mcc123.3gppnetwork.org" to "starent.com.apn.epc.mnc987.mcc654.3gppnetwork.org".
- The second **apn-remap** command above remaps "starent.com.apn.epc.mnc456.mcc123.3gppnetwork.org" to "starent.com.apn.epc.mnc234.mcc543.3gppnetwork.org".
- Wildcards characters (*) can be used in the existing operator identifier.

Configuring Charging Characteristics Override

If the UE-requested APN and apn-charging-characteristic or subscriber-charging-characteristic information returned from the HSS matches the locally configured APN and charging-characteristic details in the remap entry, then it is overridden with the configured target-ni.

configure
  apn-remap-table *table_name*
    cc behavior *0x785* **profile** *6* **apn-remap network-identifier** *company.com* **new-ni** *internet.com*
    end

Notes:

- The above command remaps "company.com" to "internet.com" if the configured charging-characteristic matches the apn-charging-characteristic or subscriber-charging-characteristic in the HSS. Also, the PDN-type must match.

Enabling MME to Send UE Requested APN

Use the following configuration commands to configure MME to send the UE requested APN in ATTACH_ACCEPT or ACTIVATE_DEFAULT_BEARER_REQ message.

configure
  apn-remap-table *table_name*
    apn-remap network-identifier *company.com* **new-ni** *internet.com* **[orig-apn]**
   cc behavior *0xff* **profile** *10* **apn-remap network-identifier** *company.com* **new-ni** *internet.com* **[orig-apn]**
    apn-selection-default lowest-context-id [orig-apn]
    apn-selection-default first-in-subscription [orig-apn]
    apn-selection-default network-identifier require-dns-fail-wildcard [orig-apn]
    end

Notes:

- **orig-apn**: This is an optional keyword newly added to the existing CLI commands to enable MME to send UE requested APN to the UE. If this optional keyword is not configured, then MME continues with its default behavior of sending the remapped APN to the UE.
- For more information on the existing CLI commands, see the *Command Line Interface Reference* guide.

Rejecting UE Requested APN with Non-standard Characters

Use the following configuration commands to configure MME to reject UE sessions containing non 3GPP standard characters in the APN.

configure
context *context_name*
mme-service *service_name*
[default] policy attach reject-non3gpp-char-apn
[default] policy pdn-connect reject-non3gpp-char-apn
end

Notes:

- **policy attach reject-non3gpp-char-apn**: This command enables MME to immediately reject the attach procedure without any APN remapping, if the UE requested APN contains non 3GPP characters. The attach procedure is rejected with ESM cause-code #27 "missing or unknown APN" and T3396 value IE is included in the Attach reject message.
- **policy pdn-connect reject-non3gpp-char-apn**: This command enables MME to immediately reject the PDN connect procedure without any APN remapping, if the UE requested APN contains non 3GPP characters. The PDN connect procedure is rejected with ESM cause-code #27 "missing or unknown APN" and T3396 value IE is included in the PDN connect reject message.
- For more information on the existing CLI commands, see the *Command Line Interface Reference* guide.

Remapping UE Requested APN with Non-standard Characters

Use the following configuration commands to configure MME to remap UE requested non 3GPP character APN to an operator defined APN.

configure
apn-remap-table *table_name*
apn-remap non3gpp-char-apn new-ni *new-ni-name* **[orig-apn]**
end

Notes:

- **apn-remap non3gpp-char-apn new-ni** *new-ni-name*: This command enables MME to remap all UE requested APNs containing non 3GPP characters to the configured new-ni APN. If the optional keyword “orig-apn” is configured, then MME sends the UE requested APN in ATTACH_ACCEPT or ACTIVATE_DEFAULT_BEARER_REQ message. If this keyword is not configured, then remapped APN is sent back to UE.
- This CLI is applied only if the UE sessions are not rejected by the new configuration options **policy attach reject-non3gpp-char-apn** and **policy pdn-connect reject-non3gpp-char-apn** under the mme-service.

- If the UE requested APN contains non-3GPP characters and the **apn-remap non3gpp-char-apn new-ni** *new-ni-name* CLI command is configured, then this CLI takes precedence over any other matching criterion for APN remapping.
- For more information on the existing CLI commands, see the *Command Line Interface Reference* guide.

Verifying the APN Override Configuration

The following command shows the override settings configured for the specified APN remap table.

show apn-remap-table full name *table_name*

```
[local]asr5x00 show apn-remap-table full name           table1
Charging Characteristic APN Override Entry1
      Match Charging Characteristics Behavior           : 0x785
      Match Charging Characteristics Profile-Index      : 6
      Match Requested APN                               : company.com
      APN to use for Overriding                         : internet.com
APN remap Entry1 :
      Match Input OI wildcard             :mnc456.mcc123.gprs
      Remap Input OI to                   :mnc987.mcc654.gprs
APN remap Entry2 :
      Match Input NI wildcard             :company.com
      Remap Input NI to                   :internet1.com
```

Monitoring and Troubleshooting the APN Override Feature

This section provides information regarding show commands and/or their outputs in support of this feature.

The following operations should be performed for any failure related to this feature:

- Verify if the feature is enabled using **show configuration** and **show mme-service all** CLI commands. If not enabled, configure the CLI commands mentioned in the *Enabling MME to Send UE Requested APN* and *Rejecting UE Requested APN with Non-standard Characters* sections and check if it works.
- Collect the output of **show mme-service statistics debug** command and analyze the debug statistics "Rejected Attach due to non3gpp char APN" and "Rejected PDN Connect due to non3gpp char APN". For further analysis, contact your Cisco account representative.

show configuration

The output of this show command is enhanced to indicate whether MME sends back UE requested APN in ATTACH_ACCEPT or ACTIVATE_DEFAULT_BEARER_REQ message.

The following is a sample output of this show command indicating that this feature is enabled.

```
[local]asr5000# show configuration
config
... ... ...
no session trace network-element saegw
  apn-remap-table abc
  apn-remap non3gpp-char-apn new-ni mappedAPn orig-apn
  apn-remap network-identifier origApn new-ni mappedApn orig-apn
  #exit
  port bits 24/4
    snmp trap link-status
... ... ...
      no heuristic-paging
```

```
      no isr-capability
      policy attach set-ue-time disable
   policy attach reject-non3gpp-char-apn
   policy pdn-connect reject-non3gpp-char-apn
      policy tau set-ue-time disable
... ... ...
... ... ...
end
```

show mme-service all

The output of this show command is enhanced to indicate whether MME rejects APNs with non-standard characters in Attach Request or PDN Connect Request message. The following fields are added in support of this feature.

- Reject attach with non-3GPP char APN
- Reject pdn connect with non-3GPP char APN

The following is a sample output of this show command with the new field included.

```
show mme-service all
Policy for Idle Mode Detach          : Explicit
NAS Max Retransmissions Count        : 4
Set UE Time (attach processing)      : Disabled
Reject attach with non-3GPP char APN : Disabled
Reject pdn connect with non-3GPP char APN : Disabled
IMEI Query (attach processing)       : None
EIR Query (attach processing)        : Disabled
```

show mme-service session full { all | imsi | mme-service }

The output of this show command is enhanced to display the name of UE requested APN with non-standard character in hexadecimal format, and with all standard characters in normal string format. The following field is added in support of this feature.

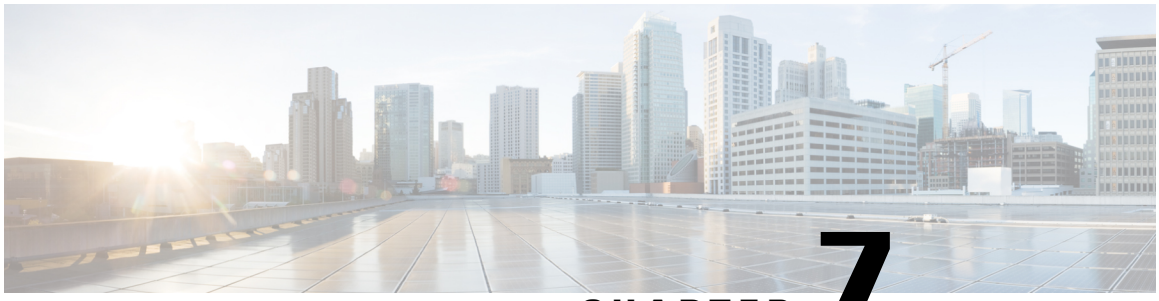
- UE Requested APN

The following is a sample output of this show command with the new field included.

```
show mme-service session full all
PDN Information:
   APN Name: starent.com
   UE Requested APN: starent-ueside.com
APN Restriction: 1
PDN Type: IPv4
```

Important The UE requested APN information will not be available for UE after the session recovery as it will not be check pointed.

show mme-service session full { all | imsi | mme-service }



CHAPTER 7

Backup and Recovery of Key KPI Statistics

The Backup and Recovery of Key KPI Statistics feature allows the MME to back up a small set of KPI counters for recovery of the counter values after a session manager (SessMgr) crash.

Feature Description

Before the Backup and Recovery of Key KPI Statistics feature was implemented, statistics were not backed up and could not be recovered after a SessMgr task restart. Due to this limitation, monitoring the KPI was a problem as the MME would loose statistical information whenever task restarts occurred.

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 - they are reset to zero. So, the KPI calculation in the next interval will result in negative values for that interval. This results in a dip in the graphs plotted using the KPI values, making it difficult for operations team to get a consistent view of the network performance to determine if there is a genuine issue or not.

This feature makes it possible to perform reliable KPI calculations even if a SessMgr crash occurs.

How It Works

A key set of counters, used in KPI computation will be backed up for recovery if a SessMgr task restarts. The counters that will be backed up are determined by the KPIs typically used in several operator networks.

The backup of counters is enabled or disabled via configuration. The configuration specifies the product for which counters will be backed up and also a time interval for the back up of the counters.

The backed up counters can be identified via CLI generated displays or via display of the MME-specific backup statistics schema: mme-bk. The operator can use this schema to compute the KPI as statistics will

have the recovered counters. During the display and the backup processes, both the normal counters and backed-up counters are cumulatively displayed or backed up.

mme-bk schema - This schema comprises a superset of key MME counters maintained by the SessMgr and are backed up. The counters in this schema are pegged per MME service. Each line of output is per MME service. Additionally, there will be one set of consolidated counters for all MME services which is displayed with the MME service name.

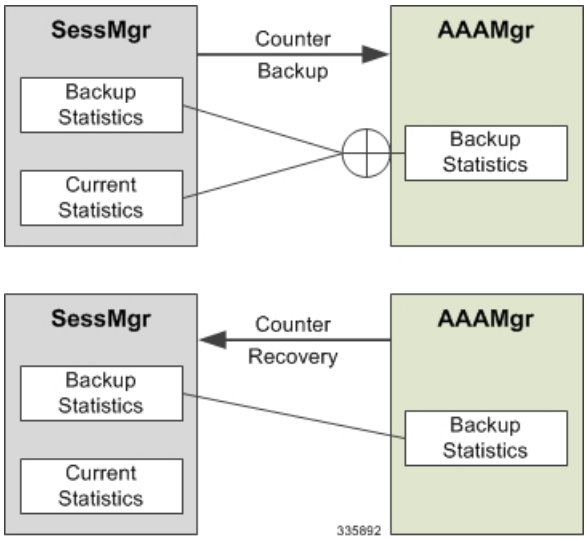
Architecture

When this feature is enabled (see *Configuring Backup Statistics Feature* below), the MME only backs up the counters maintained at the SessMgr. The recovery function does not need to be configured or started as it occurs automatically as needed when the feature is enabled.

The counters are backed up to the AAAMgr that is paired with the SessMgr. They are recovered from the AAAMgr if a SessMgr task is killed and after the SessMgr task recovers. This feature makes use of the session recovery framework to backup and retrieve the counters.

The following diagram depicts how backed-up statistics are maintained separately at the SessMgr and how the cumulative values are backed up and recovered from the AAAMgr after SessMgr task recovery completes.

Figure 9: Back Up and Recovery of Statistics for MME



Limitations

- A backup interval is *optionally* specified default is every 5 minutes. We recommend care should be taken when defining an interval as too small an interval could mean too frequent checkpoints. For example, if the backup interval is specified as 5 minutes, then counters are backed up every 5 minutes. Suppose backup happened at Nth minute and the configured backup interval is for every 5 minutes, then if a task crash happens at N+4 minutes, the MME recovers only the values backed up at Nth minute and the data for the past 4 minutes is lost.

- Only service level statistics are backed up and recovered. Any KPI that is monitored per other granularity, such as per TAC or per eNodeB, is not supported.
- Only statistics maintained at the SessMgr are backed up. Statistics at other managers are not backed up.

Configuring Backup Statistics Feature

For the Backup and Recovery of Key KPI Statistics feature to work, it must be enabled by configuring the backup of statistics for the MME.

Configuration

The following CLI commands are used to manage the functionality for the backing up of the key KPI statistics feature

Enabling

The following configures the backup of statistics for the MME and enables the Backup and Recovery of Key KPI Statistics feature.

configure
statistics-backup mme
end

Setting the Backup Interval

The following command configures the number of minutes (0 to 60) between each backup of the statistics. When the backup interval is not specified a default value of 5 minutes is used as the backup interval

configure
statistics-backup-interval *minutes*
end

Disabling

The following configures the MME to disable the backing up of statistics for the MME.

configure
no statistics-backup mme
end

Verifying the Backup Statistics Feature Configuration

Use either the **show configuration** command or the **show configuration verbose** command to display the feature configuration.

If the feature was enabled in the configuration, two lines similar to the following will appear in the output of a **show configuration [verbose]** command:

```
statistics-backup  mme
statistics-backup-interval 5
```

Notes:

- The interval displayed is 5 minutes. 5 is the default. If the **statistics-backup-interval** command is included in the configuration, then the 5 would be replaced by the configured interval number of minutes.
- If the command to disable the feature is entered, then no statistics-backup line is displayed in the output generated by a **show configuration [verbose]** command.

Managing Backed-up Statistics

A new keyword, **recovered-values**, is used with existing show and clear commands to either generate a display of the backed-up statistics or to clear the backed-up statistics.

Displaying Backed-up Statistics

Use one of the following commands to generate a display of the backed up statistics:

- **show mme-service statistics [recovered-values] [verbose]**
- **show mme-service statistics emm-only [recovered-values] [verbose]**
- **show mme-service statistics esm-only [recovered-values] [verbose]**

Notes:

- When the **recovered-values** keyword is used, output includes both current + recovered backed-up statistical values.
- If no SessMmgr crash has occurred, then the recovered values in the output of the above commands will be 0 (zero).

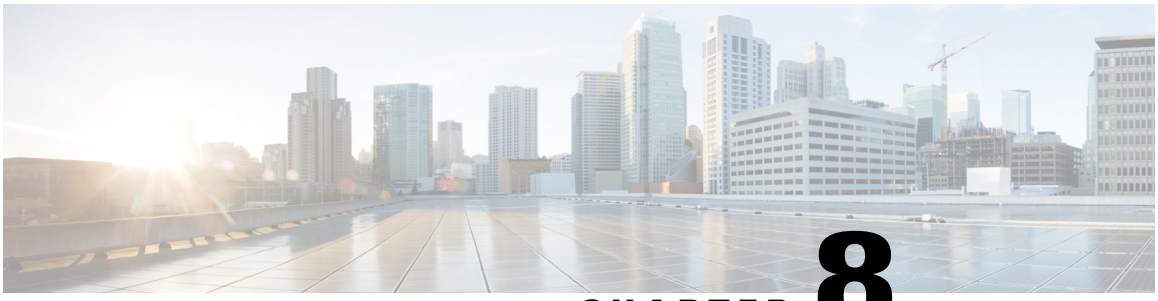
Clearing Backed-up Statistics

Use one of the following commands to clear (delete) the backed-up statistics. Note that the order entry for the service name identification varies in some of the commands. As well, the verbose keyword is not used with the **clear** commands.

- **clear mme-service statistics [recovered-values]**
- **clear mme-service statistics emm-only [recovered-values]**
- **clear mme-service statistics esm-only [recovered-values]**

Notes:

- When the **recovered-values** keyword is used, only the **recovered** values will be cleared.



CHAPTER 8

Cause Code #66

Feature Description

This feature is developed to achieve compliance with Release 11 3GPP Technical Specifications. The Release 11 3GPP Technical Specification introduced a new ESM/SM cause code "Requested APN not supported in current RAT and PLMN combination (cause code 66). This ESM/SM cause is used by the network to indicate that the procedure requested by the UE is rejected as the requested APN is not supported in the current RAT and PLMN. A UE which receives this cause will stop accessing the APN in the current RAT, but as soon as it enters another RAT type it will retry the APN.

In earlier releases only cause code 27 and cause code 33 were supported, these codes were not very effective in restricting APN in a particular RAT. For example, UE which has received cause 27 (with timer = 24hrs) will stop retrying a PDN connection in every RAT for 24 hrs. This is not the desired behavior in some cases APN cannot be restricted in a particular RAT. If the SGSN sends cause code 33 to the UE for an IMS APN, the UE/MS stops retrying the PDN connection for some time, but UE/MS will not automatically retry this APN in 4G, even though the APN is available there. The introduction of cause code 66 resolves this issue as the operator can block access to IMS APN in 2G/3G and can allow access in 4G.

Important This feature is applicable for both SGSN and MME.

Important This is a 3GPP Release 11 compliance feature, and will be applicable only to UEs capable of decoding ESM/SM cause code 66.

How It Works

This feature is developed for both SGSN and MME. In the SGSN, activation restriction of PDP context on the basis of access type can be configured using the restrict access-type command under the APN profile configuration mode. This command is now extended to MME; a new keyword "eps" is introduced to configure the APN profile to restrict the PDP context activation from EPS network access. If this CLI is enabled access to APN's associated with this APN profile are not allowed on MME/SGSN. By default, any activation on SGSN for this APN is rejected with cause code 'Requested APN not supported in current RAT and PLMN combination66'. During mobility scenarios the PDPs related to this APN are deactivated on the SGSN and the PDPs are also deactivated up to the GGSN/PGW.

On the MME attach is rejected if the default bearer related APN is not supported under the APN profile. By default the EMM cause and the ESM cause in attach reject are 'ESM failure19' and 66 respectively.

If the first default bearer APN is allowed, after a successful attach if the subsequent second default bearer APN is not supported, activation is rejected with cause 'Requested APN not supported in current RAT and PLMN combination66'. This is default MME behavior.

During mobility procedures on MME, if APN is not supported for bundle, bearers will deactivated all the way up to PGW and as well on MME for that particular bundle.

If the APN is not supported for all the bundles received from a peer node for a Tracking Area Update procedure at a new MME, Tracking Area Update is rejected with EMM cause 'No Suitable Cells In tracking area 15'.

If the APN is not supported for all the bundles received from a peer node for SRNS relocation procedure at the new MME, SRNS is rejected with GTPV2 cause 'Denied in RAT82' in Forward relocation response (if the peer node is MME/S4 SGSN). SRNS is rejected with GTPV1 cause 'Relocation failure213' in Forward relocation response if the peer node is a Gn Gp SGSN.

The operator can configure different cause values other than the default cause values mentioned in the scenarios described above. For SGSN/MME cause code remapping is done by configuring various options of the local-cause-code-mapping command under the Call Control Profile configuration mode (for both SGSN and MME) and MME Service Configuration mode (for MME only).

Standards Compliance

This feature is developed to comply with the following standards:

- 3GPP TS 24.301, Release 11 (version 11.14.0)
- 3GPP TS 23.401,Release 11 (version 11.11.0)
- 3GPP TS 24.008,Release 11 (version 11.15.0)
- 3GPP TS 23.060,Release 11 (version 11.12.0)

Configuring PDP Activation Restriction and Cause Code Values

The following configuration procedures are used to configure this feature. The access type restriction, cause code mapping for SGSN and MME can be configured using following procedures.

Configuring PDP Activation Restriction

The restrict access-type command under the APN profile configuration mode is used to configure PDP activation restriction on the basis of access type, a new command option for EPS networks is introduced for this feature. In earlier releases this command was supported only for GPRS and UMTS networks to perform QoS related restrictions. Now this command is also used to configure the APN not supported in particular RAT and PLMN combination. If this command is enabled, new PDP activations to an APN with which this APN profile is associated are rejected. During handovers PDPs/PDNs are deactivated if the APN name matches with this APN profile.

configure
apn-profile *profile_name*
[no] restrict access-type { eps | { { gprs | umts } [qos-class { background | conversational | interactive | streaming }] } }
default restrict access-type { eps | gprs | umts }
end

Notes:

- This command is disabled by default.
- In earlier releases this command was applicable only for SGSN. It is now supported by MME also.
- If the operator does not include the optional **qos-class** keyword option, then complete APN restriction is enabled and QoS related restrictions have no impact as QoS restriction is a subset of a complete APN restriction.

Configuring SM Cause Code Mapping for SGSN

The following command is used remap the cause code 66 to an operator desired cause code. This cause code is sent in activate rejection.

config
call-control-profile *profile_name*
[remove] local-cause-code-mapping apn-not-supported-in-plmn-rat sm-cause-code *cause_number*
exit

Notes:

- This mapping is not done by default.
- The keyword **apn-not-supported-in-plmn-rat** specifies the cause code for Requested APN not supported in current RAT and PLMN combination.
- The keyword **sm-cause-code** specifies the SM cause code to be used towards the UE. The value can be integer with range 1 up to 255.

Configuring ESM Cause Code Mapping for ESM Procedures (for MME)

The following command is used remap the ESM cause code sent in activate rejections (due to APN not supported) to an operator desired ESM cause code.

config
call-control-profile *profile_name*

[remove] local-cause-code-mapping apn-not-supported-in-plmn-rat esm-cause-code *cause_number* **esm-proc**
exit

Notes:

- This mapping is not done by default.
- The keyword **apn-not-supported-in-plmn-rat** specifies the cause code for Requested APN not supported in current RAT and PLMN combination.
- The keyword **esm-cause-code** specifies the ESM cause code to be used if a bearer management request is rejected due to this configuration. The value can be integer with range 1 up to 255.
- The specified esm-cause-code is used if an ESM procedure is rejected under the error condition **esm-proc**. This is specified as a keyword in the command.

Configuring EMM and ESM Cause Code Mapping for EMM Procedures (for MME)

The following command under the Call Control Profile configuration mode is used remap the EMM and ESM cause codes sent in activate rejections (due to APN not supported) to an operator desired ESM and EMM cause codes.

config
call-control-profile *profile_name*
[remove] local-cause-code-mapping apn-not-supported-in-plmn-rat emm-cause-code *cause_number* **esm-cause-code** *cause_number* **[attach [tau] | tau [attach]]**
exit

Notes:

- This mapping is not done by default.
- The keyword **apn-not-supported-in-plmn-rat** specifies the cause code for Requested APN not supported in the current RAT and PLMN combination.
- The keyword **emm-cause-code** specifies the EMM cause code to be used if a NAS request is rejected due to this configuration. A valid EMM cause value is an integer from 2 through 111.
- The keyword **esm-cause-code** specifies the ESM cause code to be used if a NAS request is rejected due to this configuration. A valid ESM cause value is an integer from 8 through 112.
- The keyword **attach** specifies the cause code to be used if an attach procedure is rejected under the error conditions.
- The keyword **tau** specifies the cause code to be used if TAU procedure is rejected under the error conditions.

Configuring ESM Cause Code Mapping for ESM Procedures (MME Service Configuration Mode)

The following command under the MME Service Configuration mode is used remap the ESM cause code sent in activate rejections (due to APN not supported) to an operator desired ESM cause code.

config
context <*context_name*>
mme-service <*service_name*>
local-cause-code-mapping apn-not-supported-in-plmn-rat esm-cause-code <*cause_number*>
esm-proc
default local-cause-code-mapping apn-not-supported-in-plmn-rat esm-cause-code esm-proc
exit

Notes:

- The default cause code for esm-proc is 66.
- The keyword **apn-not-supported-in-plmn-rat** is used to specify the cause code for Requested APN not supported in current RAT and PLMN combination.
- The keyword **esm-cause-code** is used to specify the ESM cause code to be used if a bearer management request is rejected due to this configuration. The ESM cause value is an integer with range 8 up to 112.
- The specified esm-cause-code is used if an ESM procedure is rejected under the error condition **esm-proc**. This is specified as a keyword in the command.

Configuring EMM and ESM Cause Code Mapping for EMM Procedures (MME Service Configuration Mode)

The following command under the MME Service configuration mode is used remap the EMM and ESM cause codes sent in activate rejections (due to APN not supported) to an operator desired ESM and EMM cause codes.

config
context *context_name*
mme-service *service_name*
local-cause-code-mapping apn-not-supported-in-plmn-rat emm-cause-code *cause_number*
esm-cause-code *cause_number* **[attach [tau] | tau [attach]]**
default local-cause-code-mapping apn-not-supported-in-plmn-rat [attach | tau]
exit

Notes:

- The default cause code values for Attach procedure are emm-cause-code 19 and esm-cause-code 66. The default cause code values for TAU procedure are emm-cause-code 15 and esm-cause-code 66.
- The keyword **apn-not-supported-in-plmn-rat** specifies the cause code for Requested APN not supported in current RAT and PLMN combination.
- The keyword **emm-cause-code** specifies the EMM cause code to be used if a NAS request is rejected due to this configuration. The EMM cause value is an integer with range 2 up to 111.
- The keyword **esm-cause-code** specifies the ESM cause code to be used if a NAS request is rejected due to this configuration. The ESM cause value is an integer with range 8 up to 112.

- The keyword **attach** specifies the cause code to be used if an attach procedure is rejected under the error conditions.
- The keyword **tau** specifies the cause code to be used if TAU procedure is rejected under the error conditions.

Verifying the Feature Configuration

The configuration of this feature can be verified using the following show commands.

Execute the **show configuration** command to verify the configuration, the output displays the following parameters based on the configuration:

- restrict access-type umts/gprs/eps
- local-cause-code-mapping apn-not-supported-in-plmn-rat sm-cause-code *cause_number*
- local-cause-code-mapping apn-not-supported-in-plmn-rat esm-cause-code *cause_number* esm-proc
- local-cause-code-mapping apn-not-supported-in-plmn-rat emm-cause-code 19 esm-cause-code 66 attach
- local-cause-code-mapping apn-not-supported-in-plmn-rat emm-cause-code 19 esm-cause-code 66 tau
- local-cause-code-mapping apn-not-supported-in-plmn-rat esm-cause-code 32 esm-proc
- local-cause-code-mapping apn-not-supported-in-plmn-rat emm-cause-code 15 esm-cause-code 66 attach
- local-cause-code-mapping apn-not-supported-in-plmn-rat emm-cause-code 19 esm-cause-code 66 tau

Execute the **show apn-profile full** *profile_name* command to verify the configuration, the output displays the following parameters based on the configuration:

- Service Restriction for Access Type UMTS:
- Complete APN restricted : Enabled
- Service Restriction for Access Type GPRS:
- Complete APN restricted : Enabled
- Service Restriction for Access Type EPS:
- Complete APN restricted : Enabled

Execute the **show call-control-profile full** *profile_name* command to verify the configuration, the output displays the following parameters based on the configuration:

- Mapped SM Cause For Req APN not sup in current RAT and PLMN combination: Not Configured
- Mapped SM Cause For Req APN not sup in current RAT and PLMN combination: Requested service option not subscribed (33)
- Cause Code Mapping
- APN not supported PLMN-RAT esm-proc : Operator Determined Barring (esm-8)
- APN not supported PLMN-RAT Attach : ESM failure (emm-19), Requested APN not supported in current RAT and PLMN combination (esm-66)

- APN not supported PLMN-RAT TAU : ESM failure (emm-19), Requested APN not supported in current RAT and PLMN combination (esm-66)

Execute the **show mme-service name** *mme_service* command to verify the configuration, the output displays the following parameters based on the configuration:

- APN not supported PLMN-RAT esm-proc : Requested APN not supported in current RAT and PLMN combination (esm-66)
- APN not supported PLMN-RAT Attach : ESM failure (emm-19), Requested APN not supported in current RAT and PLMN combination (esm-66)
- APN not supported PLMN-RAT TAU : No Suitable Cells In tracking area (emm-15)

Monitoring and Troubleshooting the Cause Code Configuration

This section provides information on the show commands and bulk statistics available to support this feature.

Show Command(s) and/or Outputs

This section provides information regarding show commands and/or their outputs in support of this feature.

show gmm-sm statistics verbose

The following new parameters are added to this show command to display the statistics for this feature:

- 3G-Pri-Actv-APN-Not-Sup-Rej
- 2G-Pri-Actv-APN-Not-Sup-Rej
- 3G-APN-Not-Supported-in-PLMN-RAT
- 2G-APN-Not-Supported-in-PLMN-RAT
- APN Not Supported in PLMN RAT combination Statistics
- 3G-Pdp-Dropped-During-New-SGSN-RAU
- 2G-Pdp-Dropped-During-New-SGSN-RAU
- 3G-Pdp-Dropped-During-New-SGSN-SRNS
- Pdp-Dropped-During-3G-To-2G-IRAT
- 3G-Actv-NRPCA-Reject
- Pdp-Dropped-During-2G-To-3G-IRAT

The following statistics are MME specific:

- APN not sup PLMN-RAT
- Inbound Inter node SRNS failure
- APN not sup in PLMN/RAT

Bulk Statistics

The following statistics are included in the MME and SGSN Schemas in support of the feature.

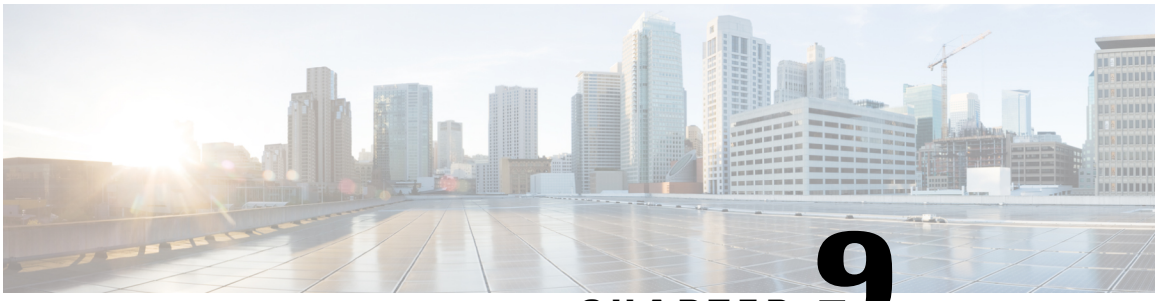
MME Schema

- inter-node-srns-proc-fail-apn-not-supported
- inter-node-tau-proc-fail-apn-not-supported
- tai-esm-msgtx-pdncon-rej-apn-not-sup-in-plmn-rat
- tai-emm-msgtx-attach-rej-apn-not-sup-in-plmn-rat
- attach-proc-fail-apn-not-sup-in-plmn-rat
- esm-msgtx-pdncon-rej-apn-not-sup-in-plmn-rat
- emm-msgtx-attach-rej-apn-not-sup-in-plmn-rat
- emmdisc-apnnotsupinplmnrat

SGSN Schema

- 3G-actv-rej-apn-not-supported-in-plmn-rat
- 2G-actv-rej-apn-not-supported-in-plmn-rat
- 3G-actv-rej-apn-not-supported-in-plmn-rat-cum
- 2G-actv-rej-apn-not-supported-in-plmn-rat-cum
- 2G-3G-irat-pdp-drop-apn-not-supported-in-plmn-rat
- 2G-israu-pdp-drop-apn-not-supported-in-plmn-rat
- 3G-israu-pdp-drop-apn-not-supported-in-plmn-rat
- 3G-srns-pdp-drop-apn-not-supported-in-plmn-rat
- 3G-nrpca-pdp-drop-apn-not-supported-in-plmn-rat
- 3G-2G-irat-pdp-drop-apn-not-supported-in-plmn-rat
- 2G-inter-svc-rau-pdp-drop-apn-not-supported-in-plmn-rat

For descriptions of these variables, see the information for the SGSN and MME schema in the *Statistics and Counters Reference*.



CHAPTER 9

Cell Broadcast Center - SBc Interface

Feature Description

The MME uses the SBc interface, between the MME and the Cell Broadcast Center (CBC), for warning message delivery and control functions.

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.

Customers can now enable CMAS functionality in their networks to provide warning notifications to subscribers.

Important Beginning with Release 18.4, a valid license key is required to enable the SBc interface. Contact your Cisco Account or Support representative for information on how to obtain a license.

How It Works

The MME accepts incoming SBc associations coming from multiple CBCs.

The MME is responsible for the delivery of the Warning Messages received from CBC to all relevant eNodeBs serving the given TAI list. In the absence of TAI list in the received Warning Message, MME sends the Warning Message to all connected eNodeBs.

The MME acknowledges to CBC when it has started distributing the Warning Message to all relevant eNodeBs. If a response is not received from any eNodeB, it shall not result in any exclusive error messaging to CBC.

Even if the MME node is experiencing congestion, Warning Messages are forwarded and not dropped.

When connected to multiple CBCs, the uniqueness of Warning Messages as identified by Message Type, Message Identifier and Serial Number, must be ensured across these CBCs.

DSCP Marking for SBc Interface

SBc services provides the Differentiated Services Code Point (DSCP) marking functionality. DSCP marking helps in packet traffic management. DSCP marking can be performed on both IPv4 and IPv6 packets leaving the SBc interface.

Either the pre-defined DSCP values can be used for marking, or any arbitrary value ranging from 0x01 to 0x3F can be assigned. The default DSCP value is 0x00 or be (Best Effort). The default DSCP value is automatically set when the configuration is disabled.

config
context *context_name*
sbc-service *service_name*
[no] ip qos-dscp *dscp_value*
end

- ip defines the Internet Protocol parameters for the packets leaving through the SBc interface.
- qos-dscp designates the Quality of Service - Differentiated Services Code Point value to the packet leaving through the SBc interface.
- *dscp_value* is a value assigned to the packet for DSCP marking. The value can be a pre-defined DSCP value or an arbitrary value ranging from 0x01 to 0x3F.

Warning Message Call Flows

In compliance with 3GPP TS 29.168 v10.2.0, the MME supports the following procedures:

- Write-Replace Warning Procedure
- Stop Warning Procedure
- Error Indication Procedure

Standards Compliance

The MME's implementation of this feature complies with the following standards:

- 3GPP TS 23.041 v10.6.0 Technical realization of Cell Broadcast Service (CBS)
- 3GPP TS 29.168 v10.2.0 Cell Broadcast Centre Interfaces with the Evolved Packet Core
- 3GPP TS 22.268 v10.4.0 Public Warning System
- 3GPP TS 36.413 v10.6.0 S1-AP Interface

Configuring SBc Interface

Creating and Configuring SBc Service

An SBc service must be created within a context to configure the SBc-AP interface to accept connections from one or more CBCs.

Important Beginning with Release 18.4, a valid license key is required to access the commands used to configure and manage the SBc interface. Contact your Cisco Account or Support representative for license information.

```
configure
    context ctxt_name
        sbc-service sbc_svc_name
            associate sctp-param-template sctp_param_template_name
            bind ipv4-address ipv4_address_value1 ipv4-address ipv4_address_value2
            cbc-associations maximum number
            sbc-mme sctp port port_num
            end
```

Notes:

- Up to 8 SGs + MME + SBc + SLs Services can be configured on the system. The SBc service name must be unique across all contexts.
- Associating the SBc service to the SCTP parameter template is not required for the SBc service to be operational. However, if a template is associated, the template must exist before the SBc service is associated to it.
- The SBc service must be bound to at least 1 IP address. Up to 2 IPv4 or 2 IPv6 addresses can be specified for multi homing purposes.
- The **cbc-associations** command is used to define the maximum number of CBC connections allowed for this SBc service. The default setting is 1. Up to 2 connections are allowed per SBc service.
- The default SCTP port used is 29168. The MME listens for incoming SBc-AP connections from an CBC on this port.

Associating the SBc Service with the MME Service

Use the following sample configuration to associate the SBc service to an MME service.

```
configure
    context ctxt_name
        mme-service mme_svc_name
            associate sbc-service sbc_svc_name [ context ctxt_name ]
            end
```

Notes:

- Each MME service can be associated with one unique SBc service.

- The SBc service is **not** a critical parameter for the MME service. Removing this configuration will **not** restart the MME service.
- The MME will always check for a valid SBc service that is up and connected to a CBC before performing any meaningful operations on the Warning Messages received on the S1-AP interface (like attempting to forward the messages).
- Use the optional context keyword if the SBc service and MME service are configured in separate contexts.
- The SBc service is not operationally STARTED unless the MME service to which it is associated is in a STARTED state.

Verifying the SBc Service Configuration

The following command displays configuration information for all SBc services, for the specified for the specified SBc service, or for the specified Cell Broadcast Center.

show sbc-service { all | cbc-associations { all | sbc-service-name *sbc_svc_name* **[path-info | summary] } | sbc-service-name** *sbc_svc_name* **}**
The following command displays the SBc Service name and SBc Service Context which has been associated with each MME service.

show mme-service all
The following command displays configuration errors and warnings related to all SBc services on the MME:

show configuration errors section sbc-service verbose

Monitoring SBc Services

This section lists the SNMP traps, bulk statistics, and show commands that display operational statistics relating to SBc services.

SNMP Traps

The following traps are available to track status and conditions relating to the SBc service.

- **starSBCServiceStart**: An SBc Service has started.
- **starSBCServiceStop**: An SBc Service has stopped.

The following traps are generated to track status and conditions of individual CBC associations.

- **starCBCAssocDown**: A CBC Association is down.
- **starCBCAssocUp**: A CBC Association is up.

SBc Bulk Statistics

SBc service related bulk statistics are provided within the **SBc** schema.

Use the following command to display a list of all variables available within this schema:

show bulkstats variables sbc
For more information about these statistics, refer to the **SBc Schema** chapter of the *Statistics and Counters Reference*.

SBc Service Show Commands and Outputs

The following command displays all statistics related to the SBc service. These statistics can be filtered based on CBC association (peer-id) or SBc service name.

show sbc statistics { all | peer-id *peer_id* **| sbc-service-name** *sbc_svc_name* **}**
The following command displays S1-AP statistics relating to the SBc interface. Check the lines for Kill Request and Kill Response in the sample below:

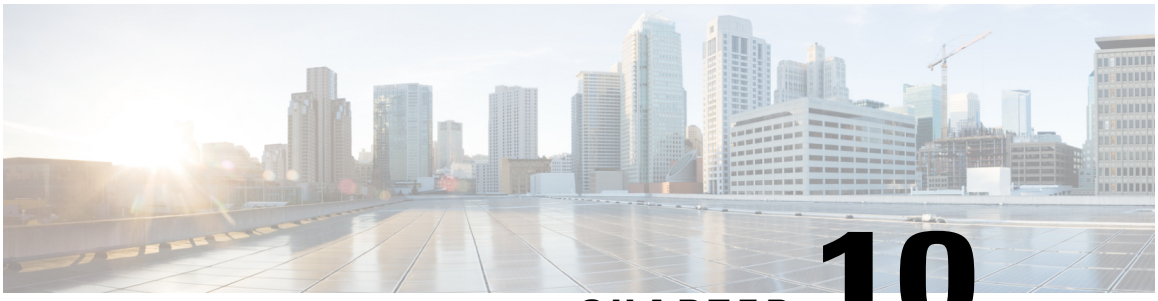
show mme-service statistics s1ap

```
S1AP Statistics:
   Transmitted S1AP Data:

       Kill Request: 0    Write-Replace Warning Request: 0
   Received S1AP Data:

       Kill Response: 0   Write-Replace Warning Response: 0
```

Event Logging

Event logging for the SBc interface can be enabled using the following command:

logging filter active facility sbc level *severity_level*
Refer to the *System Logs* chapter of the *System Administration Guide* for more information about event logging.



CHAPTER 10

Cell Traffic Trace

The Cell Traffic Trace feature for subscriber and equipment tracing provides detailed information at the call level on one or more UEs and serves as an additional source of information (along with Performance Measurements) for monitoring and optimization operations.

This section describes MME support for Cell Traffic Trace.

Feature Description

The Cell Traffic Trace feature, for subscriber and equipment tracing, provides detailed information at the call-level on one or more UEs and serves as an additional source of information (along with Performance Measurements) for monitoring and optimizing operations.

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.

Trace activation/deactivation is administered by an entity called an Element Manager (EM) on the Network Elements (NE) that comprise the network. The NE generate the trace data or results and transfers the information to a Trace Collection entity (TCE). Trace activation/deactivation can be of two types:

- Management Activation/Deactivation - Trace activated/deactivated in different NEs directly by using the management EM.
- Signaling based Activation/Deactivation - Trace activated/deactivated in different NEs using signaling interfaces between them. The NEs forward the activation/deactivation originating from EM.

In an EPS network, trace is enabled on the following NE: eNodeB, MME, SGW, PGW, HSS, EIR and so on. Cell Traffic Trace enables tracing of all active at one or more Cells in eNodeBs.

A valid license key is required to enable Cell Traffic Trace. Contact your Cisco Account or Support representative for information on how to obtain a license.

How It Works

When Cell Traffic Trace is activated in the monitored cell(s) of E-UTRAN, the eNodeB starts a Trace Recording Session for new calls/session and also for existing active calls/session. A Trace Recording Session Reference (TRSR) is allocated by eNodeB for each of the monitored call/session. The TRSR includes the TRSR reference along with the Trace Reference and TCE address in the CELL TRAFFIC TRACE message to the MME over S1 connection.

Cell Traffic Trace Procedures are used at the MME to assist the TCE Server in correlating the Trace Reference (generated by EM) and Trace Recording Session Reference (generated by the eNodeB) with the IMSI, IMEI (SV) corresponding to the traced session as the eNodeBs only have access to temporary UE identities and not permanent identities (IMSI, IMEI (SV)).

Cell Traffic Trace involves the following nodes:

- Network Element (NE): Network elements are the functional component to facilitate subscriber session trace in mobile network. The term network element refers to a functional component that has standard interfaces in and out of it. It is typically shown as a stand-alone AGW. Examples of NEs are the MME, S-GW, and P-GW.
- Element Manager (EM): The Element Manager (EM) forwards the globally unique Trace Reference to each eNodeB.
- eNodeB
- MME and
- Trace Collection Entity (TCE) server

The Cell Traffic Trace feature operates sequentially and is classified into two stages:

- Trace Files management - Creation of Trace files, renaming and moving trace files to respective directories, compression and archiving of trace files. The configuration for this process is discussed in the Configuring Cell Traffic Trace section.
- Decompression - This process is executed to extract compressed and archived files. The files are named by a **.gz** extension. It is highly recommended to use tar for the decompression process. The command syntax to decompress the trace files is as follows: **Syntax: tar -zxf <file_name>.gz**

Architecture

MME supports the following in Cell Traffic Trace:

- When MME receives a Cell Traffic Trace message from eNodeB, it extracts the Trace Reference and Trace Recording Session Reference, and checks for the IMSI and IMEI if present, from the S1 AP ID.
- The MME send the IMSI, IMEI if present, and the Trace References received in a Cell Traffic Trace to the TCE. The TCE address is received in the Cell Traffic Trace signal from eNodeB.
- The MME complies with data formats of Trace Reference, Trace recording Session Reference and TCE Address.

The Cell Traffic Trace operation takes place in the following stages:

Stage 1: Creation of trace files on expiry of Collection Timer

- A list is initialized at the session manager to store relevant information of all the incoming cell trace messages.
- Once the collection timer expires, the session manager gathers all the cell traces into a file, which has a temporary name, and writes it to the hard-disk.

Stage 2: Renaming and moving the files to archive directories by session trace

- The session trace renames these temporary filenames to C Type filenames. The C Type file name is a modified version of the 3gpp specification. A suffix is added to every C type file. Thus starting from 1 the suffix ends at 4294967295. After reaching the maximum limit, then the suffix restarts from 1. The files are then moved to the directories.
  For example, refer to the file name given below:
  `C20150520.0137-0400-MME.RTPBNGASR5KCH78.21436500008D-1C20150529.0231-0400-MME.RTPBNGASR5KCH78.3143650000FF-4294967295`
  The C Type file format is modified to provide additional trace information with a trace extension, which has three additional fields such as eNodeB ID, UE S1 AP identity and the MME UE S1 AP identity.
- A new archive directory is created by the session trace when the previous directory is full. The syntax for the new directory is as follows: Syntax: <nodename>.<time-stamp in seconds>.<tce_index>.<file-counter>. For example:
  `RTPBNGASR5KCH78.555ac613.1.1`
- If the cell trace messages are meant to be for two different TCE's, then a second directory would be created and the files are moved to their directories respectively.

Stage 3: Compression and Archiving files to directories by session trace

- Session trace waits for a configured file count or timer expiry or directory size to be reached before archiving the directories.
- Once the archive directories are full, the session trace archives or compresses these directories and moves them to the final directories.

The above mentioned files and are monitored and processed to their final directories based on the following timers:

- **Collection timer:** This timer is configurable, and the timer ranges from 0 - 255 seconds. The collection timer is triggered by the session manager. Once the timer expires, the session manager writes the files to the staging location in the hard disk. After all files are written, a messenger call is sent from session manager to session trace indicating the details of the new file.
- **Archive trigger timer:** This timer is configurable, and the timer ranges from 1 to 3600 seconds. The Archive timer is triggered by the session trace. This timer is a safety mechanism to make sure archive directories are closed and sent for compression and archiving.

Limitations

Decompression of the trace files using gzip or gunzip may cause file corruption depending on the system platform used, for example: Linux. Mac and so on

Standards Compliance

The Cell Traffic Trace feature complies with the following standards:

- 3GPP TS 36.413 Release 10, S1 Application Protocol (S1AP)
- 3GPP TS 32.422 Release 10, Trace control and configuration management
- 3GPP TS 32.423 Release 10, Trace data definition and management

Configuring Cell Traffic Trace

This section documents configuration of Cell Traffic Trace and its related functionality.

Configuring Trace Files Storage

The configuration provided in the below section is used to store the cell traffic trace files locally or on a TCE server.

The commands illustrated below configure the Cell Traffic Trace. In support of the Cell Trace feature, the **enb** keyword has been added, which monitors the traffic from the eNodeB network element. The configuration also includes archiving and compression parameters to archive and compress trace files into their directories.

Local Storage

To store the trace files locally, use the following configuration:

configure
  session trace network-element enb tce-mode none collection-timer *timer_value*
  [no] session trace network-element enb
  end

Notes:

All parameters are new to the Cell Traffic Trace feature. For information on these parameters refer to the **session trace** command in the *Command Line Interface Reference*.

TCE Server Storage

To store the trace file on a TCE server, use the following configuration:

configure
  session trace network-element enb tce-mode push transport sftp path *server_path_name* **username** *user_name* **[encrypted] password** *user_password* **collection-timer** *timer_value*
  [no] session trace network-element enb
  end

Notes:

All parameters are new to the Cell Traffic Trace feature. For information on these parameters refer to the **session trace** command in the *Command Line Interface Reference*.

Configuring Cell Traffic Trace Template - Archiving and Compressing Trace Files

The configuration provided in this section is used to archive and compress trace files into their directories.

This command creates a template with parameters that configure archiving and/or compression for the files generated by Cell Traffic Trace. Defining this template and archiving and/or compression of files is optional when setting up Cell Traffic Trace. The **enb** keyword processes Cell Traffic Trace in the MME.

configure
template-session-trace network-element enb template-name cell-trace
[no] disk-limit *disk_size*
[no] archive files *number_of_files* **size** *size* **timer** *timer_value*
[no] trace-extension enb-id ue-s1ap-id
end

Notes:

- **cell-trace** indicates the template name 'cell-trace' for storage of the eNodeB cell trace storage parameters. Note that you cannot define a template name - there is only one template and its name is 'cell-trace'.
- **disk-limit** *disk_size* is measured in megabytes (MB). This keyword defines the total space to be reserved on the hard disk. If disk-limit alone is configured then compression is not considered. The disk-limit size ranges from 1 MB to 20480 MB. If disk-limit is not configured, a default size of 200 MB is allocated in the hard disk for storing Cell Trace files.
- **archive** allows you to define the archive directory and the archive parameters.
  - **files** *number_of_files* defines the maximum number of files that can be archived in the directory. When the limit is reached, the archive closes. The range is an integer from 1 to 10000.
  - **size** *size* defines the directory limit in MB. The range is an integer from 1 to 10
  - **timer** *timer_value* defines the total time in seconds before the pending directories are archived. The range is an integer from 1 through 3600.
- The **trace-extension** keyword defines the UE or eNodeB identity extension parameters for the C Type files.
  - The **enb-id** keyword is an additional field in the C Type file that identifies the global eNodeB entry.
  - The **ue-s1ap-id** keyword is an additional field in the C Type file that identifies the eNodeB ID, UE S1 AP identity and the MME UE S1 AP identity.

Verifying the Cell Traffic Trace Configuration

The following command is used to display/verify the parameters for Cell Traffic Trace from the eNodeB network element.

show session trace template network-element enb template-name cell-trace

On running the above mentioned show command the following statistics are displayed:

```
Template name: cell-trace
NE Type: ENB
```

```
Cell Trace file Extension entries: GLOBAL-ENB-ID ENB-UE-S1AP-ID MME-UE-S1AP-ID
Storage Parameters for Archiving Cell trace files:
Disk Storage Limit: 200 MB
Files per Archive Directory: 4000
Total size per Archive directory: 3 MB
Archive directory timeout: 300 seconds
```

Monitoring and Troubleshooting the Cell Traffic Trace

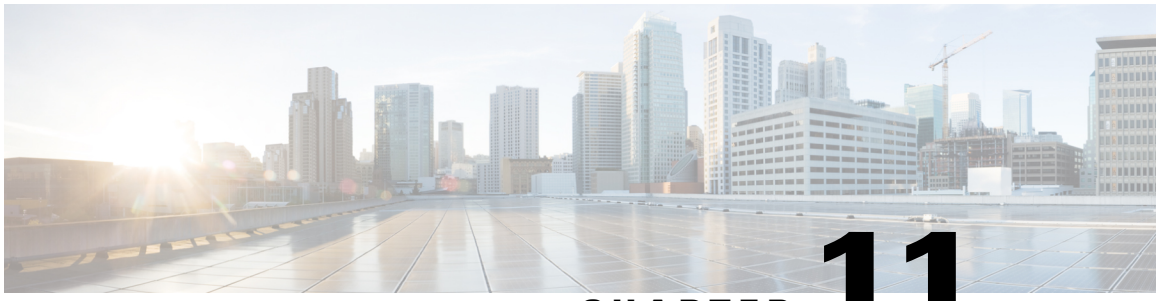
The following section describes commands available to monitor Cell Traffic Trace on the MME.

Cell Traffic Trace Show Command(s) and/or Outputs

show session trace statistics

On running the above mentioned show command, statistics similar to the following are displayed:

```
Interface not traced: 0
Total number of file generated: 25541
Number of Cell Traffic Trace files generated: 25541
Total archive files: 7
Avg Time in secs, for archiving one directory: 2.247592
Avg Time in secs, for Moving one C type file: 0.0200471
Avg files per archive directory: 3648
Frequency of Archiving Triggers:
          Files: 5
          Size: 1
          Time-out: 1
```



CHAPTER 11

Closed Subscriber Groups

Feature Description

The MME provides support for Closed Subscriber Groups (CSG). This enables the MME to provide access control and mobility management for subscribers who are permitted to access one or more CSG cells of the PLMN as a member of the CSG for a Home eNodeB (HeNB).

A CSG ID is a unique identifier within the scope of the PLMN which identifies a Closed Subscriber Group in the PLMN associated with a CSG cell or group of CSG cells.

The MME performs access control for CSG a UE will not be permitted to access the network through a CSG cell unless either the UE's subscription data includes the same CSG ID as the CSG cell, or if the CSG cell is operating in hybrid mode. The MME also optionally reports the UE's CSG information to the S-GW/P-GW, based on the MME's CLI mme-service configuration. The S-GW/P-GW, in turn, informs the MME when it should report user CSG information.

How It Works

Closed Subscriber Group functionality is comprised of three main components, each are described in this section.

Access Control

The MME performs CSG-based access control by examining the CSG cell information provided by the eNodeB through the S1AP interface for a UE connection or handover attempt, and comparing that to the CSG subscription data for that UE provided by the HSS through the S6a interface. CSG-based access control affects the following S1AP and S6a messages and messaging:

S1AP Messaging

Important For additional security, the S1AP connections between the MME and the eNBs may be secured through IPSec.

- **S1 Setup Request** If the eNB sending the S1 Setup Request supports one or more CSG cells, the S1 Setup Request will contain the CSG IDs of the supported CSGs. The MME will store the CSG IDs as part of the data pertaining to the eNB.
- **eNB Configuration Update** If the eNB sending the eNB Configuration Update supports one or more CSG cells, the eNB Configuration Update will contain the CSG IDs of the supported CSGs, which may or may not have changed from those sent in the S1 Setup Request. The MME will overwrite the stored CSG IDs for that eNB with the list contained in the eNB Configuration Update.
- **Initial UE Message** If the establishment of the UE-associated logical S1-connection is performed due to a connection originating from a CSG cell, the CSG ID is included in the Initial UE Message. If the establishment of the UE-associated logical S1-connection is performed due to a connection originating from a Hybrid cell, the CSG ID and the Cell Access Mode IE are included in the Initial UE Message. The MME stores the CSG ID and Cell Access Mode in the UE context. If the UE context already exists, the MME overwrites the existing CSG ID and Cell Access Mode with the new data, or clears the CSG ID and Cell Access Mode if the CSG ID is not present in the message. The CSG ID is checked against the subscription data from the HSS to determine if the UE is a member of the CSG. If the UE is not a member, and the cell is not a hybrid cell, access is denied.
- **Initial Context Setup Request** If the cell is a hybrid cell, the Initial Context Setup Request from the MME contains a CSG Membership Status IE indicating whether the UE is a member of the cell's CSG.
- **UE Context Modification Request** A UE Context Modification Request from the MME contains a CSG Membership Status IE if the cell has a CSG ID (if the cell is either a CSG cell or a hybrid cell). The MME sends a UE Context Modification Request indicating CSG Membership Status is Non-member if the HSS sends a Delete Subscriber Data Request with DSR Flags indicating that CSG subscription data is being deleted. The MME also sends a UE Context Modification Request indicating CSG Membership Status is Non-member if the CSG subscription data for the CSG in question includes an Expiration Date AVP and the time indicated by the AVP has been reached.
- **Paging** The Paging message may contain a list of one or more CSG IDs. If the MME includes this list, the eNodeB avoids paging the UE at CSG cells whose CSG ID does not appear in the list. If the UE has CSG IDs in its subscription data, the MME includes the intersections of the eNodeB's CSG ID list and the subscriber's CSG ID list in the Paging message whenever that UE is being paged.
- **Handover Required** The Handover Required message may contain a CSG ID if it does, there may also be a Cell Access Mode IE which indicates the target cell is a hybrid cell. When the MME receives a Handover Required message with a CSG ID, it uses the UE's subscription data to determine if the UE

is a member of the CSG in question. If the UE is not a member and the cell is not a hybrid cell, the MME refuses the handover attempt. Otherwise, the MME conveys the CSG information to the target system.

- **Handover Request** If the MME is sending a Handover Request message, a CSG ID is included in the message if the target has been specified as either a CSG cell or hybrid cell with the CSG ID in question. If the cell has been specified as a hybrid cell, the MME also includes a CSG Membership Status IE in the Handover Request as well.
- **Handover Request Ack** If the Handover Request contains both a CSG ID and a CSG Membership Status IE, but the target cell in question is a hybrid cell that broadcasts a different CSG ID, the actual CSG ID of the cell shall be included in the Handover Request Ack. Upon receipt of such a message, the MME changes the CSG ID of the UE, marks the target cell as being a hybrid cell, and considers the UE to be a non-member of the CSG. Note that the MME may later discover via subscription data from the HSS that the UE is actually a member of the CSG in question if so, it sends a UE Context Modification Request indicating that the UE is a member of the CSG. Note also that if the Handover Request contains a CSG ID and the target cell broadcasts a different CSG ID and is not a hybrid cell, the eNB sends a Handover Failure message, not a Handover Request Ack.

S6a Messaging

- **Update Location Ack** Messages from the HSS contain the UE's subscription data, which may include CSG subscription data. CSG subscription data consists of one or more CSG IDs, each of which may also have an associated expiration date. The CSG IDs are interpreted within the context of the PLMN ID sent to the HSS in the Visited-PLMN-ID AVP in the Update Location Request message. The CSG subscription data is stored in the UE's database entry along with the rest of the UE subscription data. The MME stores up to eight CSG IDs per UE. The MME uses the CSG subscription data to determine membership in a given CSG by comparing the CSG ID of the current cell against the CSG IDs in the subscription data.
- **Delete Subscriber Data Request** The HSS can indicate to the MME to delete the stored CSG subscription data by sending a Delete Subscriber Data Request message with the CSG Deleted bit set in the DSR flags. If this happens, and the UE is currently connected to a cell where it was a CSG member, the MME sends a UE Context Modification Request indicating that the UE is no longer a CSG member. The MME is responsible for enforcing the expiration date (if any) for a given CSG as indicated in the CSG subscription data. If the CSG subscription expires, the MME must send a UE Context Modification Request indicating that the UE is no longer a CSG member.

CSG Notification to S-GW/P-GW

The MME informs the P-GW whether it supports CSG change notification by setting the CSG Change Reporting Support Indication (CCRSI) flag. MME support for CSG change notification can be enabled or disabled. If it is enabled, the P-GW, based on input from the PCRF, determines if CSG change notification is required by sending the CSG Information Reporting Action IE to the MME.

CSG notification to the S-GW/P-GW affects the following S11 messages and messaging:

- **Create Session Request** The Indication IE in the Create Session Request contains a CSG Change Reporting Support Indication (CCRSI) flag, which is set when the MME is configured to support CSG information change reporting to the S-GW/P-GW. If the UE is attached through a CSG or hybrid cell, the User CSG Information (UCI) IE is be included in the Create Session Request. The User CSG

Information IE contains the PLMN and CSG ID of the CSG or hybrid cell in question, the access mode (closed or hybrid), and if the access mode is hybrid, the membership status of the UE in the CSG.

- **Create Session Response** The P-GW/S-GW will send the CSG Reporting Information IE in the Create Session Response if CSG information reporting is to be started or stopped. This IE includes three bits that indicate whether the MME should report when the UE enters or leaves a CSG (non-hybrid) cell, a subscribed hybrid cell, or an unsubscribed hybrid cell. If all three bits are set to zero, all CSG information reporting to the S-GW/P-GW is stopped. The MME stores the CSG reporting information as part of the PDN context, since the reporting requirements may be different on different P-GWs.
- **Create Bearer Request** The Create Bearer Request message from the P-GW/S-GW may include a CSG Reporting Information IE if CSG reporting from the MME is to change. The MME stores the CSG reporting information as part of the PDN context in question.
- **Modify Bearer Request** The CCRSI flag in the Indication IE is set in a Modify Bearer Request when the MME is configured to support CSG information change reporting to the S-GW/P-GW. If the P-GW/S-GW has requested CSG information reporting and a TAU, Handover, or UE-initiated Service Request is taking place, the MME includes the User CSG Information IE in the Modify Bearer Request message.
- **Update Bearer Request** The Update Bearer Request message from the P-GW/S-GW may include a CSG Reporting Information IE if CSG reporting from the MME is to change. The MME stores the CSG reporting information as part of the PDN context in question.
- **Change Notification Request** The MME sends a Change Notification Request to the S-GW/P-GW for each PDN where it is requested, if a change to the CSG connection information changes without requiring either a Create Bearer Request or Modify Bearer Request. The Change Notification Request contains a User CSG Information IE. Since Location Reporting also uses the Change Notification Request message, the MME minimizes the number of Change Notification Request messages sent by bundling the reporting of a location change with a CSG change into the same message whenever possible.
- **Change Notification Response** The Change Notification Response message from the P-GW/S-GW may include a CSG Reporting Information IE if CSG reporting from the MME is to change. The MME stores the CSG reporting information as part of the PDN context in question.

CSG Status Communication to Peer MME/SGSN

The MME indicates its ability to report location information using the "CSG Change Reporting Support Indication" which is a part of the indication flags parameter.

CSG status communication to a peer MME or SGSN affects the following S10 and S3 messages and messaging:

- **Forward Relocation Request** If the source MME or SGSN supports CSG information change reporting, the CCRSI flag is set in the Indication IE in a Forward Relocation Request message from that MME or SGSN. If the source eNB or RNC included a target CSG ID as part of the Handover Required message, the source MME or SGSN include that CSG ID in a CSG ID IE in the Forward Relocation Request. If the source eNB or RNC indicated that the target cell is a hybrid cell, the source MME or SGSN determine whether the UE is a member of the CSG and include the CSG Membership Indication IE in the Forward Relocation Request. (A Forward Relocation Request that contains a CSG ID IE but no CSG Membership Indication IE indicates that the target cell is a closed CSG cell.) The PDN Connection IE(s) in the Forward Relocation Request will contain a CSG Information Reporting Action IE if the P-GW/S-GW had previously sent it to the source MME or SGSN for the PDN in question.

- **Context Response** If the old MME or SGSN in a Context Request/Response/Ack exchange supports CSG information change reporting, the CCRSI flag is set in the Indication IE shall be set in the Context Response from that MME or SGSN. The PDN Connection IE(s) in the Context Response contains a CSG Information Reporting Action IE if the P-GW/S-GW had previously sent it to the old MME or SGSN for the PDN in question.

Message Flows

The following diagram shows the messaging between the EPC elements in a Closed Subscriber Group implementation.

Figure 10: Closed Subscriber Groups Message Flow

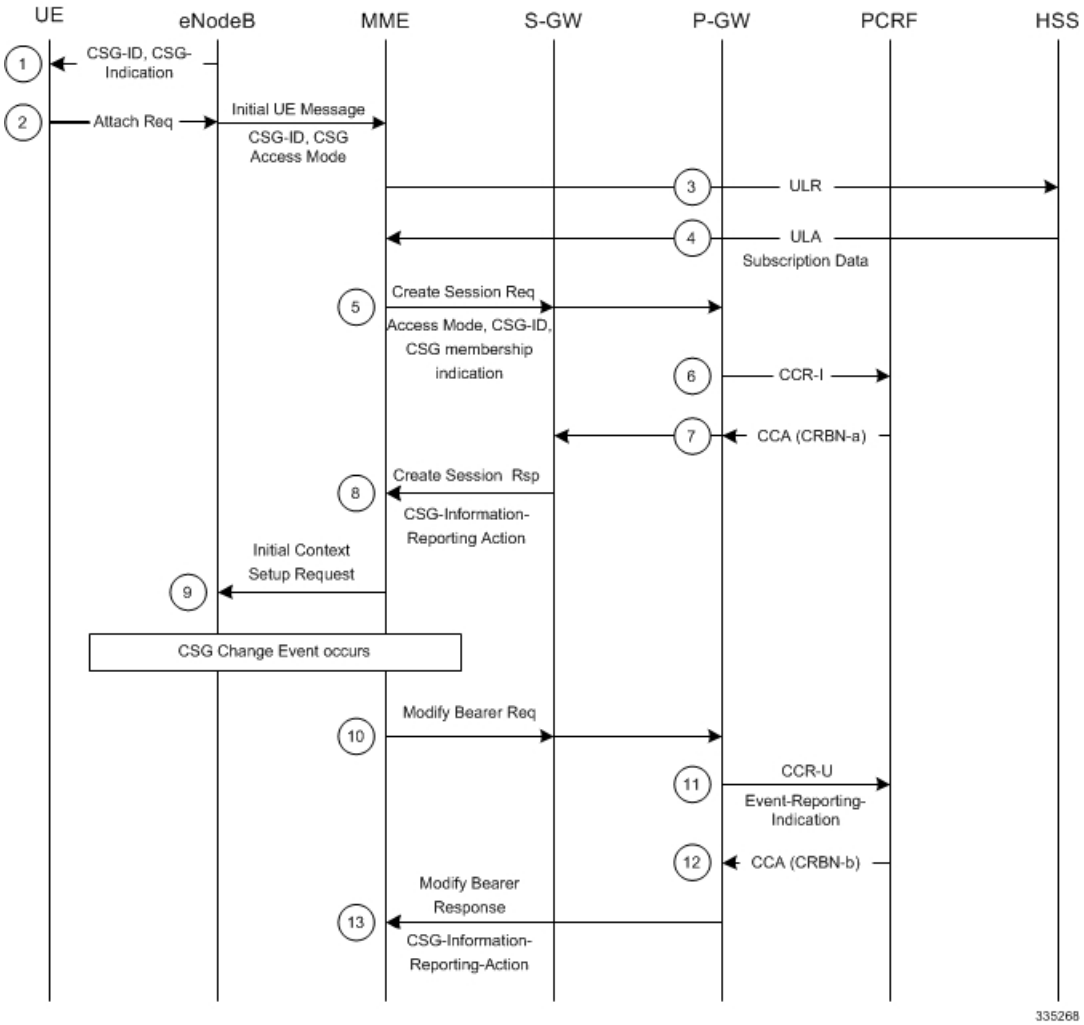


Table 8: Closed Subscriber Groups Message Flow 0

Step	Description
1	The eNodeB broadcasts the CSG Information to UEs.
2	When an Attach Request event happens, the eNodeB sends its own CSG-related Information in Initial UE message to the MME.
3	The MME sends an Update Location Request (ULR) to the HSS to get subscriber's profile.
4	The HSS responds with an Update Location Answer (ULA) including Subscription-Data which includes CSG-Subscription-Data. If the ULA does not include a CSG_ID: 1) The Attach attempt will be rejected if the Access mode is set to Closed 2) The call will proceed on a non-CSG-member basis if the Access mode is set to Hybrid.
5	The MME proceeds with the call according to the user profile from the HSS. The MME sets the CSG membership Indication and passes it to the S-GW including Access Mode and CSG-ID. The S-GW transparently passes the information to the P-GW.
6	The P-GW requests policy and charging rule from the PCRF.
7	The PCRF sends Event-Trigger:=USER_CSG_INFO_CHG and USER-CSG-INFO AVP based on user subscription profile.
8	The P-GW sets CSG-Information-Reporting-Action in Create Session Response when the P-GW receives Event-Trigger:=USER_CSG_INFO_CHG.
9	The MME sends CSG-Membership-Status to eNodeB. This is only occurs when the Access mode is set to Hybrid.
10	When a CSG change event happens, the eNodeB/MME reports the event. The MME updates CSG change event using a Change Notification Request or Modify Bearer Request.
11	The P-GW reports CSG change event using Event-Reporting-Indication AVP to the PCRF.
12	The PCRF updates the policy and charging rule with Charging-Rule-Base-Name or install new Charging-Rule-Base-Name.
13	The P-GW sends a CSG Information Reporting Action IE as part of the Modify Bearer Response, a Change Notification Response, or it can initiate a change through an Update Bearer Request.

Configuring Closed Subscriber Groups

CSG access control and status communication to peer MMEs/SGSNs is mandatory and enabled by default. CSG notification to the S-GW/P-GW is optional and may be enabled using the **csg-change-notification** CLI command within the scope of the mme-service configuration.

Use the following example to enable CSG change notification to the S-GW/P-GW.

```
configure
    context context_name
        mme-service mme_svc_name -noconfirm
            csg-change-notification
            end
```

Notes:

- By default, **csg-change-notification** is disabled and the MME does not send CSG notification to the S-GW/P-GW.

Verifying the Closed Subscriber Groups Configuration

Use either of the following Exec mode commands to verify if CSG notification to the S-GW/P-GW is enabled.

show mme-service all
show mme-service name *mme_svc_name*

The output of these commands displays the entire configuration for either all the MME services or just for the one specified. The output sample below only illustrates the line used to indicate the Closed Subscriber Groups (CSG) configuration status.

```
[local]asr5x00 show mme-service name mmesvc1
CSG Change Notification             : Enabled
```

Monitoring and Troubleshooting Closed Subscriber Groups

CSG information and per-PDN CSG reporting information is included the following Exec mode command.

show mme-service session full all
The sample output below shows only the information relating to CSG.

```
[local]asr5x00 show mme-service session full all
      CSG Cell Change Notification:  Enabled
            CSG Subscribed Hybrid Cell Change Notification:  Enabled
            CSG Unsubscribed Hybrid Cell Change Notification:  Enabled
      CSG Information:
            CSG ID at last connection: 15625 (0x3d09)
      CSG cell type: Hybrid
      CSG membership status: Non-Member
```

If the CSG cell is not a hybrid cell, the CSG Information section will be displayed as follows:

```
      CSG Information:
            CSG ID at last connection: 15625 (0x3d09)
      CSG cell type: Closed
      CSG membership status: Member
```

If the last (or current) cell is not a CSG cell, the CSG Information section will be displayed as follows:

```
      CSG Information:
            CSG ID at last connection: None
      CSG cell type: n/a
      CSG membership status: n/a
```

The following command shows CSG IDs from the subscription data:

show mme-service db record imsi `imsi_id`

```
      [local]asr5x00 show mme-service db record imsi 123456789012345
      CSG IDs                 : 10
                                25
                                625
```

If no CSG IDs are present in the subscription data, that state will be displayed as follows:

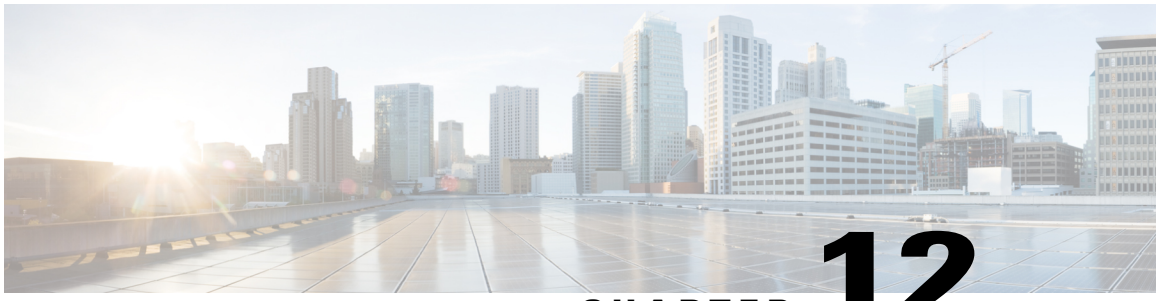
```
      CSG IDs                 : None
```

The following command shows statistics for the number of times the MME sent a NAS message with the cause value "Not authorized for this CSG". These statistics are tracked for Attach Reject, Detach Request, Service Reject, and TAU Reject.

The sample output that follows shows only the statistics relating to CSG.

show mme-service statistics

```
      [local]asr5x00 show mme-service statistics
Attach Reject:                      0
      ...
      CSG Not Subscribed:               0
Detach Request:                      0
      ...
      CSG Not Subscribed:               0
Service Reject:                      0
      ...
      CSG Not Subscribed:               0
TAU Reject:                     0
      ...
      CSG Not Subscribed:               0
```



CHAPTER 12

CSFB and SMS over SGs Interface

Circuit Switched Fallback (CSFB) provides an interim solution for enabling telephony and short message service (SMS) for LTE operators that do not plan to deploy IMS packet switched services at initial service launch.

Feature Description

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).

CSFB provides an interim solution for enabling telephony and SMS services for LTE operators that do not plan to deploy IMS packet switched services at initial service launch.

CSFB function is realized by reusing Gs interface mechanisms, as defined in 3GPP TS 29.018, on the interface between the MME in the EPS and the VLR. This interface is called the SGs interface. The SGs interface connects the databases in the VLR and the MME.

Important 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.

Supported Features

The following CSFB features are supported:

- Release 8 and Release 9 Specification Support
- SGs-AP Encode/Decode of all messages
- SGs-AP Procedure Support
  - Paging
  - Location Update
  - Non-EPS Alert
  - Explicit IMSI Detach
  - Implicit IMSI Detach
  - VLR Failure
  - HSS Failure
  - MM Information
  - NAS Message Tunneling
  - Service Request
  - MME Failure
- SMS
- Mobile Originating Voice Call
- Mobile Terminating Voice Call
- Gn/Gp Handover
- S3 Handover
- Basic and Enhanced TAI to LAI Mapping
- Basic LAI to VLR Mapping
- VLR association distribution among multiple MMEMGRs
- IMSI Paging Procedure
- SCTP Multi-homing for SGs interface
- IPv6 Transport for SGs interface
- SNMP Trap Support (Service/VLR association)
- Operator Policy Support
  - SMS-only
  - Disallow CSFB
  - Reject EPS if IMSI attach fails
  - Reject EPS if VoIMS and no CSFB
  - CSFB Not Preferred
  - Configurable RFSP based on UE Usage and and Voice Domain Preference

- PS Suspend/Resume over S11 (Release 8)
- PS Suspend/Resume over S3/S11 (Release 9)
- Support for SGs AP Timers: TS6-1, ts8, ts9, ts10, ts12-1, ts12-2, ts-13
- Idle mode Signaling Reduction (ISR)
- Multiple Association Support
- SNMP Trap Support
  - **VLRAssocDown** - sent when an SCTP association to a VLR is down.
  - **VLRDown** - sent when **all** SCTP associations to a VLR are down.
  - **VlrAllAssocDown** - sent when **all** associations to **all** VLRs are down.
- Support for Passive VLR Offload: See *VLR Management*.
- Support for Active VLR Offload: See *VLR Management*.
- UE Detach on VLR Failure: See *VLR Management*.
- UE Detach on VLR Recovery: See *VLR Management*.

DSCP Marking for SGs Interface

SGs services provides the Differentiated Services Code Point (DSCP) marking functionality. DSCP marking helps in packet traffic management. DSCP marking can be performed on both IPv4 and IPv6 packets leaving the SGs interface.

Either the pre-defined DSCP values can be used for marking, or any arbitrary value ranging from 0x01 to 0x3F can be assigned. The default DSCP value is 0x00 or be (Best Effort). The default DSCP value is automatically set when the configuration is disabled.

config
  context *context_name*
    sgs-service *service_name*
      [no] ip qos-dscp *dscp_value*
      end

- ip defines the Internet Protocol parameters for the packets leaving through the SGs interface.
- qos-dscp designates the Quality of Service - Differentiated Services Code Point value to the packet leaving through the SGs interface.
- *dscp_value* is a value assigned to the packet for DSCP marking. The value can be a pre-defined DSCP value or an arbitrary value ranging from 0x01 to 0x3F.

How It Works

EPC core networks are designed for all IP services and as such lack intrinsic support for circuit switched voice and telephony applications. This presents challenges for those operators that do not plan to launch packet switched IMS core networks at initial service deployment. CSFB represents an interim solution to address this problem by enabling dual radio mobile devices (LTE/GSM/UMTS or CDMA1xRTT) to fallback to

GSM/UMTS or CDMA1x access networks to receive incoming or place outgoing voice calls. The next section presents highlights of the CSFB procedure.

Preparation Phase

- When the GSM/UMTS/LTE access terminal attaches to the EUTRAN access network, it uses combined attachment procedures to request assistance from the MME to register its presence in the 2G/3G network.
- The MME uses SGs signaling to the MSC/VLR to register on behalf of the AT to the 2G/3G network. The MME represents itself as an SGSN to the MSC and the MSC performs a location update to the SGSN in the target 2G/3G network.
- The MME uses the Tracking Area Identity provided by UE to compute the Location Area Identity it provides to the MSC.

Execution Phase: Mobile Terminated Calls

- When a call comes in at the MSC for the user, the MSC signals the incoming call via the SGs interface to MME.
- If the AT is an active state, the MME forwards the request directly to the mobile. If the user wishes to receive the call the UE instructs the MME to hand over the call to the 2G/3G network. The MME then informs the eNodeB to initiate the handoff.
- If the AT is in dormant state, the MME attempts to page it at every eNodeB within the Tracking Area list to reestablish the radio connection. As no data transfer is in progress, there are no IP data sessions to handover and the mobile switches to its 2G/3G radio to establish the connection with the target access network.
- If the mobile is active and an IP data transfer is in progress at the time of the handover, the data transfer can either be suspended or the packet switched connection can be handed over if the target network supports Dual Transfer Mode. Note that this is typically only supported on UMTS networks.
- Once the access terminal attaches to the 2G/3G cell, it answers the initial paging via the target cell.

Execution Phase: Mobile Originated Calls

- This is very similar to the procedure for Mobile Terminated Calls, except there is no requirement for idle mode paging for incoming calls and the AT has no need to send a paging response to the MSC after it attaches to the target 2G/3G network.

Configuring CSFB over SGs

The configuration example in this section creates an SGs interface and an SGs service for communicating with a Mobile Switching Center/Visitor Location Register (MSC/VLR) for Circuit- Switched Fallback capability.

Important Circuit-Switched Fallback (CSFB) is a licensed feature and requires the purchase of the Circuit Switched Fallback feature license to enable it.

Use the following configuration example to enable CSFB capability on the MME:

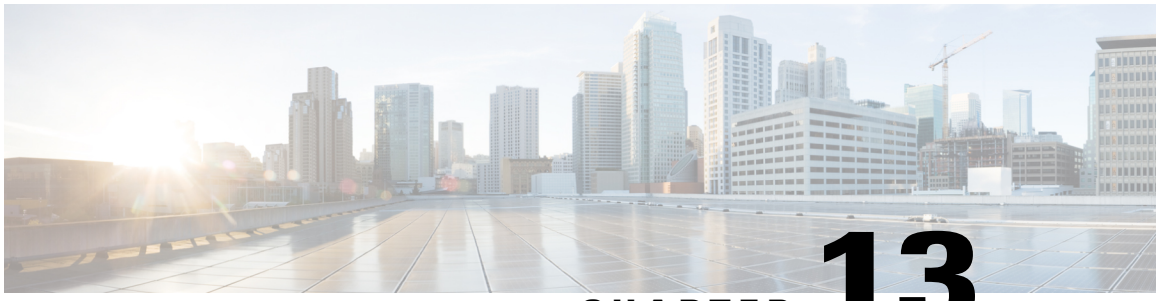
```
configure
    lte-policy
        tai-mgnt-db db_name
            tai-mgmt-obj object_name
                lai mcc number mnc number lac area_code
                tai mcc number mnc number tac  area_code
                end
    context mme_context_name -noconfirm
        interface sgs_intf_name
            ip address ipv4_address
            exit
        sgs-service name -noconfirm
            sctp port port_number
            tac-to-lac-mapping tac value map-to lac value +
            vlr vlr_name ipv4-address ip_address port port_number
            pool-area pool_name
                lac area_code +
                hash-value non-configured-value use-vlr vlr_name>
                hash-value range value to value use-vlr vlr_name
                exit
            bind ipv4-address sgs-intf_ipv4_address
            exit
        mme-service service_name
            associate tai-mgmt-db db_name
            associate sgs-service sgs_svc_name
            end
```

Notes:

- The MME will attempt to map a TAI to LAI in the following order:
  - If a TAI Management Database is configured, the MME will first use any TAI to LAI mapping defined within the database.
  - If no TAI Management Database is configured or if no suitable mapping is found within the TAI Management Database, the MME will next attempt to map a specific TAC to a specific LAC as defined in the SGs service according to the **tac-to-lac-mapping** command.
  - Lastly, the MME will attempt to use the default LAC value. This is defined using the **tac-to-lac-mapping** command with the **any-tac** keyword option.
- In this release, the number of TAC to LAC mappings is increased from 512 to 1024 entries.
- For the SGs interface, the **tac-to-lac-mapping** command supports the configuration of multiple TAC-to LAC values in the same configuration line.
- The SGs IP address can also be specified as an IPv6 address. To support this, the **ip address** command can be changed to the **ipv6 address** command and the **bind ipv4-address** command can be changed to **bind ipv6-address** command.

This command also allows for the configuration of a secondary IP address in support of SCTP multi-homing.

- The VLR interface (**vlr** command) also supports IPv6 addressing and SCTP multi-homing.



CHAPTER 13

CSFB for 1xRTT

The MME supports circuit-switched fallback (CSFB) for CDMA2000 1x (single-carrier) radio transmission technology (1xRTT) networks as defined by 3GPP TS 23.272 R10.

CSFB for 1xRTT Feature Description

The primary purpose of circuit-switched fallback (CSFB) for 1xRTT is to take the CDMA2000 messages received from the caller's phone (UE) and relay them to the CSFB interworking solution function for 3GPP2 (1xCS IWS) associated with the mobile switching center (1x RTT MSC) (or vice-versa) through S1-APP and S102 interfaces. This ensures the UE moves seamlessly from an LTE network to a CDMA2000 network.

The MME uses the S102 interface to tunnel the 1xRTT messages between the MME and IWS/MSC to support the following CS services:

- MO/MT Voice calls
- MO/MT SMS
- Emergency calls

This feature requires that a valid license key be installed to use the commands to configure this functionality. Speak with your Cisco Representative for information about this license. For information about the commands and their use, refer to the *Configuring CSFB for 1xRTT* section later in this chapter.

Supported Features

The MME provides the following features in support of CSFB for 1xRTT functionality:

MSC Pool Areas: Multiple MSCs would be handled by pooling all the MSCs mapping to a particular cell for load distribution. MSC pool areas can be configured for load balancing and intelligent selection of MSC servers based on IMSI hash values. Up to 10 MSC servers can be defined per S102 service.

MSC Non-Pool Areas: MSC selection, based on local MSC configuration.

MSC Selection: If an MSC pool area has been configured, the selection logic for the pool area is based on the CDMA2000 sector cell ID (includes the MSC ID and the Cell ID) in the CDMA2000 1xRTT network

Both the MSC ID and the cell ID are used to locate the pool / non-pool area. The MME attempts to select an MSC using the following selection order:

1 The MME attempts to match the MSC ID and the Cell ID:
   - If the match is found in the non-pool area configuration, then the configured MSC is selected.
   - If the match is found in the pool area configuration,
     - then IMSI hashing is used to select the MSC.
     - if no hash corresponds, then the MSC selected is the one configured for the 'non-configured-values'.

2 If no MSC is found, a failure message is returned.

Important When the UE attaches with IMEI, the MSC configured for the non-pool area is always selected because IMSI hashing cannot be performed for that UE.

DSCP Marking for S102 Interface

S102 interface allows Differentiated Services Code Point (DSCP) marking functionality. DSCP marking helps in packet traffic management. DSCP marking can be performed only on IPv4 packets leaving the S102 interface.

Either the pre-defined DSCP values can be used for marking, or any arbitrary value ranging from 0x01 to 0x3F can be assigned. The default DSCP value is 0x00 or be (Best Effort). The default DSCP value is automatically set when the configuration is disabled.

```
config
    context context_name
        S102-service service_name
            [no] ip qos-dscp dscp_value
            end
```

- ip defines the Internet Protocol parameters for the packets leaving through the S102 interface.
- qos-dscp designates the Quality of Service - Differentiated Services Code Point value to the packet leaving through the S102 interface.
- *dscp_value* is a value assigned to the packet for DSCP marking. The value can be a pre-defined DSCP value or an arbitrary value ranging from 0x01 to 0x3F.

Relationships to Other Features

CSFB for 1xRTT is related to the SRVCC for 1xRTT feature. Each requires a separate license to take advantage of the separate functionality and use the configuration commands.

If licenses for both features are installed in the system and both features are configured, then the MME can use the S102 interface for both CSFB for 1xRTT and SRVCC for 1xRTT.

1xRTT CSFB and 1xRTT SRVCC calls will be decided based on the presence or absence of the CDMA2000 1xRTT SRVCC Info IEs in an UPLINK S1 CDMA2000 TUNNELING message. This IE should not present for a 1xRTT CSFB call. If only one feature is licensed and configured and if the above condition is not appropriately satisfied for any received call, then that call will be dropped.

The SRVCC for 1xRTT feature is described elsewhere in this administration guide.

How It Works

Multiple components enable the MME to support CSFB for 1xRTT.

S1-App

The MME's CSFB for 1xRTT feature complies with 3GPP 36.413 Section 8.8, which define S1 CDMA2000 Tunneling Procedures to carry CDMA2000 signaling between a UE and a CDMA2000 RAT over S1 interface to perform:

- signaling for preparation for handover from the E-UTRAN to the CDMA2000 /1xRTT, and
- pre-registration and paging of the UE with the CDMA2000 1xRTT CS system.

These procedures use an established UE-associated logical S1-connection.

The CDMA2000 Tunneled messages are packaged and transported in the following messages:

- DOWNLINK S1 CDMA2000 TUNNELING: If a CDMA2000 message needs to be sent from an MME to a given UE, the MME uses an existing S1 connection. The MME sends a DOWNLINK S1 CDMA2000 TUNNELING message, which includes the CDMA2000 message in a CDMA2000-PDU IE. Similarly, the MME sends other IE's, such as the CDMA2000 HO Status IE during Handover, through the DOWNLINK S1 CDMA2000 TUNNELING message.
- UPLINK S1 CDMA2000 TUNNELING: When the eNB receives a CDMA2000 message intended for a UE, the eNB determines which MME has an existing UE-associated logical S1 connection. The eNB sends the UPLINK S1 CDMA2000 TUNNELING message to the MME. The UPLINK S1 CDMA2000 TUNNELING message includes the CDMA2000 message for the UE in the CDMA2000-PDU IE.

S102-App

Messages for the S102

The MME's S102 application is based on the UDP/IP transport medium. S102 (MME-to-IWS) /udp/23272 is the registered destination UDP port number to be used for signaling interconnection between an MME and an IWS for the S102 application.

The S102 application defines a set of messages between the MME and 1xCS IWS to provide CSFB. The MME uses a bound S102 interface to pass signaling messages (A21 messages) between the UE and the IWS:

- **A21-1x Air Interface Signaling message**: When the MME receives an Uplink CDMA2000 message from the eNB, the MME sends an A21-1x air interface message to 1xCS IWS. The MME encapsulates the 1x air interface message in an A21-1x air interface signaling message and sends it to the 1xCS IWS via the S102 interface. This message type is used by the MME or 1xCS IWS during registration, paging, and mobile-originated / mobile-terminated SMS procedures.
- **A21-Ack message**: This message is sent from an MME or a 1xCS IWS to acknowledge receipt of some A21 message to the peer 1xCS IWS or MME. The Correlation ID in an A21-Ack message is copied from the Request message to which the MME or 1xCS IWS is replying.
- **A21-Event Notification message**: This message is sent by either the MME or the 1xCS IWS to notify the peer node of a specific event. The "S102 Redirection" value is used to indicate S102 tunnel redirection during MME relocation.

A21 Network/Transport Messaging Procedures.

The destination port number is set to 23272 in the UDP packet that carries an A21-1x Air Interface Signaling message or an A21-Event Notification message.

The receiver of an A21-1x Air Interface Signaling message or of an A21-Event Notification message shall set the source port and source IP address and the destination port and destination IP address of the UDP packet that carries the corresponding A21-Ack message to the destination port / destination IP address and the source port / source IP address of the UDP packet that carried the A21-1x Air Interface Signaling message or the A21-Event Notification message respectively.

MME-App

The UE performs the 1x-RTT pre-registration when it successfully attaches and then:

1. The MME receives an S1-UPLINK CDMA2000 message in ATTACHED state from the eNB.
2. The MME sends an A21 Air Interface message via the S102 interface to the IWS/MSC.
3. The MME receives an A21 message from the IWS/MSC.
4. The MME sends an S1 Downlink CDMA2000 message to the eNB.

The MO/MT call or SMS are handled in Idle and Connected modes:

- In Connected mode, the EMM FSM will be in REGISTERED CONNECTED state. In this state, the messages from the MSC through the S102 messages are directly dispatched over the S1 interface through S1 DOWNLINK CDMA2000 messages.

- In Idle mode, when an MT-call or an MT-SMS arrives from an MSC, the MME needs to trigger paging to make the UE return to CONNECTED state. During this time, S102 message is stored inside the S102 context. Once the UE returns to connected state the message is dispatched over the S1 interface.

Other Support Functions

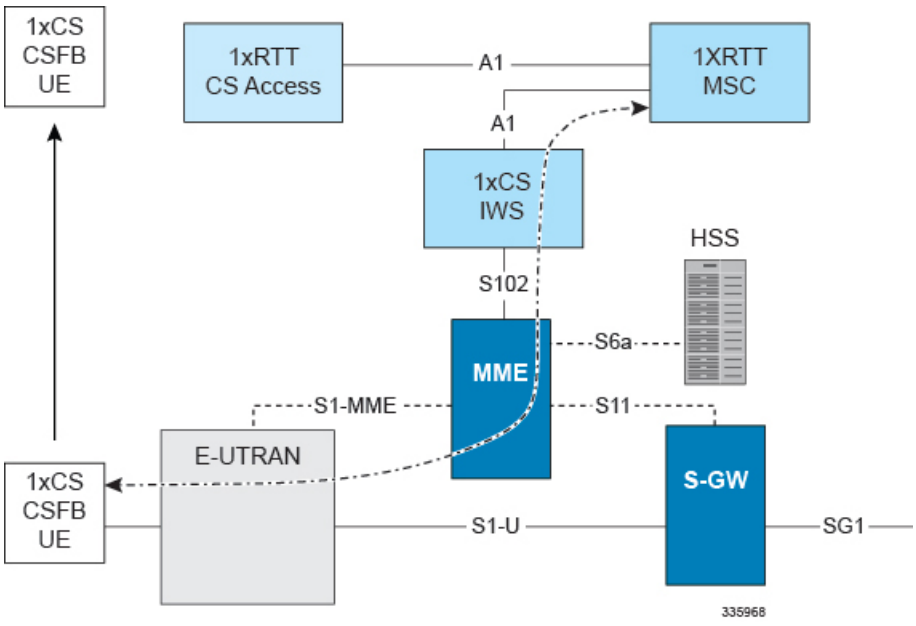
Attach Procedure: As parts of the existing Attach procedure, the 1x RTT UE includes an indication of support for enhanced CSFB to 1xRTT. The UE context will be updated with this information for further processing.

TAU Procedure: The 1xRTT UE performs the Tracking Area Update with the MME change. After Location Update Ack is received from the HSS, theMME sends a Context Request to the old MME and the 1x CS IWS ID is sent back in the Context Response message. This information would be stored in the UE's context and would be used when the CSFB procedure performs S102 Tunnel Redirection.

eGTPC: Whenever there is a change of MME, the target MME gets the IWS-ID (the MSC address) through the Context Response message from the source MME. In the case of SRNS relocation, the source MME send the IWS-ID (the MSC address) through the Forward Relocation Request message, which is stored in the UE context and will be used in the S102 Redirection procedures.

Architecture

Figure 11: Architecture of the MME s CSFB for 1xRTT



Flows

The following call flows are supported as defined by 3GPP TS 23.272, "Circuit Switched (CS) fallback in Evolved Packet System (EPS)":

- 1xRTT CS Pre-Registration
- S102 Tunnel Redirection
- UE-Initiated Detach Procedure
- MO Call - Normal CSFB to 1xRTT
- MO Call - enhanced CSFB to 1xRTT
- MT Call - Normal CSFB to 1xRTT
- MT Call - enhanced CSFB to 1xRTT
- Emergency Call
- SMS Procedures

Limitations

- SMS procedures will only apply if the UE is 1xRTT CS registered and the CS access domain is chosen by the UE and/or the home PLMN for delivering short messages.
- The MME only buffers the last received SMS until the UE returns to connected state.

Standards Compliance

The CSFB for 1xRTT complies with the following standards:

- 3GPP TS 23.401 Release 10, "GPRS enhancements for E-UTRAN access "
- 3GPP TS 23.402 Release 10, "Architecture enhancements for non-3GPP accesses"
- 3GPP TS 36.413 Release 10, "Evolved Universal Terrestrial Radio Access Network (E-UTRAN) S1 Application Protocol (S1AP)".
- 3GPP TS 23.272 Release 10, "Circuit Switched (CS) fallback in Evolved Packet System (EPS)"
- 3GPP2 A.S0008-C Release 3.0, "Interoperability Specification (IOS) for High Rate Packet Data (HRPD) Radio Access Network Interfaces with Session Control in the Access Network".
- 3GPP2 A.S0009-C Release 3.0, "Interoperability Specification (IOS) for High Rate Packet Data (HRPD) Radio Access Network Interfaces with Session Control in the Packet Control Function".
- 3GPP2 A.S0013-D Release 3.0, "Interoperability Specification (IOS) for cdma2000 Access Network Interfaces"

Configuring CSFB for 1xRTT

If you have the appropriate license, you will be able to see and configure the commands identified below to

- setup an S102 service for the use of an S102 interface.
- associate the S102 service configuration with the MME service.

- configure MSC selection.
- allow/disallow CSFB service and/or SMS-only service via an Operator Policy.

Important The first three sets of configuration must be completed for this feature to function.

Important For more details on commands and keywords indicated below, we recommend that you refer to the *Command Line Interface Reference, StarOS Release 19* or higher.

Configuring the S102 Service

This configuration enables you to define the characteristics for a specific S102 interface as an S102 service instance, including:

- configuring the interface to work with CSFB for the 1xRTT CDMA2000 messaging.
- binding or unbinding a logical IPv4 address and ports to the S102 service.
- configuring an IPv4 address and ports for the IWS/MSC in the S102 service configuration.

```
configure
    context context_name
        [ no ] s102-service service_name
            [ no ] 1xRTT csfb
                [ no ] bind ipv4-address ipv4_address port port_number
                [ no ] msc msc_name
                    [ no ] ipv4-address ipv4_address port port_number
                    exit
                [ no ] msc msc_name
                    [ no ] ipv4-address ipv4_address port port_number
                    end
```

Notes:

- *context_name* enter a string of 1 to 79 alphanumeric characters to define the name of the context in which the S102 service is configured. You can configure the S102 service in the same context in which the associated MME service is configured.
- *service_name* enter a string of 1 to 63 alphanumeric characters to define the name. We recommend that each service name be unique on this MME.
- The MME supports configuration of an undefined number of S102 services (interfaces). As there is a 1-to-1 correlation between S102 service configurations and MME services, the only limiting factor is the maximum number of MME services that can be configured per system maximum number is 8.
- **1xrtt** configures the S102 interface to provide either CSFB or SRVCC capabilities for the 1xRTT CDMA2000 network The 1xrtt command can be repeated so that a single S102 interface provides both CSFB and SRVCC functionality.
- **bind ipv4-address** *ipv4_address* **port** *port_number* binds the S102 interface to the specified source (MME) IPv4 interface address, and optionally to a specific port number if the port option is included.

The value for the IPv4 address must be entered in standard IPv4 dotted-decimal notation and, if included, the port number must be an integer from 1 to 65535.

- **msc** *msc_name* enter 1 to 63 alphanumeric characters to define a unique name for the MSC. Executing the msc command causes the system to enter the S102-MSC configuration mode to define the target IPv4 address (and optionally the port ID). This associates the S102 interface to the specified MSC.
- **ipv4-address** *ipv4_address* **port** *port_number* identifies IPv4 interface address of the MSC, and optionally a specific port number if the port option is include. The value for the IPv4 address must be entered in standard IPv4 dotted-decimal notation and, if included, the port number must be an integer from 1 to 65535.
- It is possible to associate up to 10 IWS/MSCs with the S102 interface/service configuration. Repeat the **msc**, **ipv4-address**, and **exit** commands sequence as often as needed to identify all MSCs.
- **no** prefix included with a command, disables and/or erases the specified configuration from the MME's configuration.
- **default** prefix is unused at this time and is available for future development.

Verify the S102 Service Configuration

Use the **show s102-service name** *s102_service_name* command to verify the S102 configuration that you have entered following the steps outlined above. The output will appear *similar* to the following:

```
[local]MME show s102-service name s102-mme1
Service name      : s102-mme1
Context           : test
Status            : NOT STARTED
1xRTT type        : CSFB
Bind              : Done
IP Address        : nnn.nnn.nnn.1
Port              : 54321
```

Associating the S102 Service

Use the following to add an association between a previously configured MME service and an S102 service.

config
context *context_name*
mme-service *mme_service_name*
associate s102-service *s102_service_name* **[context** *context_name* **]**
end

Notes:

- **context** *context_name* enter a string of 1 to 79 alphanumeric characters to identify the name of the context in which the S102 service is configured. We recommend that you identify the context if it is not the same one in which the associated MME service is configured.

Verifying the S102 Association

Use the **show mme-service name** *mme_service_name* command to verify the S102 association that you have entered following the steps outlined above. The output will appear *similar* to the following:

```
[local]MME show mme-service name mme1
Service name                          : mme1
Context                               : test
Status                                : NOT STARTED
Bind                                  : Not Done
. . .
. . .
IPNE Service                          : Not defined
S102 Context                          : test
S102 Service                          : s102-A
Max bearers per MS                    : 11
. . .
. . .
```

Configuring MSC Selection

The following process configures up to 10 MSC pool/non-pool areas per S102 service in support of MSC selection. Both the MSC-Id and the Cell-Id are used to locate the pool or non-pool area for the MSC selection process.

Prerequisite: Each of the MSCs must have been defined and associated with an S102 service (see *Configuring the S102 Service* noted above) before the MSC can be included in the non-pool-area or pool-area configuration.

Defining a Non-Pool Area

config
context *context_name*
[no] s102-service *service_name*

Important The **plmn** option that is visible in the code is not supported at this time and is included for future development.

non-pool-area *non_pool_area_name* **msc** *msc_name* **msc-id** *msc_id* **cell-id** *cell_id +*
no non-pool-area *non_pool_area_name* **cell-id** *cell_id +*
Notes:

- *non_pool_area_name* enter a string of 1 to 63 alphanumeric characters to uniquely identify the non-pool-area definition used for MSC selection.
- **msc** *msc_name* enter a string of 1 to 63 alphanumeric characters to identify one of the MSCs previously configured in the S102 service configuration.
- **msc-id** *msc_id* **cell-id** *cell_id +*
  - *msc_id* enter an integer from 1 through 16777215 to identify the unique numeric ID for the MSC.
  - *cell_id +* enter an integer from 1 through 65535 to identify a CDMA2000 sector cell ID that you are assigning to this non-pool area configuration. Enter up to 24 cell IDs, separated by a single blank space, in the same command.

- **plmnid { any | mcc** *mcc_id* **mnc** *mnc_id* **}** is not operationally supported at this time. The code is included for future development.
- **no** prefix included with the command, erases or disables the specified configuration from the MME's configuration.

Defining a Pool Area

config
context *context_name*
[no]s102-service *service_name*
[no] pool-area *pool_area_name*
[no] cell-id *cell-id cell-id*
[no] hash-value { *hash_value* | **non-configured-values** | **range** *lower_hash_value* **to** *higher_hash_value* } { **msc** *msc_name* }
[no] msc-id *msc-id*
[no] plmnid { any | mcc *mcc_id* **mnc** *mnc_id* **}**
end

Notes:

- **pool-area** *pool_area_name* enter a string of 1 through 63 alphanumeric characters to create a unique name of an MSC pool area configuration. After the command is entered, the system enters the S102-Pool-Area configuration mode.
- **cell-id** *cell-id* **[***cell-id* **+]** enter an integer from 1 through 65535 to identify a CDMA2000 sector cell ID that you are assigning to this pool area configuration. Enter up to 24 cell IDs, separated by a single blank space, in the same command.
- **hash-value**
  - *hash_value* enter an integer from 0 through 999 to identify a specific MSC.
  - **non-configured-values msc** *msc_name* assigns all non-configured hash values to use the named MSC.
  - **range** *lower_hash_value* **to** *higher_hash_value* **msc** *msc_name* specifies the range of hash values for an MSC:
    - *lower_hash_value* enter an integer from 0 through 999 to identify the start value for a range of hash. The *lower_hash_value* must be lower than *higher_hash_value*.
    - *higher_hash_value* enter an integer from 0 through 999 to identify the end value for a range of hash. The *higher_hash_value* must be higher than *lower_hash_value*.
- *msc_id* enter an integer from 1 through 16777215 to identify the unique numeric ID for the MSC.
- **plmnid { any | mcc** *mcc_id* **mnc** *mnc_id* **}** is not operationally supported at this time. The code is included for future development.
- **no** prefix included with the command, erases the specified configuration from the MME's configuration.

Verifying Pool and Non-Pool Area Configuration

Use the **show configuration** command to view the S102 pool area and S102 non-pool area configuration. It should appear similar to the following:

```
[local]MME show configuration
 ...
     s102-service s102test
      bind ipv4-address 123.123.123.1 port 54321
      1xrtt CSFB
      msc msc1
        ipv4-address nn2.nn2.nn2.2 port 33333
      exit
      msc msc10
        ipv4-address nn1.nn2.nn1.2 port 23272
      exit
      pool-area poolone
        cell-id 2 4 5
        hash-value 34 msc msc10
      exit
      non-pool-area np1 msc msc1 msc-id 1233 cell-id 223
      non-pool-area np3 msc msc1 msc-id 14441 cell-id 6 7 8
```

Allowing CSFB and/or SMS-only in the Operator Policy

The operator can configure the type of CSFB service the MME provides at the Operator Policy level.

Enabling SMS-only

The following configuration sequence instructs the MME that the CSFB function will only support SMS.

config
call-control-profile *ccprof_name*
[remove] csfb sms-only
end

Notes:

- **remove** prefix included with the command, erases the specified configuration from the Call-Control Profile configuration.

Enabling CSFB for Voice and SMS

The following configuration sequence instructs the MME that the CSFB function is

- not allowed for both voice and SMS, or
- only allowed for SMS.

config
call-control-profile *ccprof_name*
[remove] csfb policy { not-allowed | sms-only }
end

Notes:

- **remove** prefix included with the command, erases the specified configuration from the Call-Control Profile configuration.

Verifying the Call-Control Profile Configuration

Use the **show call-control-profile full name** command to display the configuration entered with the procedures outlined above. The output should appear similar to the following:

```
[local]MME show call-control-profile full name ccprof1
Call Control Profile Name = ccprof1
SAMOG Home PLMN                                                    : Not configured
CSFB Restrictions
     SMS Only                                                      : TRUE
     Not Allowed                                                   : FALSE
```

Monitoring and Troubleshooting the CSFB for 1xRTT

Monitoring Protocol

When using the monitor protocol command, enable option 86 to see all A21 messages.

Show Command(s) and/or Outputs

show s102-service statistics name

The show **s102-service statistics name** *s102_service_name* command generates statistical output indicating the status and activity of the interface. The output generated will appear similar to the following:

```
S102-AP Statistics:
  S102-AP Data:                                Tx    ReTx    Rx
    A21-1x Air Interface Signaling message     0      0      0
     A21-Ack message                           0      0      0
Unknown MSG                                    0      0      0
Error Statistics:
  Encoding Errors:                                0
  Mismatch in Correlations:                       0
  Decoding Errors:                                0
    Missing Mandatory IEs:                        0
    Syntax Errors:                                0
  Misc Errors:                                    0
```

Bulk Statistics

Bulk statistics are described in the *Statistics and Counters Reference*.

MME Schema

The MME tracks the number of CSFB 1xRTT calls using the following variables:

- s1ap-transdata-dlinktunnel
- s1ap-recdata-ulinktunnel

S102 Schema

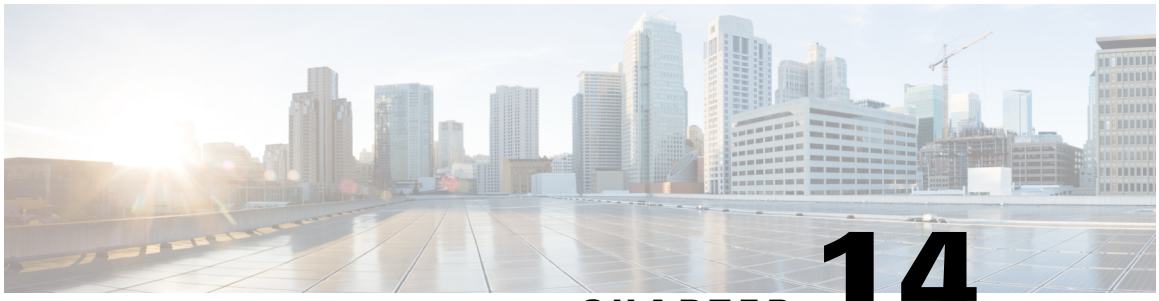
The MME will use the S102 interface to tunnel the 1xRTT messages between the MME and IWS/MSC. The S102 schema has been created to track performance over this interface and includes all of the following stat variables (which are described in detail in the *Statistics and Counters Reference*) :

- vpnname
- vpnid
- servname
- servid
- s102ap-tx-a21-air-signal-msg
- s102ap-tx-a21-ack-msg
- s102ap-tx-a21-evt-ntfy-msg
- s102ap-tx-unknown-msg
- s102ap-retx-a21-air-signal-msg
- s102ap-retx-a21-ack-msg
- s102ap-retx-a21-evt-ntfy-msg
- s102ap-retx-unknown-msg
- s102ap-rx-a21-air-signal-msg
- s102ap-rx-a21-ack-msg
- s102ap-rx-a21-evt-ntfy-msg
- s102ap-rx-unknown-msg
- s102ap-encode-errors
- s102ap-missing-mandatory-ies
- s102ap-corelation-mismatch
- s102ap-decode-errors
- s102ap-syntax-errors
- s102ap-misc-errors

Traps

Traps are defined to indicate when an S102 service starts or stops. The trap information includes the context identification in which the S102 service is configured the unique identification of the S102 service. The following are examples of how the traps would appear :

```
Internal trap notification <XXXX> (S102ServiceStop) context S102 service s102-service
Internal trap notification <YYYY> (S102ServiceStart) context S102 service s102-service
```



CHAPTER 14

DDN Throttling

Feature Description

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

MME supports the following functions for DDN Throttling:

- Rejection of DDN requests when configured congestion threshold is reached.
- Allows the configuration of cause value to be sent in DDN Ack message when DDN is rejected during congestion.
- Allows DDN rejection based on ARP.
- Allows DDN rejection based on LAPI.
- Allows configuration of DDN throttling factor and throttling delay values to be sent in DDN Ack message to SGW during congestion.

A valid license key is required to enable DDN Throttling. Contact your Cisco Account or Support representative for information on how to obtain a license.

How It Works

The SGW determines whether a bearer needs DDN throttling based on the bearer's ARP priority level and operator policy (operator's configuration in the SGW of the ARP priority levels to be considered as priority or non- priority traffic). While throttling, the SGW throttles the DDN Requests for low and normal bearers

based on priority. The MME determines whether a Downlink Data Notification request is priority or non-priority traffic on the basis of the ARP priority level that was received from the SGW and operator policy.

Congestion Control Profile supports DDN Throttling. The Congestion Control policy allows the operator to configure three different action profiles critical, major and minor based on the congestion level. During Congestion the operator configures the action to be taken using action profiles. Congestion Action profile allows configuration of DDN Throttling parameters.

When congestion threshold is reached the following actions are taken on DDN requests based on the operator configuration:

- Reject all DDN requests based on ARP and LAPI. DDN Ack message is sent with failure cause to the SGW. Paging is not initiated.
- Reject all DDN requests if ARP or LAPI values are not configured.
- Enable SGW Throttling. DDN Ack message is sent to the SGW with throttling factor and throttling delay values.

Session Manager

The Session Manager is configured to handle DDN requests based on the DDN's current congestion status and the operator configuration. Session Manager stores the congestion status information along with S1-AP or NAS messages received from the MME manager. This data is used to handle DDN requests.

The Session Manger handles congestion for incoming DDN requests in the following ways:

- If the congestion status does not indicate any congestion, session manager initiates paging without any change in existing behavior.
- If the congestion threshold is reached, session manager either decides to reject DDN requests or enable throttling DDN requests towards SGW, based on the action profile corresponding to the threshold level. A throttling factor and throttling delay is added to the DDN Ack message and is sent to the SGW. If DDN Rejection is based on **reject ddn** configuration then DDN Ack will not contain any throttling factor and throttling delay value.
- If the action profile indicates DDN requests to be rejected, the sessmgr does not initiate paging. A DDN Ack message is sent with the configured cause value. The default cause value is "Unable to page UE".
- If the action profile indicates throttling in SGW is enabled, then the sessmgr includes the throttling factor and the throttling delay value in the DDN Ack, which is sent to the SGW. If action profile indicates DDN requests to be rejected, then throttling parameters are not included in the DDN Ack message.
- If **reject ddn** is configured with arp-watermark, and if the PDN has multiple bearer and ARP values, the DDN requests are serviced depending on the following scenarios:
  - If DDN is received without bearer ID and ARP value, then the DDN requests are allowed and all bearers remain active. The DDN requests will not be rejected unless MME receives the ARP values and all bearers remain active, as part of the paging procedures.
  - If DDN is received with a bearer ID but not an ARP value, the DDN requests are still allowed and all bearers will be active as part of a paging procedure. But, if a stored ARP value matches with the configured arp-watermark value, DDN requests are rejected.

Important The action to reject DDN requests or enable SGW throttling is independent of each other. The operator can configure either or both actions for each action profile.

If there is a configuration change in DDN Throttling parameters, then the action is applied only upon receiving the next DDN request.

- If configuration is modified to disable throttling, then it will come into effect immediately while processing the next DDN. MME shall send throttling IE so that it de-activates the DDN throttling timer at SGW.
- If configuration is modified to change throttling values, throttling begins after a delay of few seconds. The new throttling value is sent to the SGW when the ongoing throttling time (timer = previously sent timestamp + new throttling delay) expires.

Important If the Session Manager crashes, the SGW list with throttling information is lost on recovery. In this condition, the throttling parameter information is sent to the SGW even before the ongoing throttling expires. If congestion persists after session manager recovery, the throttling parameters are sent again for recovery.

Limitations

Memory Impact -- There is a negligible impact on memory, which stores the SGW information created to process the incoming DDN throttling request. A list of SGW entries are created in this process. The following information is stored in the SGW:

- SGW IP address
- Congestion Status time at which throttling status were sent in the DDN Ack
- Timestamp Congestion status for which throttling information was last sent

The above mentioned information is required to keep the Session Manager in sync with the SGW's throttling status. However, to keep the memory impact minimal the SGW information list is created only during congestion and throttling factors are configured in the action profile. On completion of DDN throttling, congestion is cleared and the SGW entry in the list is deleted to process the subsequent DDN request.

Standards Compliance

The DDN Throttling feature complies with the following standards:

- 3gpp TS 29.274, Version 10.4.0, Tunneling Protocol for Control plane (GTPv2-C).
- 3gpp TS 23.401, Version 10.4.0, General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access.

Configuring DDN Throttling

This section documents the configuration procedures for DDN Throttling and related functionality.

Configuring DDN Throttling Factor and Throttling Delay

reject

The **ddn** is a newly added keyword to this command. This keyword allows the operator to reject DDN requests during congestion. The operator can reject DDN requests based on ARP or LAPI values or both. An option is provided to reject all DDN requests without using ARP/LAPI values.

configure
lte-policy
congestion-action-profile *profile_name*
reject ddn [arp-watermark *arpwatermark_value* **[cause** *cause_value* **] | cause** *cause_value* **| lapi [cause** *cause_value* **]]**
none ddn [lapi | arp-watermark]
end

Notes:

- The ddn keyword configures action to be taken for all DDN requests
- The lapi keyword indicates that DDN reject is applicable for UEs with LAPI.
- The arp-watermark keyword indicates that DDN reject is applicable for ARP values greater than or equal to the ARP specified. The ARP value ranges from 1 through 15.
- The cause keyword rejects DDN with the specified cause value. The valid cause value ranges from 1 through 255. The default value is 90 with the display message “Unable to page ue”.
- none disables DDN configuration.

Important If the value of arp-watermark does not match with the DDN's ARP value, then the DDN notifications is not rejected, and all bearers remain active.

ddn sgw-throttling

The **sgw-throttling**, **throttle factor** and **delay** are new keywords added to this command in this release. This Command allows the operator to configure the throttling factor and throttling delay values to be sent in DDN Ack message.

Important Throttling delay value will be converted internally to seconds, minutes or hours as defined in the 3gpp Spec 29.274.

configure
lte-policy
congestion-action-profile *profile_name*
ddn sgw-throttling throttle-factor *percentage_value* **delay** *delay_time*
no ddn sgw-throttling
end

Notes:

- The **sgw-throttling** keyword enables DDN throttling towards SGW.
- The **throttle-factor** keyword indicates throttling factor as a percentage from 1 to 100.
- The **delay** keyword indicates the amount of time taken for throttling delay in seconds. The delay value ranges from 2 to 1116000 seconds.
- **no** removes DDN throttling towards SGW.

Verifying the DDN Throttling Configuration

The following command displays the configuration fields in the Congestion Action Profile for the DDN Throttling feature:

```
show lte-policy congestion-action-profile name test
Congestion Action Profile test
none handovers
none combined-attaches
none ps-attaches
none addn-pdn-connects
none addn-brr-requests
none brr-ctxt-mod-requests
none service-request
none tau-request
none s1-setups
none init-ues
none ddn
ddn sgw-throttling throttle-factor 3 delay 1116000
none paging
no exclude-emergency-events
no exclude-voice-events
```

Monitoring and Troubleshooting DDN Throttling

This section provides information on how to monitor congestion control.

DDN Throttling Show Command(s) and/or Outputs

This section provides information regarding show commands and/or their outputs in support of enhanced congestion control.

show congestion-control statistics mme

The command generates a display that provides a concise listing of congestion control statistics. The command offers four keyword options: **critcal | full | major | minor**

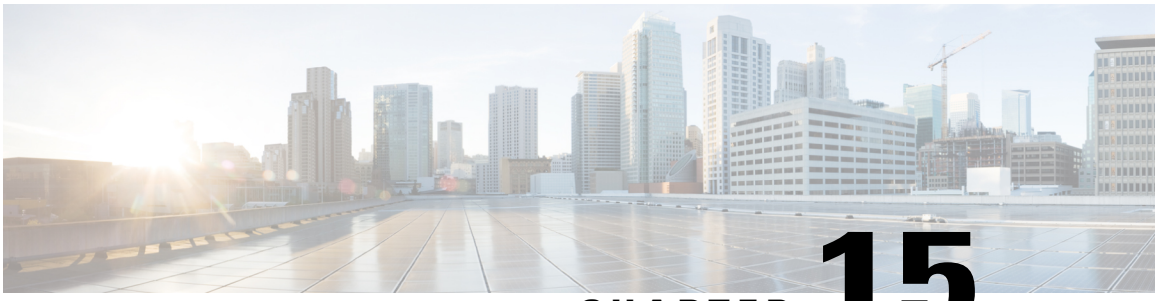
In the output example below, the critical keyword has been included in the command so only Critical information is shown. The displayed fields are the same when the full, major, or minor options are used with the command.

```
Critical Congestion Policy Action
    Congestion Policy Applied           :    0 times
    PS attaches
                    Rejected            :      0 times
                    Dropped             :      0 times
    PS attaches
                    Rejected            :      0 times
                    Dropped             :      0 times
    Combined attaches
                    Rejected            :      0 times
                    Dropped             :      0 times
    S1-Setup
                    Rejected            :      0 times
                    Dropped             :      0 times
    Handover
                    Rejected            :      0 times
                    Dropped             :      0 times
    Addn-pdn-connect
                    Rejected            :      0 times
                    Dropped             :      0 times
    Addn-brr-connect
                    Rejected            :      0 times
                    Dropped             :      0 times
    Service-Request
                    Rejected            :      0 times
                    Dropped             :      0 times
    TAU-Request
                    Rejected            :      0 times
                    Dropped             :      0 times
    S1AP Overload Start Sent            :      2 times
    S1AP Overload Stop  Sent            :      2 times
    Excluded Emergency Events           :      0 times
    Excluded Voice Events               :      0 times
    DDN Request
                    Rejected            :      0 times
                       ARP-Based        :      0 times
                       LAPI-Based       :      0 times
```

Notes:

- The DDN Request field indicates the number of DDN requests rejected based on the CLI configuration in the Congestion Action Profile.
- The Rejected field provides information on the total number of DDN rejections based on the CLI configuration.
- The ARP-based field indicates the number of DDN rejected based on the ARP value. For example, reject ddn arp-watermark 10 increments the counter once the ARP value of DDN requests received is 10 and above.
- The LAPI-Based field indicates the number of DDN rejected based on the LAPI value.

Important For LAPI based UEs, both cli are valid, it means if DDN rejection happened due to ARP-based condition then only ARP-based counter will be incremented.



CHAPTER 15

Default APN for DNS Failure

With Release 18.2, it is possible for the operator to configure the MME to use a default APN in some situations where the DNS resolution fails due to a problem with the subscriber-requested APN. As a result, the Attach could proceed or the PDP context activation could complete.

Feature Description

The Default APN for DNS Failure feature makes it possible for the operator to ensure that calls and PDP context activation are not rejected because of possible UE errors, such as, the UE requested a misspelled APN name. This feature allows the operator to promote activation success if

- the DNS query would fail

when

- the subscriber-requested APN is not present in the subscription record,

and if

- the wildcard subscription is present in the subscription record.

This functionality is configured with the use of the **require-dns-fail-wildcard** keyword. This keyword is currently supported only on MME.

By default, this new functionality is not enabled. If not enabled, then the MME sends a PDN connectivity reject to the eNodeB if the DNS resolution fails for the reasons indicated above.

Relationships to Other Features

Operator Policy - Default APN for DNS Failure is configured with the commands in the APN Remap Table configuration mode which is a key component of the Operator Policy feature. For information about this feature, see the chapter on *Operator Policy*.

How It Works

With the Default APN for DNS Failure enabled by configuring the 'required-dns-fail-wildcard', if DNS resolution fails because the UE-requested APN name is not present in the subscription record but the wildcard subscription is present, then MME overrides the requested APN with a configured default APN. The MME proceeds with the DNS resolution of the configured default APN and then proceeds with the Attach or PDP context activation.

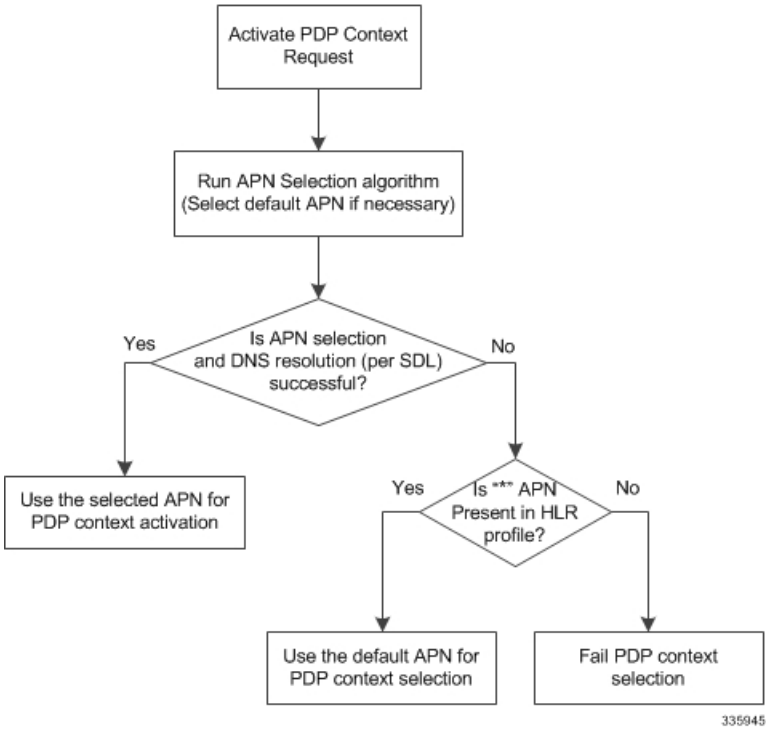
The MME checks the subscription record with the configured default APN. If subscription record of the configured default APN is available, then the MME takes the QoS profile and the ARP values from that record. If the subscription record is not available, then the MME checks the QoS profile and ARP values included in the wildcard subscription record.

Important Note that DNS query will be retried with default APN only once. If DNS resolution fails again, even after applying the configured default APN, then the Activation Request will be rejected.

Architecture

The graphic below illustrates the intenal procedure the MME follows to determine if a default APN should be used.

Figure 12: Decision Tree for MME Using Default APN



Standards Compliance

The Default APN for DNS Failure feature complies with the following standards:

- 3GPP TS 23.060
- 3GPP TS 36.413
- 3GPP TS 24.301
- 3GPP TS 29.274
- 3GPP TS 23.401

Configuring Default APN for DNS Failure

Enabling Default APN for DNS Failure is configured in the APN Remap Table configuration mode. This mode generates a remap table that is a key component of the Operator Policy feature. The operator policy

must be assigned subscribers in the LTE Policy, the LTE policy's subscriber map must be associated with the MME service.

Check the MME's current configuration for names of already created APN remap tables, operator policies, subscriber maps and mme-service instances. If desired, these names can be used to create associations *with pre-configured* tables, policies and services.

Important We recommend that all table, policy, and service names be unique - not only within a context but across the MME's configuration. Do not use preconfigured names unless the association is desired.

This configuration procedure will take you through all of the following:

1. creating an APN remap table and enabling 'require-dns-fail-wildcard',
2. creating an operator policy and associating the remap table with the operator policy,
3. associating the remap table with the operator policy,
4. assigning subscribers to the operator policy in the LTE policy,
5. associating the LTE policy's subscriber map to the MME service configuration.

All commands, keywords, and variables are defined in the *Command Line Interface Reference* for this release.

All components must be completed for the feature to be enabled. Begin this procedure in the Local context in the Exec mode.

Enabling 'require-dns-fail-wildcard'

The following configuration components deals with creating an APN Remap Table and configuring the special keyword specific to enabling the Default APN for DNS Failure feature.

config
apn-remap-table <*table_name*> **-noconfirm**
apn-selection-default network-identifier *net_id* **require-dns-fail-wildcard**
end

Notes:

- *net_id* - Specifies the network identifier to be used as the default APN name. Must be a string of 1 to 62 characters, including digits, letters, dots (.) and dashes (-).
- require-dns-fail-wildcard - The keyword that enables the use of the default APN when DNS resolution fails. This keyword is currently supported only on MME.
- **no** prefixed to the command will remove the require-dns-fail-wildcard configuration from the remap table.

Associating the APN Remap Table with the Operator Policy

The following configuration components deals with creating an operator policy or accessing the operator policy configuration to associate the APN remap table identified in the configuration procedure above.

config
operator-policy name <*policy_name*> **-noconfirm**
associate apn-remap-table <*table_name*>
end

Assigning Subscribers to the Operator Policy

The following configuration components deals with assigning subscribers to the operator policy in the LTE policy.

config
lte-policy
subscriber-map <*map_name*> **-noconfirm**
precedence *precedence* **match-criteria all operator-policy-name** <*policy_name*>
end

Associating the Subscriber's Map with the MME Service

The following configuration components deals with associating the LTE policy's subscriber map to the MME service configuration

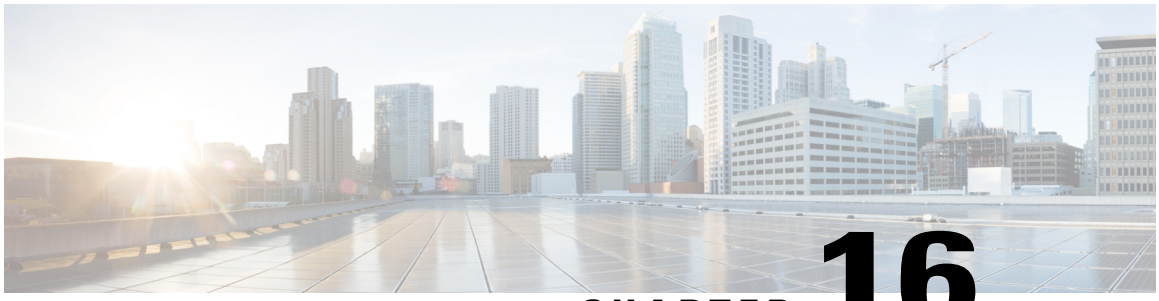
config
context *context_name* **-noconfirm**
mme-service <*srvc_name*> **-noconfirm**
associate subscriber-map <*map_name*>
end

Verifying the Feature's Configuration

The **show apn-remap-table full all** command generates a display that indicates the configuration for the APN Remap Table. The Use Default APN when DNS Query fails field indicates if the Default APN for DNS Failure feature has been enabled.

The following is a sample display is only a portion of the output and this sample shows *star.com* configured as the default APN name.

```
[local]asr5000 show apn-remap-table full all
APN Remap Table Name = test-table
Default APN                          : star.com
    Require Subscription APN                                  : Not Configured
        Use Default APN when no APN is requested              : Yes
        Use Default APN when DNS Query fails                  : Yes
        Fallback APN to use when Default APN not present
        in subscription                                       : Not Configured
        . . . .
```



CHAPTER 16

eDRX Support on the MME

This feature describes the Extended Discontinuous Reception (eDRX) support on the MME in the following sections:

Feature Description

The Extended Discontinuous Reception (eDRX) feature allows IoT devices to remain inactive for longer periods. This feature allows the device to connect to a network on a need basis – the device can remain inactive or in sleep mode for minutes, hours or even days, thus increasing the battery life of the device.

Extended DRX cycles provide UEs longer inactive periods between reading, paging or controlling channels.

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

How eDRX Works

In order to use the eDRX feature, the UE requests eDRX parameters during ATTACH and TAU procedures.

Based on the configuration, the MME may accept or reject the UE's request to enable the eDRX feature. If the MME accepts the eDRX request, different values of the eDRX parameters are provided based on operator policies, apart from the parameters requested by the UE.

eDRX Parameters

A Hyper-SFN (H-SFN) frame structure is defined for regular idle mode DRX. Each H-SFN value corresponds to a legacy SFN cycle comprised of 1024 radio frames (10.24 seconds). The eDRX consists of values that are a power of 2, ranging from 5.12 seconds (that is, 5.12, 10.24, 20.48 seconds and so on) up to a maximum of 2621.44 seconds (43.69 minutes). When EDRX is enabled for a UE, the UE is reachable for paging in specific Paging Hyperframes (PH), which is a specific set of H-SFN values. The PH computation is a formula that is function of the EDRX cycle, and a UE specific identifier. This value can be computed at all UEs and MMEs without need for signalling. The MME includes the extended idle mode DRX cycle length in paging message to assist the eNodeB in paging the UE.

The MME also assigns a Paging Time Window length, and provides this value to the UE during attach/TAU procedures together with the extended idle mode DRX cycle length. The UE first paging occasion is within the Paging Hyperframe. The UE is assumed reachable for paging for an additional Paging Time Window

length after first paging occasion. After the Paging Time Window length, the MME considers the UE unreachable for paging until the next Paging Hyperfame.

Loose Hyper SFN Synchronization

In order for the UE to be paged at roughly similar time, the H-SFN of all eNodeBs and MMEs should be loosely synchronized.

Each eNodeB and MME synchronizes internally the H-SFN counter so that the start of H-SFN=0 coincides with a preconfigured time. It is assumed that eNodeBs and MMEs are able to use the same H-SFN value with accuracy in the order of legacy DRX cycle lengths (For example, 1 to 2 seconds). There is no need for synchronization at SFN level.

There is no signaling between network nodes required to achieve this level of loose H-SFN synchronization.

Paging and Paging Retransmission Strategy

When the MME receives trigger for paging and the UE is reachable for paging, the MME sends the paging request. If the UE is not reachable for paging, then the MME pages the UE just before the next paging occasion.

The MME determines the Paging Time Window length based on paging retransmission strategy, and uses it to execute the retransmission scheme.

Standards Compliance

The eDRX feature complies with the following standards:

- 3GPP TS 23.682 version 13.4.0, Architecture enhancements to facilitate communications with packet data networks and applications (Release 13)
- 3GPP TS 24.302 version 13.5.0, Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3 (Release 13)
- 3GPP TS 23.401 version 13.5.0, General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access.

- 3GPP TS 29.274 version 13.5.0, 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunneling Protocol for Control plane (GTPv2-C); Stage 3

Limitations and Restrictions

The eDRX feature is compatible only with IoT devices. It is not available for all Mobile Stations (MS), that is, only those MSs and their respective Base Service Stations (BSS) that have the extended coverage parameters are supported by the SGSN.

Configuring eDRX on the MME

Enabling eDRX on MME

The following CLI configuration enables the eDRX feature on the MME.

The below configuration is available under the Call Control Profile Configuration mode.

configure
call-control-profile *profile_name*
edrx { ue-requested | ptw *ptw_value* **edrx-cycle** *cycle_length_value* **[dl-buf-duration [packet-count** *packet_count_value* **]] }**
remove edrx
end

Notes:

- **remove**: disables the eDRX configuration on the MME.
- **edrx** : configures Extended Discontinuous Reception parameters.
- **ue-requested** : specifies the accepted UE requested values of the eDRX cycle length .
- **ptw** : specifies the Paging Time Window (PTW) value received from the UE in the Attach Request/TAU Request message. The PTW value is an integer ranging from 0 to 20 seconds.
- **edrx-cycle** : specifies the accepted UE requested values of the Paging Time Window and the eDRX Cycle Length.
- **dl-buf-duration**: sends Downlink Buffer Duration data in the DDN ACK message when MME is unable to page the UE.
- **packet-count** : send DL Buffering Suggested Packet Count data in DDN ACK when MME is unable to page the UE.
- MME sends Downlink Buffer Duration IE in Downlink Data Notification Acknowledgment message to the gateway when MME is unable to page the UE.
- MME sends Downlink Buffering Suggested Packet Count value to gateway in Downlink Data Notification Acknowledgment message when MME is unable to page UE. the packet count is an integer that ranges from 0 to 65535.

Verifying eDRX on the MME

The below given command displays the following new fields that are added to support the eDRX feature:

show call-control-profile full name *cp_name*

```
Extended DRX:
    Paging Time Window                                    : 10 Seconds
    eDRX Cycle Length                                     : 512 Seconds
    Downlink Buffer Duration in DDN Ack                   : Enabled
    DL Buffering Suggested Packet count in DDN Ack        : 10
```

Configuring Hyper SFN Synchronization

The following CLI allows to configure the Hyper SFN Synchronization start time.

configure
context *context_name*
mme-service *service_name*
edrx hsfn-start *UTC_Time*
no edrx hsfn-start
end

Notes:

- The **no** option disables the H-SFN synchronization time configuration.
- The **edrx** command specifies the Extended Discontinuous Reception H-SFN start time.
- The **hsfn-start** keyword specifies the UTC Time at which H-SFN=0 starts. The time should be entered in the UTC Time format as follows: **YYYY:MM:DD:hh:mm:ss**. For example: 2016:03:01:12:34:56.

Verifying H-SFN Synchronization

The below given command displays the following new fields that are added to verify H-SFN Synchronization:

show mme-service full <service-name>

```
Extended DRX:
      H-SFN Start: 2016:03:01:12:34:56
```

Monitoring and Troubleshooting eDRX

eDRX Show Command(s) and /or Outputs

This section provides information regarding show commands and their outputs for the eDRX feature.

show mme-service statistics

- EDRX Subscribers
  - Attached Cells
  - DDN Rejects

Notes:

- Attached Calls: Displays the number of attached subscribers for which EDRX is enabled.

- DDN Rejects: Displays the number of DDNs rejected when EDRX subscribers cannot be paged (UE is out of the paging window)

show egtpc statistics verbose

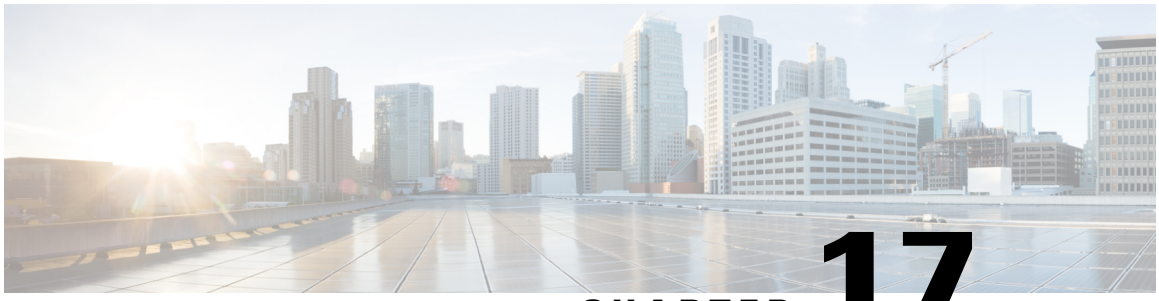
Executing the above command displays the following fields for this feature:

- Create Bearer Denied
- Create Bearer Denied TX
  - UE not reachable due to PSM
- Update Bearer Denied
- Update Bearer Denied TX
  - UE not reachable due to PSM

Bulk Statistics

Functional descriptions, triggers and statistic type are defined for each of the bulk statistics listed below in the *Statistics and Counters Reference*

- %attached-edrx-subscriber%
- %ddn-rejects-edrx%



CHAPTER 17

Emergency Bearer Services

This chapter describes the MME's implementation of Emergency Bearer services that support IMS emergency sessions.

Feature Description

The MME's emergency bearer services are provided to support IMS emergency sessions. Emergency bearer services are functionalities provided by the serving network when the network is configured to support emergency services.

Emergency bearer services are provided to normal attached UEs, depending on local regulation, to UEs that are in limited service state. Receiving emergency services in limited service state does not require a subscription. Depending on local regulation and an operator's policy, the MME may allow or reject an emergency attach request for UEs in limited service state.

In release 19.2, the Emergency Bearer Service feature provides a functionality to disable Emergency Bearer Service at a TAI management database level.

Important This feature is license controlled. Please consult your Cisco Account Representative for information about the specific license. This license was not enforced in earlier releases.

Feature Capabilities

The Emergency Bearer Support is equipped with the following capabilities:

UE capabilities

For Emergency Bearer Services in EPS, the UE supports the following functionalities:

- IMS Voice Calls.
- ATTACH requests with IMEI as the mobile identity if SIM is not detected in the network.
- PDN Connectivity procedures with request type set to "EMERGENCY".

MME Capabilities

The MME can accept an Attach Request for an Emergency Bearer Service or a PDN Connectivity Request to an emergency PDN if the network capabilities are configured to support Emergency Bearer Services.

As of 19.2, the MME now also supports:

- Emergency Bearer Service profile configuration. The profile should include the following to complete the profile configuration:
  - APN name
  - PGW FQDN or IP Addresses
  - QoS parameters to setup a session
- Configuration to disable emergency services at TAI management object level to reject emergency calls for a configured list of TAIs

Call Admission Control

In this release, all emergency calls are allowed until the configuration limit is reached. Deletion of existing calls to admit emergency attaches is not in scope of this release.

Attach for Emergency Bearers

Emergency Bearer Support supports the following ATTACH behaviors:

- Valid UEs only: Only normal UEs that have a valid subscription, authenticated and authorized for PS service in the attached location, are allowed. The normal Authentication and Attach procedures will be executed. The HSS subscription of the UE should allow the UE to be attached to EPS in its current TAI and in the current CSG (if applicable). The emergency attach procedure is not any different from the normal ATTACH procedure in this case.
- Authenticated UEs: These UEs must have a valid IMSI. These UEs are authenticated and may be in limited service state due to being in a location that is restricted from service. The Authentication procedure should complete successfully. The Update Location procedure to the HSS failing, or any further validation of HSS provided subscription data does not affect the processing of the ATTACH request successfully.
- IMSI: These UEs must have an IMSI. If authentication fails, the UE is granted access and the unauthenticated IMSI is retained in the network for the records purposes.

- All UEs: Along with authenticated UEs, this includes UEs with an IMSI that can not be authenticated and UEs with only an IMEI. In this case, an emergency attach request with the IMEI is accepted by the network.
- ISR is deactivated for an emergency attached UE.

As of release 19.2

- MME rejects the emergency attach procedure if emergency services are disabled for a TAI from which attach request is initiated.

Important When authentication fails, the MME queries the UE for IMEI, and the received IMEI is used as the key for the UE in the network. The IMSI is used for recording purposes only. If IMEI is used as the key for identifying the UE in the network, there will be no backup database context associated with the call.

PDN Connectivity for Emergency Bearer Service

A UE that is already attached to the network for EPS services requests for Emergency Bearer Service using a PDN connectivity request. The request-type in PDN Connectivity request is set to "emergency", and no APN information is supplied by the UE.

The MME does not consider HSS provided information to setup a connection, rather uses the locally configured PGW and APN information to setup the PDN connection. The UE is not allowed to request bearer allocations from this PDN, the requests are rejected.

As of release 19.2, the MME rejects emergency PDN activation if emergency services are disabled for a TAI.

Important The setup for PDN connection and associated bearers should not be affected by the policy configuration on the MME.

Tracking Area Update Procedure

MME supports the following in the TAU procedure:

- Skip Authentication procedure for a UE that only has PDNs for Emergency Bearer Services.
- If the UE is restricted on the new TAI, and the UE has PDN connection for Emergency Bearer services, the MME:
  - Deactivate all non-Emergency service PDN using with signaling to the UE if the UE is in ECM-CONNECTED.
  - Deactivate all non-emergency service PDN locally, and sending the EPS Bearer Context status IE in the TAU accept message if the UE is ECM-IDLE.
  - The MME shall also indicate to the UE that ISR is turned off
- If re-authentication fails the MME,
  - Deactivate all non-Emergency service PDN using with signaling to the UE if the UE is in ECM-CONNECTED

- Deactivate all non-emergency service PDN locally, and sending the EPS Bearer Context status IE in the TAU accept message if the UE is ECM-IDLE.

- If a UE attached only for EMERGENCY SERVICES, the MME shall set the mobile reachability timer to the configured T3412 value, and locally detach the UE if mobile reachability timer expires.

As of release 19.2, MME also supports:

- If a TAU for a UE in ECM-IDLE state is received after an emergency attach procedure, which arrives from an area whose emergency services are disabled, MME provides the following functions:
  - Rejection of TAU in case of single emergency PDN.
  - De-activation of all emergency PDNs in case of multiple PDNs.

Note The above functions are applicable for TAU arriving in idle mode

Inbound relocation Procedures

- Handling inbound relocations with no IMSI and security context present in the incoming MM context.
- If the UE is not valid in new location, or if local policy forbids setup of all bearers in the context, ensure that bearers set up for emergency services are not torn down.
- As of release 19.2, S1 and X2 handovers occurring after an emergency attach from an area where emergency services are disabled, is allowed to continue in connected mode.

MME Emergency Configuration Data

MME is supported with the following configuration data:

- Emergency Access Point Name (em APN): A label according to DNS naming conventions describing the access point used for Emergency PDN connection (wild card not allowed).
- Emergency QoS profile: The bearer level QoS parameter values for Emergency APN's default bearer (QCI and ARP). The ARP is an ARP value reserved for emergency bearers.
- Emergency APN-AMBR: The Maximum Aggregated uplink and downlink MBR values to be shared across all Non-GBR bearers, which are established for the Emergency APN, as decided by the PDN GW.
- Emergency PDN GW identity: The statically configured identity of the PDN GW used for emergency APN. The PDN GW identity may be either an FQDN or an IP address. It has be possible to support multiple PDN GW identity to support PGW redundancy.
- Disable emergency services: In release 19.2, MME provides CLI control to disable emergency-services at TAI management object level.

Information Storage

Currently, MME-APP stores UE contexts in lists indexed by IMSI, GUTI or PTMSI. To support emergency IMS bearers for UE without IMSI, MME supports indexing the list of active call lines by IMEI too.

Interdependences

The Emergency Bearer Service feature affects the related features described in this section, during Attach/TAU processing.

Regional Zone Code Restriction

The MME does not release a call if,

- Regional Zone Code restriction for a call in progress, and the TAI is restricted
- UE has emergency PDN connections, and emergency connections are allowed in restricted zone codes

Load Rebalancing

The MME does not impact UEs that are connected for Emergency Bearer Services during load rebalancing procedures (3GPP TS 23.401- 9.6.0 - 4.3.2.7).

SRVCC

If any of the bearers setup for emergency services have a QCI value of 1, such bearers is moved to CS domain on SRVCC activity. There is no conflict between SRVCC and Emergency Bearer Services. The Sv interface accepts messages without an IMSI, and unauthenticated UEs is supported over the Sv interface.

CSFB

The attach type IE is used for signaling either a "combined" or "emergency" attach. A UE that is "combined" attached might send a PDN connectivity request for emergency bearer services. After setup of such a bearer, if CSFB is requested, CSFB procedure will proceed with no interaction. Because the UE has been authenticated in the network, there is successful transfer of the UE context to a Gn/Gp SGSN. The SMS functionality of a UE is unaffected by a PDN Connectivity to a emergency PDN.

Gn/Gp Interface

Since the current version of Gn/Gp interface supported on the MME does not support handover of unauthenticated UE MM contexts to SGSN, Context Requests for an unauthenticated UE context from a Gn/Gp SGSN will be rejected by the MME.

Operator Policy

The interdependency of the Operator Policy that applies to the Emergency Bearer Service are as follows:

- Maximum PDN or Bearers reached
- Current TAI not supported
- Authentication required by policy fails
- Equipment identification through policy fails.

The specifications are only for calls which have both emergency and non-emergency PDNs. In any of the above policy restriction, the emergency PDN stays established, regardless of what validation level is required for emergency attach.

Interface

S11

The following changes are implemented on the S11 interface to support Emergency Service:

- IMSI is made optional in the Create Session Request.
- An indication flag is added to indicate if the IMSI is available but unauthenticated.

NAS

- New header type added to NAS parser to specify if the message header type is "integrity protected" or "integrity protected and ciphered"
- New Attach type.
- Emergency service support indicator for Attach/TAU accept.

S3/S10

The following interface changes apply to Context Response and Forward Relocation Request messages:

- Optional IMSI.
- IMSI Validation flag.
- Security Parameters if available.

S6A

The changes to the S6A interface includes the following:

- Optional HSS handle in UE_CONTEXT.
- Authentication Information Request not mandatory for all call flows.
- Update Location Requests not sent for Emergency Bearer Services Attach, if the configuration does not require it.

- Cancel Location Request will not clear a call in the MME if the associated IMSI has a PDN connection for Emergency Bearer Services.

How It Works

The UE can request Emergency Bearer Services depending on its current network state using the following options:

- If the UE is in a limited-access service state, that is, if the UE received a Attach-Reject message from the network or if the UE does not have a SIM, the UE can initiate an ATTACH request message to receive emergency bearer services. On successful ATTACH, the UE receives emergency bearer services.
- If the UE is in a regular connected state, the UE can request emergency bearer services by initiating an ATTACH request using the PDN Connectivity procedures.

Call Flows

This sections describes the procedures involved in providing Emergency Bearer Support in the MME

- Management of Security context
- Authentication procedure
- Attach procedure
- Detach procedure
- Tracking Area Update procedure
- Service Request procedure
- PDN Disconnection procedure
- Bearer resource exhaustion
- PDN Connect procedure for emergency bearers services
- PGW initiated Dedicated Bearer creation
- UE requested bearer resource allocation procedure
- UE requested bearer resource modification procedure
- Outbound relocation procedures
- TAU Attach
- Inbound relocation procedures

For details on the call flow procedure refer to the links provided in the *Standards Compliance* section.

Limitations

In this release, the Emergency Bearer Support has the following limitations:

- No checks will be made whether the same IMEI is used by UEs that are authenticated using IMSI.
- Only one call shall be allowed for a non-authenticated UE for a particular IMEI.
- Since the MME does not support Context Transfer without IMSI on the Gn/Gp interface, context transfer to a Gn/Gp SGSN will be rejected by MME if the UE has bearers for emergency services.

The following limitations apply to UEs that are ATTACHed for Emergency Bearer Services:

- The UE shall not request for additional PDN Connectivity. Any UE initiated PDN Connectivity requests will be rejected by the network.

The following limitations apply to PDN connection used for Emergency Bearer Services:

- The UE shall not request any Bearer Resource Allocation for such a PDN connection - a request will be rejected by the MME.

The following limitations apply to a EPS bearer context within a PDN connection for Emergency Bearer Services:

- The UE shall not request for Bearer modifications on such a bearer - any requests will be rejected by the MME.

Standards Compliance

The Emergency Bearer Service complies with the following standards:

- 3GPP TS 23.401 v9.7.0 (2010-12), 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 9)
- 3GPP TS 24.301 V9.5.0 (2010-12), 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3 (Release 9)

Configuring Emergency Bearer Service

Configuring Emergency Bearer Service Parameters

This section describes the configuration of the parameters to support Emergency Bearer Services.

A new object is added to abstract the configuration required for emergency bearer service. This object is then associated with **mme-service**. This object prevents the need to configure the same parameters multiple times

for multiple services within the same chassis. It also provides the flexibility to change parameters for different services when required.

The **lte-emergency-profile** command is used to configure a profile, which is associated to a mme-service or sgsn-service to provide emergency bearer services. A maximum of four profile configurations are supported.

```
config
    lte-policy
        lte-emergency-profile test profile_name
            [ [ default ] ue-validation-level ] {auth-only | full | imsi | none }
            [ [ remove ] apn ] apn_name pdn-type {ipv4 | ipv4v6 | ipv6 } restoration-priority
            [ [ remove ] qos ] qci  qci_value arp arp_value preemption-capability { may | shall-not }
vulnerability { not-preemptable | preemptable }
            apn-ambr max-ul uplink_value max-dl downlink_value
            pgw ip-address ip_address protocol { both | gtp | pmip } weight weight_value
                    exit
                exit
        exit
    context context_name
        mme-service service_name
            associate lte-emergency-profile profile_name
                    end
```

Notes:

- A maximum of four LTE emergency profiles can be configured on the system.
- In the **pgw** command, the valid protocol types are: **both, gtp, and pmip**. A maximum of four P-GW IP addresses can be configured per profile. An FQDN can also be configured in place of the IP addresses but only one P-GW FQDN can be configured per profile.
- To configure the MME to ignore the IMEI validation of the equipment during the attach procedure in emergency cases, use the following command in the **mme-service** configuration mode:
  `policy attach imei-query-type <imei | imei-sv | none> verify-equipmentidentity`
  verify-emergency
- To configure the MME to ignore the IMEI validation of the equipment during TAU procedures in emergency cases, use the following command in the mme-service configuration mode:
  `policy tau imei-query-type <imei | imei-sv | none> verify-equipmentidentity`
  verify-emergency

Disabling Emergency Bearer Services

This section describes the configuration to disable Emergency Bearer Services.

A new CLI is added at TAI management object level to disable emergency services. If the emergency request is received from a TAC, for which emergency services are disabled, then the request would be rejected.

```
configure
    lte-policy
        tai-mgmt-db db_name
            tai-mgmt-obj obj_name
                emergency-services-not-supported
                end
```

Notes:

- The **emergency-services-not-supported** is a newly added keyword to disable emergency bearer services.

Verifying the Emergency Bearer Service Configuration

Verify the configuration Emergency Bearer Services by entering the following command:

show mme-service all
The output for the above command is as shown below:

```
Service name                                          :   mmesvc
Context                                                :   ingress
Status                                                 :   STARTED
Bind                                                   :   Done
S1-MME IP Address                                 :   192.20.20.2
Crypto-Template Name                              :   None
Max Subscribers                                    :   4000000
S1-MME sctp port                                  :   25
MME Code                                               :   2
MME Group                                             :   32777
PLMN Id                                                :   MCC: 123, MNC: 456
Emergency Service Profile                    :   None
EGTP Context                                          :   ingress
EGTP Service                                          :   egtp_mme
```

Monitoring and Troubleshooting the Emergency Bearer Services

The following sections describe commands available to monitor Emergency Bearer Services on the MME

Emergency Bearer Services Show Command(s) and/or Outputs

This section provides information regarding show commands and/or their outputs in support of the Emergency Bearer Services

The show commands in this section are available in support of the Emergency Bearer Services

show lte-policy tai-mgmt-db name db_name

```
TAI Management DB tmd1
    TAI Management Object tmo1
        Time Zone UTC +05:15 DST 2
          Zone Code: 1111
          emergency-service-not-supported
          TAI   mcc 123 mnc 456 tac 2345
          TAI   mcc 123 mnc 456 tac 2348
          TAI   mcc 123 mnc 456 tac 1000
          TAI   mcc 123 mnc 456 tac 1001
          TAI   mcc 123 mnc 456 tac 1002
          SGW  10.6.0.14 s5-s8-protocol gtp weight 100
```

show mme-service statistics mme-service mmesvc

The mme-service statistics command displays the number of attach rejects, TAU rejects and PDN connectivity rejects, on disabling emergency services.

The output of the above command is as follows:

```
Attach Reject:                                                    0
    IMSI Unknown in HSS:                                0    Illegal UE:
              0
    Illegal ME:                                                   0    EPS Not Allowed:
```

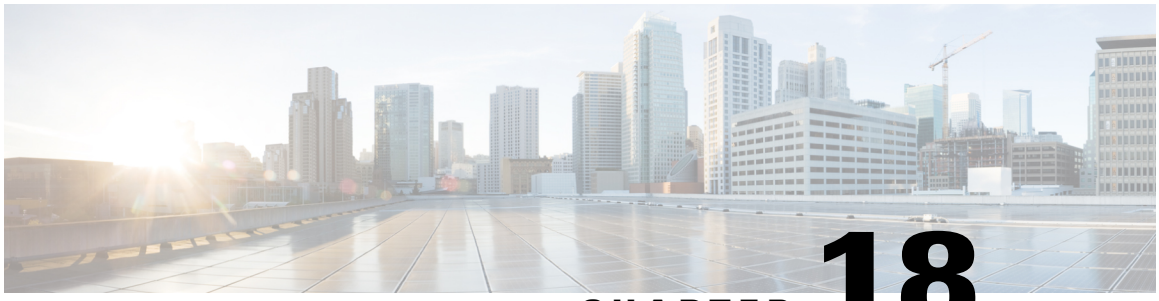
```
                0
    Emergency-services-disabled:    1
TAU Reject Total:                        0
    IMSI Unknown in HSS:                                  0    Illegal UE:
              0
    Illegal ME:                                                0    EPS Not Allowed:
                0
    Emergency-services-disabled:    2
 TAU Reject Intra MME:                   0
    IMSI Unknown in HSS:                                  0    Illegal UE:
              0
    Illegal ME:                                                0    EPS Not Allowed:
                0
    Emergency-services-disabled:    1
 TAU Reject Inter MME:                   0
    IMSI Unknown in HSS:                                  0    Illegal UE:
              0
    Illegal ME:                                                0    EPS Not Allowed:
                0
    Emergency-services-disabled:    1
PDN Connectivity Reject:             0
    PTI Already in Use:                                  0    Unknown or Missing APN:
     0
    Unknown PDN Type:                                      0    Invalid Bearer Id:
             0
    Invalid PTI:                                                0    Rejected By PGW/SGW:
               0
    Authentication Failed:                             0    Svc Opt Not Supported:
   0
    Svc Opt Not Subscribed:                           0    Opr Determined Barring:
 0
    Insufficient Resource:                             0    Activation Rejected:
     0
    Svc Opt Tmp OutOfOrder:                           0    Protocol Errors:
        0
    APN Restrict Incomt:                                  0    APN not sup PLMN-RAT:
      0
    Emergency-services-disabled: 1
```

Emergecny Bearer Services Bulk Statistics

The following statistics are included in the MME Schema in support of the Emergency Support Services:

For descriptions of these variables, see "MME Schema Statistics" in the *Statistics and Counters Reference*.

- %emm-msgtx-emergency-disabled%
- %emm-msgtx-tau-emergency-disabled%
- %emm-msgtx-tau-inter-emergency-disabled%
- %emm-msgtx-tau-intra-emergency-disabled%
- %esm-msgtx-pdncon-rej-emergency-disabled%



CHAPTER 18

Enhanced Congestion Control and Overload Control

Feature Description

The MME provides an enhanced congestion control and overload control feature set.

This feature builds on the base congestion control functionality provided on the MME. Refer to the *Congestion Control* and *Overload Control* sections in the *MME Overview* chapter for more information about the basic functionality.

To use this feature, you need a valid license key (MME Resiliency) installed. Contact your Cisco Account or Support representative for information on how to obtain a license.

Enhanced Congestion Control and Overload Control

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.

Relationships to Other Features

This license-enabled feature builds on the base congestion control functionality provided on the MME.

Refer to the *Congestion Control* and *Overload Control* sections in the *MME Overview* chapter for more information about the basic functionality.

Additional information is also provided in the *Congestion Control* chapter in the *System Administration Guide*.

Limitations

The base congestion control functionality also can monitor congestion of the following resources:

- Port-specific RX and TX utilization
- Port RX and TX utilization
- Message queue utilization
- Message queue wait time

The license-enabled Enhanced Congestion Control funtionality on the MME does not support the monitoring of these resources using three different threshold levels (critical, major and minor). Only a single threshold level (critical) can be monitored for these resources.

Configuring Enhanced Congestion 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.

Configuring Enhanced Congestion Control

This section includes configuration procedures for the following:

- Configuring Thresholds and Tolerances
- License Utilization Thresholds
- Maximum Session Per Service Thresholds
- Service Control CPU Thresholds
- System CPU Thresholds
- System Memory Thresholds
- Configuring a Congestion Action Profile
- Associating a Congestion Action Profile with Congestion Control Policies
- Configuring Overload Control
- Configuring Congestion SNMP Traps

Configuring Thresholds and Tolerances

Congestion threshold values must be defined to establish when a congestion condition is reached. Congestion threshold tolerances must also be configured to establish when a congestion condition is cleared. Individual thresholds values and tolerances can be defined for *critical* , *major* and *minor* thresholds.

The default tolerance window for critical thresholds is 10. The default for major and minor thresholds is 0.

If the tolerance is configured greater than threshold, then the tolerance will be treated as zero.

When configuring thresholds and tolerances for critical, major and minor congestion levels, the threshold levels and tolerances should never overlap. Consider the following example configuration, where the following threshold levels do not overlap:

- Critical congestion will trigger at 80 and will clear at 70
- Major congestion will trigger at 70 and will clear at 60
- Minor congestion will trigger at 60 and will clear at 50.

configure
congestion-control threshold tolerance critical *10*
congestion-control threshold max-sessions-per-service-utilization major *70*
congestion-control threshold tolerance major *10*
congestion-control threshold max-sessions-per-service-utilization minor *60*
congestion-control threshold tolerance minor *10*
congestion-control threshold max-sessions-per-service-utilization critical *80*
end

For information about all of the congestion control commands available, refer to the *Global Configuration Mode Commands* chapter of the *ASR 5x00 Command Line Interface Reference* .

License Utilization Thresholds

The license-utilization threshold is calculated based on the configured license values for the chassis.

In this example configuration, the minor threshold will be triggered at 4000 calls, major threshold will be triggered at 6000 calls, and critical threshold will be triggered at 8000 calls.

```
congestion-control threshold license-utilization critical 80
congestion-control threshold license-utilization major 60
congestion-control threshold license-utilization minor 40
```

Maximum Session Per Service Thresholds

This threshold is configured across all MME services.

```
config
   congestion-control threshold max-sessions-per-service-utilization critical 80
```

When there are multiple MME services configured with different max-subscribers parameters, chassis congestion will be calculated using the minimum of max-subscribers configured in each of the different MME services.

However, congestion actions will be applied to each individual service based on its corresponding max-session-per-service parameters.

For example:

```
configure
   context ingress
      mme-service mmesvc1
         bind s1-mme ipv4-address 10.10.10.2 max-subscribers 10000
         exit
      exit
      mme-service mmesvc2
         bind s1-mme ipv4-address 10.10.10.3 max-subscribers 1000
         exit
      exit
      mme-service mmesvc3
         bind s1-mme ipv4-address 192.80.80.3 max-subscribers 20000
         end
```

In the above example, chassis level critical congestion will get triggered when the number of subscribers in mmesvc2 is at 800. Corresponding SNMP traps will be generated. However, congestion policies will not be applied for mmesvc1 and mmesvc3. When the number of subscribers in mmesvc1 and mmesvc3 reaches 8000 and 16000 respectively, then congestion policies will be applied for mmesvc1 and mmesvc3.

Chassis congestion will be cleared only when the congestion is cleared in all MME services.

Similarly, when minor, major and critical threshold are configured for max-session-per-service for many MME services, the maximum value of the threshold will be considered for chassis level congestion.

For example, if mmesvc1 reaches the major threshold, mmesvc2 reaches the critical threshold and mmesvc3 reaches the minor threshold, then chassis congestion state will be critical.

Service Control CPU Thresholds

This threshold is calculated from the system's demux CPU. The threshold is calculated based on a five minute average CPU usage.

The highest CPU usage value of two CPU cores of the demux CPU is considered. For example, if CPU core 0 has a five minute CPU usage of 40 and CPU core 1 has a five minute CPU usage of 80, then CPU core 1 will be considered for threshold calculation.

The following example configuration shows threshold levels of 80, 60, and 40 usage:

```
congestion-control threshold service-control-cpu-utilization critical 80
congestion-control threshold service-control-cpu-utilization major 60
congestion-control threshold service-control-cpu-utilization minor 40
```

System CPU Thresholds

This threshold is calculated using the five minute CPU usage average of all CPUs (except standby CPU and SMC CPU).

The highest CPU usage value of two CPU core of all CPU will be considered.

The following example configuration shows threshold levels of 80, 60, and 40 usage:

```
congestion-control threshold system-cpu-utilization critical 80
congestion-control threshold system-cpu-utilization major 60
congestion-control threshold system-cpu-utilization minor 40
```

System Memory Thresholds

This threshold is calculated using the five minute memory usage average of all CPUs (except standby CPU and SMC CPU).

The following example configuration shows threshold levels of 80, 60, and 40 usage:

```
congestion-control threshold system-memory-utilization critical 80
congestion-control threshold system-memory-utilization major 60
congestion-control threshold system-memory-utilization minor 40
```

Configuring a Congestion Action Profile

Congestion Action Profiles define a set of actions which can be executed after the corresponding threshold is crossed.

Use the following example configuration which creates a congestion action profile named *critical_action_profile* and defines several actions for this profile:

```
configure
   lte-policy
      congestion-action-profile critical_action_profile
         reject s1-setups time-to-wait 60
         drop handovers
         reject combined-attaches
         report-overload permit-emergency-sessions enodeb-percentage 50
         end
```

See the *Congestion Action Profile Configuration Commands* chapter in the *Command Line Reference* for details about all the congestion action profile commands available.

Refer to *Configuring Overload Control* in this chapter for more information about the **report-overload** keyword and associated functionality.

Associating a Congestion Action Profile with Congestion Control Policies

Each congestion control policy (critical, major, minor) must be associated with a congestion control profile.

The following example configuration to associate the congestion action profile named *critical_action_profile* with the **critical** congestion control policy:

```
configure
   congestion-control policy critical mme-service action-profile critical_action_profile
```

Separate congestion action profiles can be associated with major and minor congestion control policies, for example:

```
   congestion-control policy major mme-service action-profile major_action_profile
   congestion-control policy minor mme-service action-profile minor_action_profile
```

Configuring Overload Control

When an overload condition is detected on an MME, the system can be configured to report the condition to a specified percentage of eNodeBs and take the configured action on incoming sessions.

To create a congestion control policy with overload reporting, apply the following example configuration:

```
configure
   lte-policy
      congestion-action-profile  <profile_name>
      congestion-action-profile  <profile_name>
      end
```

```
configure
   congestion-control policy critical mme-service action report-overload reject-new-sessions
 enodeb-percentage <percentage>
   end
```

Notes:

- The following overload actions are also available (in addition to **reject-new-sessions**):
  - **permit-emergency-sessions-and-mobile-terminated-services**
  - **permit-high-priority-sessions-and-mobile-terminated-services**
  - **reject-delay-tolerant-access**
  - **reject-non-emergency-sessions**

See the *Congestion Action Profile Configuration Mode Commands* chapter in the *Command Line Reference* for details about all the congestion action profile commands available.

Configuring Enhanced Congestion SNMP Traps

When an enhanced congestion condition is detected, an SNMP trap (notification) is automatically generated by the system.

To disable (suppress) this trap:

configure
snmp trap suppress EnhancedCongestion
end

To re-enable generation of the Enhanced Congestion trap:

configure
snmp trap enable EnhancedCongestion target <*target-name*>
end

Verifying the Congestion Control Configuration

Use the following Exec mode command to display the configuration of the congestion control functionality.

show congestion-control configuration

The following output is a concise listing of all threshold and policy configurations showing multi-level Critical, Major and Minor threshold parameters and congestion control policies:

```
Congestion-control: enabled

Congestion-control Critical threshold parameters
```

```
    system cpu utilization:                                  80
    service control cpu utilization:              80
    system memory utilization:                          80
    message queue utilization:                          80
    message queue wait time:                              10 seconds
    port rx utilization:                                     80
    port tx utilization:                                     80
    license utilization:                                     100
    max-session-per-service utilization:      100
    tolerence limit:                                             10
Congestion-control Critical threshold parameters
    system cpu utilization:                                  80
    service control cpu utilization:              80
    system memory utilization:                          80
    message queue utilization:                          80
    message queue wait time:                              10 seconds
    port rx utilization:                                     80
    port tx utilization:                                     80
    license utilization:                                     100
    max-session-per-service utilization:      100
    tolerence limit:                                             10
Congestion-control Major threshold parameters
    system cpu utilization:                                   0
    service control cpu utilization:              0
    system memory utilization:                          0
    message queue utilization:                          0
    message queue wait time:                              0 seconds
    port rx utilization:                                     0
    port tx utilization:                                     0
    license utilization:                                     0
    max-session-per-service utilization:      0
    tolerence limit:                                             0
Congestion-control Minor threshold parameters
    system cpu utilization:                                   0
    service control cpu utilization:              0
    system memory utilization:                          0
    message queue utilization:                          0
    message queue wait time:                              0 seconds
    port rx utilization:                                     0
    port tx utilization:                                     0
    license utilization:                                     0
    max-session-per-service utilization:      0
    tolerence limit:                                             0
Overload-disconnect: disabled
Overload-disconnect threshold parameters
    license utilization:                                     80
    max-session-per-service utilization:     80
    tolerance:                                                           10
    session disconnect percent:                          5
    iterations-per-stage:                                   8
Congestion-control Policy
    mme-service:
        Critical Action-profile : ap3
        Major    Action-profile : ap2
        Minor    Action-profile : ap1
```

Verifying Congestion Action Profiles

To verify the configuration of a congestion action profile, use the following Exec mode command:
show lte-policy congestion-action-profile { name <*profile_name*> **| summary }**

Monitoring and Troubleshooting

This section provides information on how to monitor congestion control.

Congestion Control Show Command(s) and/or Outputs

This section provides information regarding show commands and/or their outputs in support of enhanced congestion control.

show congestion-control statistics mme

The following command shows an overview of all congestion control statistics for the MME.
show congestion-control statistics mme [full | critical | major | minor]

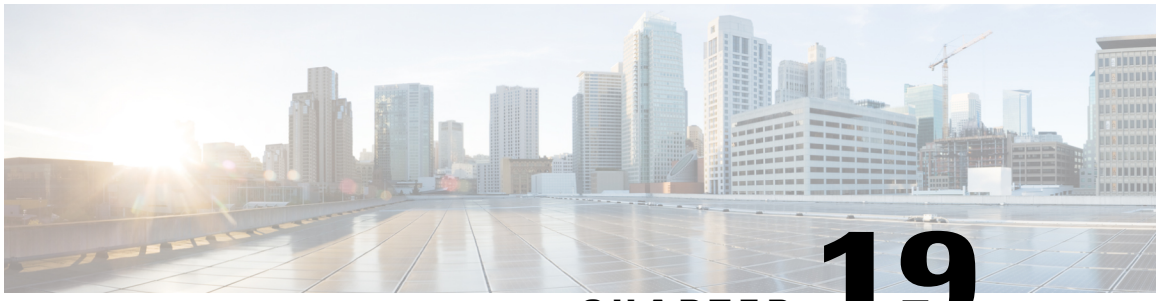
The following output is a concise listing of congestion control statistics. In this example output, only the **Critical** information is shown.

```
Critical Congestion Policy Action
    Congestion Policy Applied                       :    0 times
    PS attaches
                    Rejected            :      0 times
                    Dropped              :      0 times
    PS attaches
                    Rejected            :      0 times
                    Dropped              :      0 times
    Combined attaches
                    Rejected            :      0 times
                    Dropped              :      0 times
    S1-Setup
                    Rejected            :      0 times
                    Dropped              :      0 times
    Handover
                    Rejected            :      0 times
                    Dropped              :      0 times
    Addn-pdn-connect
                    Rejected            :      0 times
                    Dropped              :      0 times
    Addn-brr-connect
                    Rejected            :      0 times
                    Dropped              :      0 times
    Service-Request
                    Rejected            :      0 times
                    Dropped              :      0 times
    TAU-Request
                    Rejected            :      0 times
                    Dropped              :      0 times
    S1AP Overload Start Sent                         :      2 times
    S1AP Overload Stop  Sent                         :      2 times
    Excluded Emergency Events                       :      0 times
    Excluded Voice Events                               :      0 times
```

show congestion-control statistics mme

The following command shows SNMP event statistics for the EnhancedCongestion trap and EnhancedCongestionClear trap .

```
show snmp trap statistics verbose | grep EnhancedCongestion
```



CHAPTER 19

Enhanced Multimedia Priority Service (eMPS)

The MME supports eMPS (Enhanced Multimedia Priority Service) in PS (Packet Switched) and CS (Circuit Switched) domains.

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.

How it Works

The MME receives the eMPS subscription information which is indicated by the MPS-Priority IE in HSS subscription data or local configuration for eMPS subscription. Local configuration of eMPS subscription overrides the information received from the HSS.

For PS paging the MME supports Paging Priority in S1AP Paging Messages. A configurable mapping support is provided for ARP to S1AP Paging Priority. The MME includes paging priority for PS paging if corresponding ARP to paging priority is configured and the user has an eMPS PS subscription.

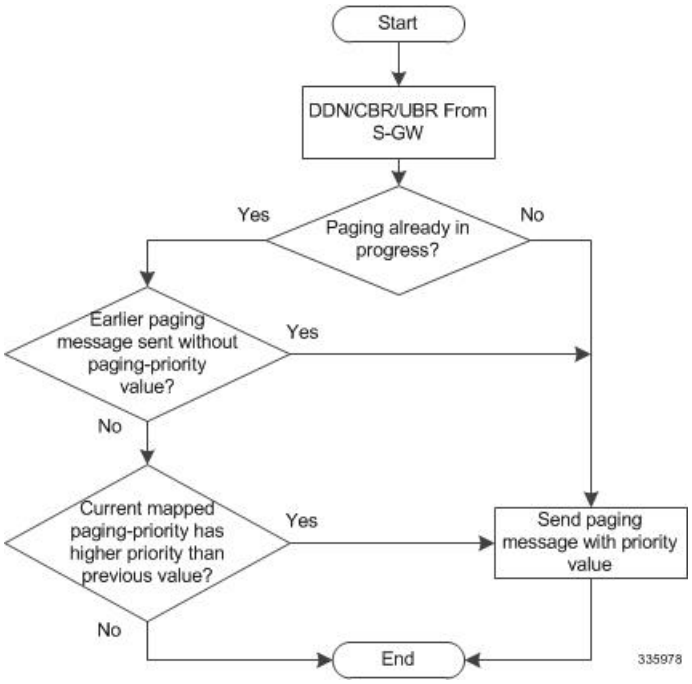
In previous releases (release 19.2) the MME supports paging priority for CS paging (refer to feature chapter "Paging Priority IE Support"). By default the MME sends the received eMLPP priority present in SGs-AP Paging-Request message as the S1 paging priority for CS paging. From this release onwards the MME supports configuration of one to one mapping of eMLPP priority to paging priority. The **paging-priority** command can be configured to map eMLPP priority to paging priority. In earlier releases this mapping was limited to single paging priority value override. The MME by default sends the eMLPP priority as paging priority for CS paging, this functionality does not require a feature license. However the mapping and subscription override functionality for PS and CS paging requires an eMPS license. All the priority PS traffic is completely controlled by the license. Priority CS MT/MO calls are allowed do not require a license in the following scenarios:

- MT calls are allowed always because “paging-priority cs” CLI is enabled by default.
- MO calls are allowed if eMPS CS subscription is received from HSS as subscribed, this functionality is not controlled by CLI configuration.

The **csfb** command is enhanced to configure HO-restriction for csfb MO Emergency calls. When HO-restriction is enabled the MME sets the "Additional CS Fallback Indicator IE" in S1AP UE Context Setup/Modification as "restriction".

Support for ARP based heuristics paging profile selection is added by this feature. This allows differentiated paging treatment based on the ARP of the corresponding PS traffic. ARP based paging profile selection requires a Heuristics paging license. For more information refer to the feature chapter on Heuristic and Intelligent Paging.

This feature adds support for priority SRVCC Handovers. When handover request message with SRVCC HO Indication flag set is received from eNodeB, the UE is subscribed to MPS in the EPS domain and the MME detects the SRVCC HO requires priority handling, the MME provides priority indication in SRVCC PS to CS Request. The MME detection of priority handling is based on the ARP associated with the EPS bearer used for IMS signaling (bearer with QCI 5) and corresponding paging priority mapping configured for this ARP. The priority indication here corresponds to the ARP information element.



Listed below are the various scenarios describing the MME behavior on receiving S11 Downlink Data Notification or Create Bearer Request or Update Bearer Request:

Scenario 1: DDN is received with ARP

- The MME includes paging priority in the S1 Paging message if the mapping configured for that ARP.
- Heuristics paging enabled, the MME selects the paging profile based on ARP if paging-profile with matching ARP value is configured in paging-map.
- The paging profile with the highest precedence is selected even if both ARP and QCI are configured in the paging-map.

Scenario 2: DDN received with only Bearer Id (No ARP)

- The MME fetches the ARP for that bearer id and includes paging priority in the paging message if mapping is configured for that ARP
- Heuristics paging enabled, MME selects the paging profile based on ARP if paging-profile with matching ARP value is configured in paging-map.
- The paging profile with the highest precedence is selected even if both ARP and QCI are configured in the paging-map.

Scenario 3: DDN received without the Bearer id

- The MME fetches the lowest ARP value from all the bearers and includes mapped paging priority for that ARP in the paging message if mapping is configured for that ARP
- Heuristics paging enabled, MME selects the paging profile based on ARP if paging-profile with matching ARP value is configured in paging-map.
- The paging profile with the highest precedence is selected even if both ARP and QCI are configured in the paging-map

Scenario 4: CBR is received

- MME includes paging priority in the S1 Paging message if the mapping configured for that ARP
- Heuristics paging enabled, MME selects the paging profile based on ARP if paging-profile with matching ARP value is configured in paging-map.
- The paging profile with the highest precedence shall be selected even if both ARP and QCI are configured in the paging-map.

Scenario 5: UBR is received from SGW for QOS modification

- MME includes paging priority in the S1 Paging message if the mapping configured for that ARP
- Heuristics paging enabled, MME selects paging profile based on ARP if paging-profile with matching ARP value is configured in paging-map.
- The paging profile with the highest precedence shall be selected even if both ARP and QCI are configured in the paging-map

Limitations

Congestion control is applied to all subscribers irrespective of eMPS subscription.

Standards Compliance

Enhanced Multimedia Priority Service complies with the following 3GPP standards:

- 3GPP TS 29.272
- 3GPP TS 36.413
- 3GPP TS 23.401
- 3GPP TS 29.280

Configuring Enhanced Multimedia Priority Service

The following configuration procedures are used to configure this feature:

Configuring MPS in EPS Domain

The **mps** command under the Call Control Profile Configuration mode has been enhanced to support Multimedia Priority Service (MPS) in the EPS domain. A new keyword **eps-priority** is added to the command; this keyword is used to configure support for MPS in EPS domain.

configure
call-control-profile *profile_name*
[remove] mps [cs-priority | eps-priority] { subscribed | none }
exit

Notes:

- By default MPS in EPS domain is disabled.
- The **remove** keyword deletes the existing configuration.
- The keyword **eps-priority** configures support for MPS in the EPS domain.
- The keyword **subscribed** indicates the UE subscribed to priority service in the CS/EPS domain.
- The keyword **none** indicates the UE not subscribed to priority service in the CS/EPS domain.
- The keyword **mps cs-priority** is used only for Mobile originated calls.
- The operator will be able to prioritize EPS calls for a set of subscribers irrespective of them being subscribed to MPS services.
- This configuration is not configured by default.

Configuring Paging Priority

The **paging-priority** command has been enhanced to support PS traffic. New keywords are added to configure priority value of enhanced Multi Level Precedence and Pre-emption service, configure the value of paging-priority to be sent to eNodeB and configure the value of allocation and retention priority.

[remove] paging-priority { cs { *cs_value* **| map emlpp-priority** *emlpp_value* **s1-paging-priority** *priority_value* **} | ps map arp** *arp_value* **s1-paging-priority** *priority_value* **}**
Notes:

- The keyword **cs** is used to configure the value of paging-priority to be sent to eNodeB for Circuit Switched (CS) traffic. The paging priority value can be configured or it can be used to map the received value to the paging-priority. The **cs_value** is an integer in the range “0” up to “7”. Configuring a value of “0” disables sending of paging priority value to eNodeB.
- The keyword **ps** is used to configure the value of paging-priority to be sent to eNodeB for Packet Switched (PS) traffic. The paging priority value can be configured or it can be used to map the received value to the paging-priority.
- The keyword **map** is used to map the received value to paging-priority.
- The keyword **emlpp-priority** is used to configure the priority value of enhanced Multi Level Precedence and Pre-emption service. The **emlpp_value** is an integer in the range “0” up to “7”.
- The keyword **s1-paging-priority** is used to configure the value of paging-priority to be sent to eNodeB. The priority value is an integer in the range “0” up to “7”. Configuring a value of “0” disables sending of paging priority value to eNodeB.
- The keyword **arp** is used to configure the value of allocation and retention priority. The value is an integer in the range “1” up to “15”.
- Mapping is not enabled by default.
- The keyword **remove** deletes the existing configuration.

Configuring Precedence

The **precedence** command enables the operator to apply a priority for different paging-profiles based on traffic type. The priority value that can be configured for the precedence has been enhanced. The operator can define ARP priority based paging for PS traffic type in the paging-map.

precedence *priority* **traffic-type { cs [voice | sms | other] | ps [arp** *arp_value* **| qci** *qci_value* **] | signaling [detach | idr | lcs | node-restoration] } paging-profile** *paging_profile_name*
no precedence *priority*
Notes:

- The range for precedence priority value is updated from 1 up to 35 , where 1 is the highest priority and 35 is the lowest priority. The numbers of paging-profiles supported are increased from 8 to 16.
- The keyword **arp** is added to the **precedence** command. It is used to define the ARP priority based paging for PS traffic type in the paging-map. The **arp_value** is an integer from 1 up to 15.

Configuring HO Restriction

The **csfb** command configures circuit-switched fallback options. CSFB is the mechanism to move a subscriber from LTE to a legacy technology to obtain circuit switched voice or short message. This command is updated with the keyword ho-restriction, to enable ho-restriction support for CSFB MO Emergency Calls.

csfb { policy { ho-restriction | not-allowed | not-preferred | sms-only | suppress-call-reject } | sms-only }
remove csfb { policy | sms-only }
Notes:

- The keyword **ho-restriction** enables ho-restriction support for priority CS calls. If this keyword is enabled the MME sets the "Additional CS Fallback Indicator IE" in S1AP UE Context Setup/Modification as "restriction".
- HO-Restriction is not enabled by default.

Sample configuration

```
config
  apn-profile apn1
     apn-type ims
  exit
  operator-policy name op1
    associate call-control-profile ccp
    apn network-identifier starent.com apn-profile apn1
  exit
  call-control-profile ccp
    csfb policy ho-restriction
    mps cs-priority subscribed
    mps eps-priority subscribed
    paging-priority cs map emlpp-priority 1 s1-paging-priority 2
    paging-priority ps map arp 5 s1-paging-priority 2
  exit
exit
```

Verifying the Configuration

show configuration

The following new fields are added to the show configuration command to verify the configured eMPS parameters:

- **mps eps-priority**: Displayed as either “Subscribed” or “None”.
- **paging-priority** *traffic_type*: Displayed as either “PS” or “CS”.
- **map**: Displayed if mapping is configured.
- **emlpp-priority priority_value**: Displays the configured emlpp priority value.
- **s1-paging-priority value**: Displays the configured s1-paging priority value.

- **arp** *arp_value*: Displays the configured ARP value.
- **precedence** *precedence_value*: Displays the configured precedence value.
- **traffic-type** *type*: Displays the traffic type as “CS” or “PS”.
- **paging-profile** *profile_name*: Displays the name of the paging profile.

Monitoring and Troubleshooting

This section provides information regarding show commands and bulk statistics for this feature.

Show Command(s) and/or Outputs

Note Paging counter includes the S1 paging for priority and non-priority paging requests. Paging CS Priority and Paging PS Priority counters only count the priority S1 paging requests.

show mme-service *service_name* peer-id *id* statistics

The following new fields are added to the show output to display the configured eMPS parameters:

- Paging CS Priority
- Paging PS priority
- UE Initiated Priority Voice Procedures
- Attempted
- Failures
- Success
- NW Initiated Priority Voice Procedures
- Attempted
- Failures
- Success

show session subsystem facility mmemgr

The following new parameters are added show output:

- Paging CS Priority
- Paging PS priority

show lte-policy paging-map name

The following new parameters are added to the show output:

- Precedence
- Packet-Switched(PS)
- ARP
- Paging is performed as per paging-profile *name*

show mme-service statistics

The following new parameters are added to the show output:

- Paging Initiation for PS ARP-N Events
- Attempted
- Success
- Failures
- Success at Last n eNB
- Success at Last TAI
- Success at TAI List

show call-control-profile full all

The following new fields are added to the show output to display the configured eMPS parameters:

- MPS EPS priority
- Paging priority to be sent to eNodeB for CS
- Paging priority mapping for CS
- Paging priority mapping for EPS
- Handover Restriction

Enhanced Multimedia Priority Support Bulk Statistics

The following statistics are included in the MME Schema in support of this feature**:**

- s1ap-transdata-pagingpriocs
- s1ap-transdata- pagingpriops
- csfb-ue-prio-voice-total
- csfb-ue-prio-voice-success

- csfb-ue-prio-voice-failures
- csfb-nw-prio-voice-total
- csfb-nw-prio-voice-success
- csfb-nw-prio-voice-failures
- ps-arp-1-paging-init-events-attempted
- ps-arp-1-paging-init-events-success
- ps-arp-1-paging-init-events-failures
- ps-arp-1-paging-last-enb-success
- ps-arp-1-paging-last-tai-success
- ps-arp-1-paging-tai-list-success
- ps-arp-2-paging-init-events-attempted
- ps-arp-2-paging-init-events-success
- ps-arp-2-paging-init-events-failures
- ps-arp-2-paging-last-enb-success
- ps-arp-2-paging-last-tai-success
- ps-arp-2-paging-tai-list-success
- ps-arp-3-paging-init-events-attempted
- ps-arp-3-paging-init-events-success
- ps-arp-3-paging-init-events-failures
- ps-arp-3-paging-last-enb-success
- ps-arp-3-paging-last-tai-success
- ps-arp-3-paging-tai-list-success
- ps-arp-4-paging-init-events-attempted
- ps-arp-4-paging-init-events-success
- ps-arp-4-paging-init-events-failures
- ps-arp-4-paging-last-enb-success
- ps-arp-4-paging-last-tai-success
- ps-arp-4-paging-tai-list-success
- ps-arp-5-paging-init-events-attempted
- ps-arp-5-paging-init-events-success
- ps-arp-5-paging-init-events-failures
- ps-arp-5-paging-last-enb-success
- ps-arp-5-paging-last-tai-success

- ps-arp-5-paging-tai-list-success
- ps-arp-6-paging-init-events-attempted
- ps-arp-6-paging-init-events-success
- ps-arp-6-paging-init-events-failures
- ps-arp-6-paging-last-enb-success
- ps-arp-6-paging-last-tai-success
- ps-arp-6-paging-tai-list-success
- ps-arp-7-paging-init-events-attempted
- ps-arp-7-paging-init-events-success
- ps-arp-7-paging-init-events-failures
- ps-arp-7-paging-last-enb-success
- ps-arp-7-paging-last-tai-success
- ps-arp-7-paging-tai-list-success
- ps-arp-8-paging-init-events-attempted
- ps-arp-8-paging-init-events-success
- ps-arp-8-paging-init-events-failures
- ps-arp-8-paging-last-enb-success
- ps-arp-8-paging-last-tai-success
- ps-arp-8-paging-tai-list-success
- ps-arp-9-paging-init-events-attempted
- ps-arp-9-paging-init-events-success
- ps-arp-9-paging-init-events-failures
- ps-arp-9-paging-last-enb-success
- ps-arp-9-paging-last-tai-success
- ps-arp-9-paging-tai-list-success
- ps-arp-10-paging-init-events-attempted
- ps-arp-10-paging-init-events-success
- ps-arp-10-paging-init-events-failures
- ps-arp-10-paging-last-enb-success
- ps-arp-10-paging-last-tai-success
- ps-arp-10-paging-tai-list-success
- ps-arp-11-paging-init-events-attempted
- ps-arp-11-paging-init-events-success

- ps-arp-11-paging-init-events-failures
- ps-arp-11-paging-last-enb-success
- ps-arp-11-paging-last-tai-success
- ps-arp-11-paging-tai-list-success
- ps-arp-12-paging-init-events-attempted
- ps-arp-12-paging-init-events-success
- ps-arp-12-paging-init-events-failures
- ps-arp-12-paging-last-enb-success
- ps-arp-12-paging-last-tai-success
- ps-arp-12-paging-tai-list-success
- ps-arp-13-paging-init-events-attempted
- ps-arp-13-paging-init-events-success
- ps-arp-13-paging-init-events-failures
- ps-arp-13-paging-last-enb-success
- ps-arp-13-paging-last-tai-success
- ps-arp-13-paging-tai-list-success
- ps-arp-14-paging-init-events-attempted
- ps-arp-14-paging-init-events-success
- ps-arp-14-paging-init-events-failures
- ps-arp-14-paging-last-enb-success
- ps-arp-14-paging-last-tai-success
- ps-arp-14-paging-tai-list-success
- ps-arp-15-paging-init-events-attempted
- ps-arp-15-paging-init-events-success
- ps-arp-15-paging-init-events-failures
- ps-arp-15-paging-last-enb-success
- ps-arp-15-paging-last-tai-success
- ps-arp-15-paging-tai-list-success

For descriptions of these variables, see "MME Schema Statistics" in the *Statistics and Counters Reference*.

Troubleshooting

If paging priority information is not being sent to the eNodeb during mobile terminating PS traffic then, verify the following:

- Ensure the licensing is configured for eMPS.
- Verify if ps-priority is received from the HSS in ULA message or “mps ps-priority subscribed” is configured under the call control profile.
- Verify if ARP to paging-priority mapping is configured.

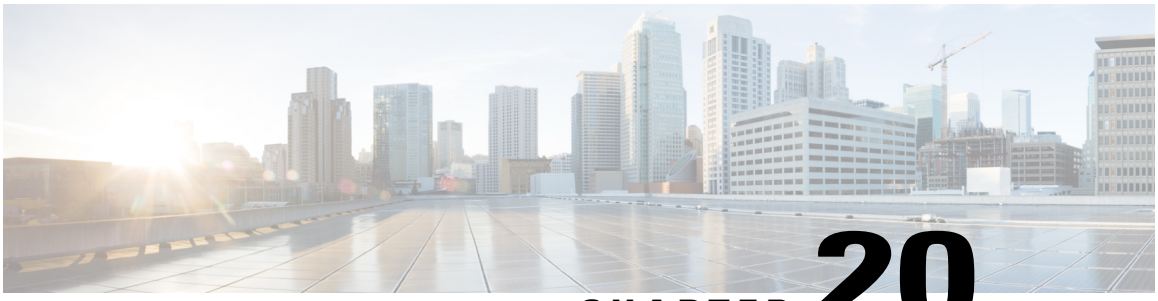
Execute the show command "show call-control-profile full all" to verify the configuration parameters listed above.

If ARP IE is not being sent in Sv PS to CS Request message, verify the following:

- Ensure eMPS PS subscription is configured.
- The apn-type should be ims, it is configured in the apn-profile configuration for IMS PDN.
- IMS signaling bearer uses QCI 5
- ARP for IMS signaling bearer has corresponding paging priority mapping configured.

If Additional CSFB indicator is not included for MO CS emergency call/ traffic, verify the following:

- Ensure the CLI configuration for HO restriction is enabled.



CHAPTER 20

Enhanced Event Logging

This chapter describes the MME's Event Logging functionality which occurs at the subscriber level, from the MME to an external server.

Feature Description

The MME handles numerous subscriber calls from different eNodeBs in the network. In order to troubleshoot any issues for a particular subscriber, the events that caused the issue is recorded. The events could be individual procedures listed below:

- Attach Procedures
- Detach Procedures
- TAU Procedures
- Handover Procedures
- All types of Service Requests
- Paging based on different triggers
- PDN Connectivity Requests
- All types of PDN detach and network initiated PDN detach procedures
- Dedicated Bearer Activation Requests
- Dedicated Bearer Deactivation Requests
- All types of Bearer modification procedures
- CSFB procedures
- SRVCC procedures

- eCSFB procedures
- eSRVCC procedures

The Event Data Record is a proprietary feature of StarOS. In this feature, MME provides a debugging framework to capture procedure level information for each subscriber. On the completion of a procedure successfully or unsuccessfully, the MME generates a procedure summary. This summary provides details of the events and issues, which is nearly comparable to real-time debugging.

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

MME supports the following functionality in this feature:

- Event Logging for 4G subscribers.
- The Event Records are stored in CSV file format.
- A framework to collect information and eventually provide log information. The framework is extensible to hold more procedures and information fields.
- The order of fields are easily changeable.
- The event logs are generated on completion of the procedure successfully or unsuccessfully. The procedure could be unsuccessful because of local reasons such as – HSS/Peer element triggered reasons, Timeouts for responses, arrival of procedures and so on.
- Each record has a smgr-no and sequence-no field. If there is no guaranteed delivery of events, the sequence number will help in identifying the lost events.
- Event reporting can be enabled or disabled through the CLI command reporting-action mme-event-record under the Call Control Configuration mode. For detailed information on feature configuration see the *Configuring Event Logging* section in this feature chapter.

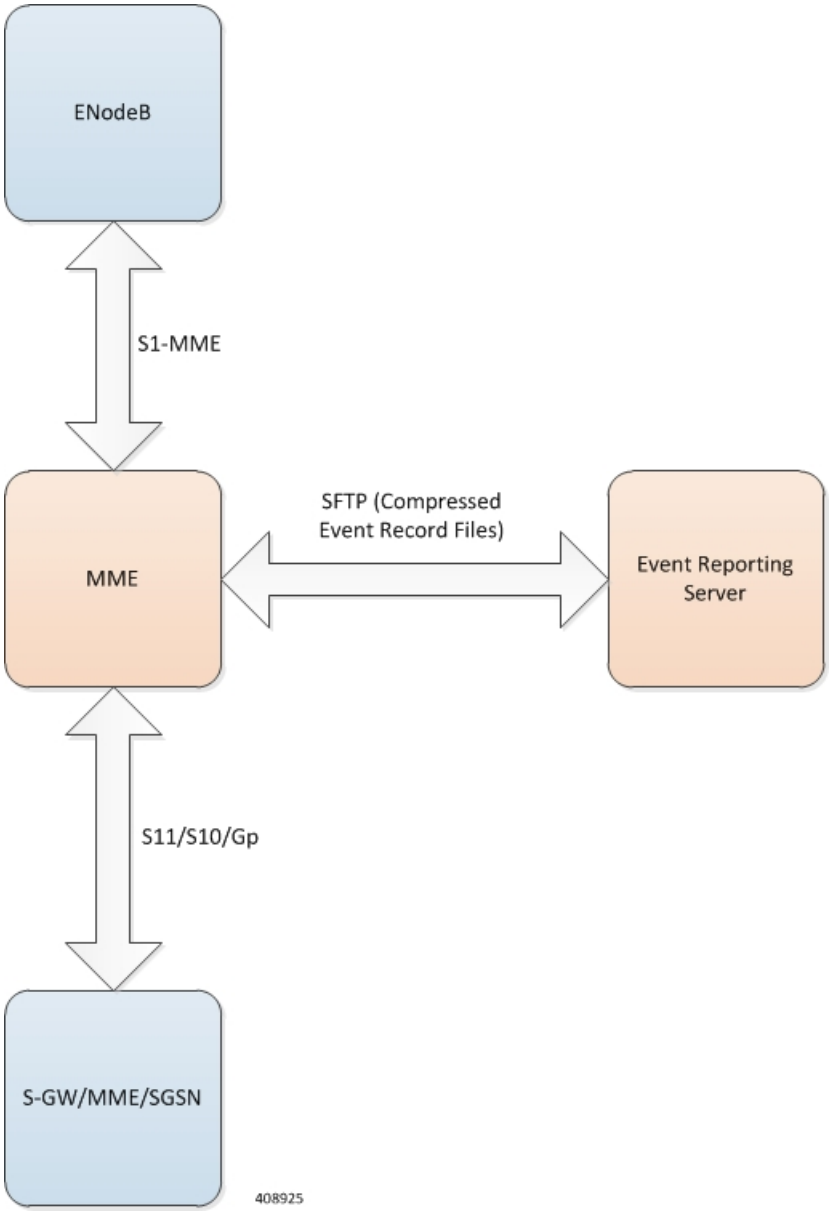
How Event Logging Works

Event Logging in the MME is implemented by providing subscriber event information to an external server. Data analyzers use the event information in the record, which is stored in the external server, to debug and troubleshoot subscriber issues.

Architecture

This section describes the framework designed in the MME to support Event Logging.

Figure 13: Event Logging - Interfaces



The interface between the MME and the external server is based on SFTP. Each record (CSV record) is generated as comma-separated ASCII values. The MME sends one ASCII formatted CSV record per line. The CSV records are stored in a file. If configured, these files can be compressed before sending it to the external server.

The transfer of CSV record files between the MME and the external server is based on either PULL or PUSH model. In case of the PULL model, the external server is responsible for initiating the SFTP with MME, and in the PUSH model, MME is responsible for sending the CSV record file to external server based on the configured PUSH timer interval.

The event report includes the information in CSV format as shown in the table given below.

Table 9: Information Fields in the EDR

Sl.No	Description	Format information	Range
1	smgr_number	Number	1 up to 1023
2	sequence_no	Number	1 up to 4294967295
3	Time	YYYY-MMM-DD+HH:MM:SS.SSS	
4	event-idenity	enum: Attach; Detach; TAU; Handover ; Service Request; Paging; PDN Connect/Disconnect; Bearer Activation/Deactivation; CSFB and SRVCC procedures.	
5	Result	enum: 0-Success; 1-failure; 2-Aborted;3-eps_only	
6	mme-address	Dotted-string	
7	Msisdn	String of decimal digits	
8	imsi	String of decimal digits	1 - 15 digits
9	Imei (sv)	String of decimal digits	14 or 16 digits
10	old-guti	mcc: mnc: mmegroup: mmecode: mtmsi	
11	old-guti-type	Enumeration [0 - native, 1 - mapped]	
12	guti	mcc: mnc: mmegroup: mmecode: mtmsi	0 up to 65535
13	Ecgi	mcc: mnc: cellid	
14	current-tac	Tac	
15	enodeB-id	20 bit value	1 - 1048574
16	disc-reason	Number	0 up to 65535
17	ebi	Number	5-15
18	linked-ebi	Number	

Sl.No	Description	Format information	Range
19	apn	String	
20	pdn-type	Number	1-4
21	ipv4-address	Dotted String	
22	ipv6-address	Dotted String	
23	pti	Number	1-255
24	qci	Number	1-9,65,66, 69,70,128-254
25	arp	Number	1-255
26	qos-change	Enum [0-No, 1-Yes]	0/1
27	lai	mcc-mnc-lac	

If a particular information is not relevant for the procedure being logged or if particular information isn't available, the event record is left blank. For example, if the IMEI is unavailable after the completion of an Attach procedure, the event record is left blank.

Important All enumerations will be listed by Cisco for every software release. The external server is designed to be aware of the same listing and to interpret the number accordingly. The event records contain 0-based index value of such enumerations to save space and processing overhead.

The Event IDs that are tracked as part of the EDR logging is shown in the below table:

Events	ENUM Value
Attach Procedures	
MME_EDR_EVENT_ID_EPS_ATTACH	1
MME_EDR_EVENT_ID_EMERGENCY_ATTACH	2
MME_EDR_EVENT_ID_COMBINED_ATTACH	3
MME_EDR_EVENT_ID_EPS_HO_ATTACH	4
MME_EDR_EVENT_ID_ATTACH_TYPE_MAX	
Detach Procedures	
MME_EDR_EVENT_ID_UE_INITIATED_DETACH	51

Events	ENUM Value
MME_EDR_EVENT_ID_NW_INITIATED_DETACH	52
MME_EDR_EVENT_ID_HSS_INITIATED_DETACH	53
MME_EDR_EVENT_ID_CSFB_UE_INIT_IMSI_DETACH	54
MME_EDR_EVENT_ID_CSFB_NW_INIT_IMSI_DETACH	55
MME_EDR_EVENT_ID_DETACH_TYPE_MAX	
TAU Procedures	
MME_EDR_EVENT_ID_TAU_SGW_RELOC	101
MME_EDR_EVENT_ID_TAU_NO_SGW_RELOC	102
MME_EDR_EVENT_ID_TAU_COMBINED_SGW_RELOC	103
MME_EDR_EVENT_ID_TAU_COMBINED_NO_SGW_RELOC	104
MME_EDR_EVENT_ID_TAU_PERIODIC	105
MME_EDR_EVENT_ID_TAU_ATTACH_SGW_RELOC	106
MME_EDR_EVENT_ID_TAU_ATTACH_NO_SGW_RELOC	107
MME_EDR_EVENT_ID_TAU_ATTACH_COMBINED_SGW_RELOC	108
MME_EDR_EVENT_ID_TAU_ATTACH_COMBINED_NO_SGW_RELOC	109
MME_EDR_EVENT_ID_TAU_TYPE_MAX	
Handover Procedures	
MME_EDR_EVENT_ID_S1_HO_SGW_RELOC	151
MME_EDR_EVENT_ID_S1_HO_NO_SGW_RELOC	152
MME_EDR_EVENT_ID_X2_HO_SGW_RELOC	153
MME_EDR_EVENT_ID_X2_HO_NO_SGW_RELOC	154
MME_EDR_EVENT_ID_INBOUND_S10_HO_SGW_RELOC	155
MME_EDR_EVENT_ID_INBOUND_S10_HO_NO_SGW_RELOC	156
MME_EDR_EVENT_ID_INBOUND_S3_HO_SGW_RELOC	157

Events	ENUM Value
MME_EDR_EVENT_ID_INBOUND_S3_HO_NO_SGW_RELOC	158
MME_EDR_EVENT_ID_INBOUND_GNGP_HO	159
MME_EDR_EVENT_ID_OUTBOUND_S10_HO	160
MME_EDR_EVENT_ID_OUTBOUND_S3_HO	161
MME_EDR_EVENT_ID_OUTBOUND_GNGP_HO	162
MME_EDR_EVENT_ID_HO_TYPE_MAX	
Service Request Procedures	
MME_EDR_EVENT_ID_SERV_REQ_UE_INITIATED	201
MME_EDR_EVENT_ID_SERV_REQ_NW_INIT_PROC	202
MME_EDR_EVENT_ID_SERV_REQ_EXTENDED	203
MME_EDR_EVENT_ID_SERV_REQ_TYPE_MAX	
Paging Procedures	
MME_EDR_EVENT_ID_PAGING_DDN_TRIGGER	251
MME_EDR_EVENT_ID_PAGING_DETACH_TRIGGER	252
MME_EDR_EVENT_ID_PAGING_BRR_TRIGGER	253
MME_EDR_EVENT_ID_PAGING_IDR_QUERY_TRIGGER	254
MME_EDR_EVENT_ID_PAGING_PCSCF_RESTORATION	255
MME_EDR_EVENT_ID_PAGING_UE_OFFLOAD_TRIGGER	256
MME_EDR_EVENT_ID_PAGING_SGS_TRIGGER	257
MME_EDR_EVENT_ID_PAGING_GMLC_TRIGGER	258
MME_EDR_EVENT_ID_PAGING_PGW_NODE_RESTORATION	259
MME_EDR_EVENT_ID_PAGING_S102_TRIGGER	260
MME_EDR_EVENT_ID_PAGING_IPNE_QUERY_TRIGGER	261
MME_EDR_EVENT_ID_PAGING_TYPE_MAX	

Events	ENUM Value
PDN Connectivity Requests	
MME_EDR_EVENT_ID_PDN_CONN_REQ	301
MME_EDR_EVENT_ID_PDN_EMERGENCY_CONN_REQ	302
MME_EDR_EVENT_ID_PDN_CONN_TYPE_MAX	
UE and Network Initiated PDN Detach	
MME_EDR_EVENT_ID_UE_PDN_DISCONN_REQ	351
MME_EDR_EVENT_ID_MME_PDN_DISCONN_REQ	352
MME_EDR_EVENT_ID_HSS_PDN_DISCONN_REQ	353
MME_EDR_EVENT_ID_NW_PDN_DISCONN_REQ	354
MME_EDR_EVENT_ID_PDN_DISCONN_TYPE_MAX	
Dedicated Bearer Activation Requests	
MME_EDR_EVENT_ID_DED_BEARER_ACT_REQ	401
MME_EDR_EVENT_ID_DED_BEARER_ACT_MAX	
Dedicated Bearer Deactivation Requests	
MME_EDR_EVENT_ID_UE_DED_BEARER_DEACT_REQ	451
MME_EDR_EVENT_ID_MME_DED_BEARER_DEACT_REQ	452
MME_EDR_EVENT_ID_PGW_DED_BEARER_DEACT_REQ	453
MME_EDR_EVENT_ID_DED_BEARER_DEACT_MAX	
Bearer Modification Requests	
MME_EDR_EVENT_ID_NW_BEARER_MODIF	501
MME_EDR_EVENT_ID_HSS_BEARER_MODIF	502
MME_EDR_EVENT_ID_BEARER_MODIF_TYPE_MAX	
CSFB Prodecures	
MME_EDR_EVENT_ID_CSFB_MO_CALL	551

Events	ENUM Value
MME_EDR_EVENT_ID_CSFB_MT_CALL	552
MME_EDR_EVENT_ID_CSFB_MO_PRIORITY_CALL	553
MME_EDR_EVENT_ID_CSFB_MT_PRIORITY_CALL	554
MME_EDR_EVENT_ID_CSFB_MO_EMERGENCY_CALL	555
MME_EDR_EVENT_ID_CSFB_MO_SMS	556
MME_EDR_EVENT_ID_CSFB_MT_SMS	557
MME_EDR_EVENT_ID_ECSFB_MO_CALL	561
MME_EDR_EVENT_ID_ECSFB_MT_CALL	562
MME_EDR_EVENT_ID_ECSFB_EMERGENCY	563
SRVCC Procedures	
MME_EDR_EVENT_ID_SRVCC_SV_CSPS	601
MME_EDR_EVENT_ID_SRVCC_SV_CS	602
MME_EDR_EVENT_ID_SRVCC_SV_NO_DTM	603
MME_EDR_EVENT_ID_SRVCC_1XRTT	604
MME_EDR_EVENT_ID_SRVCC_MAX	

The status of each event is as shown in the table given below:

Table 10: Event Status

Sl No.	Format Information	ENUM Value
1	MME_EDR_EVENT_RESULT_SUCCESS	0
2	MME_EDR_EVENT_RESULT_FAILURE	1
3	MME_EDR_EVENT_RESULT_ABORT	2
4	MME_EDR_EVENT_RESULT_EPS_ONLY	3

Limitations

The reliability of event generation is limited by the CDRMOD framework – particularly in the following ways:

- Any reboot of the chassis, will result in loss of records that are not yet flushed to the hard-disk or an external server
- In case of overload of the CDRMOD, the SESSMGR ignores event records if the queue is full.
- EDR sequence numbers are within the scope of the Session Manager. If a different Session Manager is selected, the EDR sequence number may reset or continue from the last sequence number allocated in that Session Manager.
- The statistics are key parameters for logging EDRs, if the statistics have any discrepancies the EDRs are not generated. Listed below are some scenarios where the EDRs are not generated due to discrepancies in statistics:
  - Network or MME initiated dedicated bearer de-activation during SRVCC procedures.
  - HSS initiated modification failures.
  - HSS initiated PDN disconnect failures.

Relationship with Other Products

The SGSN has a similar function, GMM-SM Event Logging. For information about this functionality refer to the *SGSN Administration Guide.*

Configuring Event Logging

The following configurations are discussed in this section for Event Data Records (EDRs):

Enabling Event Logging

The following CLI configuration is executed in the Call Control Profile mode to enable Event Logging on the MME.

config
call-control-profile *profile_name*
reporting-action mme-event-record
exit

Notes:

- The call-control-profile configuration enables Event Logging for MME, provided this profile is associated to the **mme-service** through operator policy and subscriber map.
- **reporting-action** enables procedure reports.
- **mme-event-record** reports MME procedures in the form of event records using CDRMOD.

Enabling EDR Logs

The CDRMOD proclet writes the individual records into a single file received from several session managers. The CDRMOD proclet is enabled with the configuration below.

config
context *context_name*
edr-module active-charging-service reporting
cdr { push-interval *interval_time* **| remove-file-transfer | use-harddisk | transfer-mode { pull | push primary { encrypted-url | url }** *url* **[secondary { encrypted-secondary | secondary-url }** *url_* **] } [module-only] }**
end

Configuring File Parameters

File parameters can be configured using the configuration given below.

config
context *context_name*
session-event-module
file name *file_name* **current-prefix** *current_file_prefix* **rotation volume** *file_rotation_size* **rotation time** *file_rotation_time* **field-separator underscore sequence-number padded charging-service-name include compression gzip }**
end

EDR Profile Association

The Call Control Profile configuration enables event Logging for MME, provided the EDR profile is associated to the MME-Service through Operator Policy and Subscriber Map (LTE-Policy).

config
operator-policy name *policy_name*
associate call-control-profile *edr_profile_name*
`exit`
lte-policy
subscriber-map *map_name*
precedence *precedence_value* **match-criteria all operator-policy-name** *policy_name*
`exit`
`exit`
context *context_name*
mme-service *service_name*
associate subscriber-map *map_name*
end

Verifying the Event Logging Configuration

The following commands are used to verify the parameters for Event Logging.

- **show call-control-profile full all**
- **show operator-policy full all**

- **show lte-policy subscriber-map name sub1**
- **show mme-service all**

Monitoring and Troubleshooting Event Logging

This section provides information on how to monitor Event Logging.

Event Logging Show Command(s) and/or Outputs

This section provides information regarding show commands and/or their outputs in support of Event Logging.

The show commands in this section are available in support of the Event Logging.

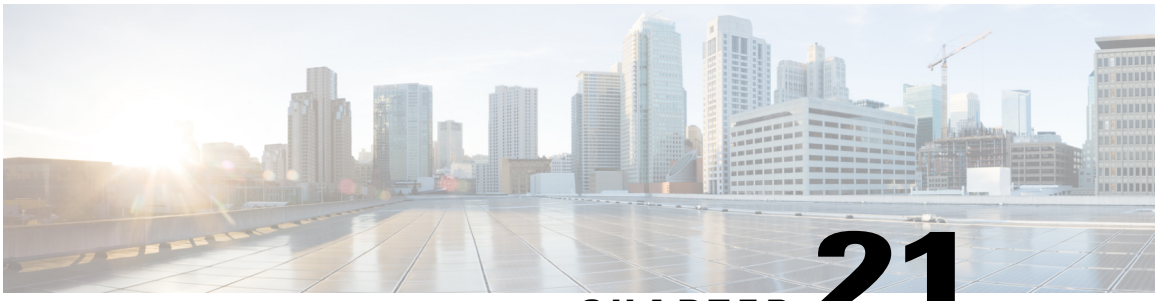
show call-control-profile full all

```
Call Control Profile Name = TEST
SAMOG Home PLMN                                    : Not configured
Accounting Mode (SGW/SaMOG)                      : None
Accounting stop-trigger (SGW)                  : Not configured
Accounting Policy (SaMOG)                        : Not configured
Event Data Records (MME)                          : Enabled
```

show cdr statistics

On running the above command , the following statistics are displayed:

```
EDR-UDR file Statistics:
CDRMOD Instance Id: 2
    Overall Statistics:
      Files rotated:
          30
      Files rotated due to volume limit:                                    0
      Files rotated due to time limit:                                        3
      Files rotated due to tariff-time:                                      0
      Files rotated due to records limit:                                 11
      File rotation failures:
   0
      Files deleted:
            7
      Records deleted:
          0
      Records received:
 23754
      Current open files:
       0

Time of last file deletion:                            Sunday November 08 23:32:53 EST
2015
Session-Event Record Specific Statistics:
Session-Event files rotated:                                                  30
Session-Event files rotated due to volume limit:                 0
Session-Event files rotated due to time limit:                     3
Session-Event files rotated due to tariff-time:                   0
Session-Event files rotated due to records limit:              11
    Session-Event file rotation failures:                                  0
    Session-Event files deleted:                                             7
    Session-Event records deleted:                                         0
    Session-Event records received:                                  23754
    Current open Session-Event files:                                      0
Time of last Event file deletion:                Sunday November 08 23:32:53 EST 2015
```



CHAPTER 21

Foreign PLMN GUTI Management

This feature allows operators to gain some savings on signaling by avoiding DNS request attempts to foreign PLMNs if a foreign PLMN GUTI is not allowed.

Feature Description

In releases prior to 15.0, all Attach and TAU Requests containing a foreign GUTI would result in a DNS lookup for the peer MME or SGSN, followed by an S10, S3 or Gn/Gp Identification or Context Request. This could result in significant delay when the GUTI is from a foreign PLMN, which the local MME cannot access.

Beginning with Release 15.0, a Foreign PLMN GUTI Management Database can be configured to allow or immediately reject Attach Requests or TAU Requests containing a GUTI from a foreign PLMN. This Foreign PLMN GUTI Management Database contains as many as 16 entries, where each entry consists of a PLMN (MCC and MNC) and an action, which can either be Allow or Reject. If the action is Reject, the MME will not perform any DNS requests to locate a peer MME or SGSN to which any foreign GUTI from that foreign PLMN maps.

How it Works

When an Attach Request or TAU Request containing a foreign GUTI is received, the MME must first determine if the GUTI's PLMN matches either the MME's own PLMN or one of the MME's shared PLMNs. If such a match is found, the foreign GUTI belongs to a local PLMN, no foreign PLMN check is made, and a DNS request for a peer MME or SGSN may be made as the request is processed normally. If the GUTI's PLMN does not match either the MME's own PLMN or one of the MME's shared PLMNs, the foreign GUTI belongs to a foreign PLMN and the MME Service is checked for an association to a Foreign PLMN GUTI Management Database. If there is no such association, all Attach Requests and TAU Requests containing foreign GUTIs from foreign PLMNs are allowed to be processed, and a DNS request for a peer MME or SGSN may be made.

If an association to a Foreign PLMN GUTI Management Database is present, the database is checked for a matching foreign PLMN. If no match is found, the MME continues processing the Attach Request or TAU Request, and a DNS request may be made. If a match is found, the action specified for the foreign PLMN (either Allow or Reject) is applied. If the action is Reject, and the request is a TAU Request, a TAU Reject message is sent immediately with cause code 9 (UE Identity cannot be derived by the network), and no DNS lookup is performed to find a peer MME or SGSN. If the action is Reject, and the request is an Attach Request, the MME sends a NAS Identity Request to the UE to determine its IMSI, and no DNS lookup is performed to find a peer MME or SGSN. If the action is Allow, the MME continues processing the Attach Request or TAU Request, and a DNS request may be made.

If a TAU Request containing a foreign GUTI is rejected due to its PLMN being present in the Foreign PLMN GUTI Management Database, the mme-foreign-plmn-guti-rejected session disconnect reason will be incremented.

Similarly, the emmdisc-foreignplmnreject bulk statistic counter, which tracks the number of times this disconnect reason, is incremented..

Configuring Foreign PLMN GUTI Management

This section explains the configuration procedures required to enable this feature.

Creating a Foreign PLMN GUTI Management Database

A Foreign PLMN GUTI Management Database is configured as part of the LTE Policy configuration mode.

config
lte-policy
foreign-plmn-guti-mgmt-db *fguti_db_name*
end

Up to four Foreign PLMN GUTI Management Databases can be configured.

To delete an existing database, in the lte-policy mode include the **no** prefix with the command. You need to identify the database to be deleted.

no foreign-plmn-guti-mgmt-db fguti-db1

Configuring Foreign PLMN GUTI Management Database Entries

A Foreign PLMN GUTI Management Database entry consists of an MCC, an MNC, and an action (either Allow or Reject). The following example creates two entries:

configure
lte-policy
foreign-plmn-guti-mgmt-db*db_name*
plmn mcc *123* **mnc** *456* **allow**
plmn mcc *321* **mnc** *654* **reject**
end

The **any** keyword may be used as a wildcard in place of both the MCC and MNC values, or in place of an MNC value with a specific MCC value. In other words, the following commands are allowed:

plmn mcc 123 mnc any allow
plmn mcc any mnc any reject

Important The examples listed above are only to understand the significance of the keyword **any**. The examples do not suggest any particular order of configuration.

However, a wildcard MCC is not allowed with a specific MNC value. For example, the following command is not allowed:

plmn mcc any mnc 456 allow

It is strongly recommended that a Foreign PLMN GUTI Management Database contain an **mcc any mnc any** entry in order to define the default behavior when a GUTI with an unknown MCC / MNC combination is received. If such an entry is absent, the default behavior will be to allow Attach Requests and TAU Requests with unknown MCC/ MNC combinations, which may result in DNS lookups for peer MMEs and SGSNs. This default behavior would be the same as if there were no Foreign PLMN GUTI Management Database defined.

Up to 16 foreign PLMN entries can be added to a database.

The **no** prefix followed by a PLMN ID removes a specific entry from the database. Refer to the following example:

no plmn mcc 123 mnc 456

Associating an MME Service with a Foreign PLMN GUTI Management Database

An MME Service can be associated with a database using the **associate foreign-plmn-guti-mgmt-db** command in MME Service Configuration mode.

configure
context *ctxt_name*
mme-service *mme_svc*
associate foreign-plmn-guti-mgmt-db *db_name*
end

Multiple MME Services may be associated with a single Foreign PLMN GUTI Management Database. Because of this, it is not possible to cross-check the PLMNs in the database against an MME Service's own PLMN or its shared PLMNs. However, the MME Service's own PLMN or shared PLMNs will never be checked against the Foreign PLMN GUTI Management Database, regardless of whether those PLMNs are configured in the database or not. In other words, any Attach Request or TAU Request containing a GUTI from the MME Service's own PLMN or one of its shared PLMNs will always be processed, and may result in a DNS lookup for a peer MME or SGSN.

The association can be removed using the following command:

no associate foreign-plmn-guti-mgmt-db

Verifying the Configuration

Use the following command to display the list of Foreign PLMN GUTI Management databases configured on the system:

show lte-policy foreign-plmn-guti-mgmt-db summary

Use the following command to display the entries configured within a specific Foreign PLMN GUTI Management Database:

show lte-policy foreign-plmn-guti-mgmt-db name *fguti-db1*

```
Foreign PLMN GUTI Mgmt DB fguti-db1
```

```
PLMN mcc 123 mnc 456 allow
PLMN mcc 321 mnc 654 reject
PLMN mcc any mnc any reject
PLMN mcc 123 mnc any allow
```

Use the following command to display the Foreign PLMN GUTI Management database to which an MME Service has been associated:

show mme-service name *mme_svc_name*
Refer to the Foreign-PLMN-GUTI-Mgmt-DB field in the output, as shown here:

```
Foreign-PLMN-GUTI-Mgmt-DB            : fguti-db1
```

Monitoring Foreign PLMN GUTI Management

This section provides information on how to monitor the Foreign PLMN GUTI Management feature.

Show Command(s) and/or Outputs

This section provides information regarding show commands and/or their outputs relating to this feature.

show session disconnect-reasons

If a TAU Request containing a foreign GUTI is rejected due to its PLMN being present in the Foreign PLMN GUTI Management Database, the following session disconnect reason is incremented.

- mme-foreign-plmn-guti-rejected(534)

Bulk Statistics

MME Schema

The following statistic is included in the MME Schema in support of the Foreign PLMN GUTI feature:

- emmdisc-foreignplmnreject

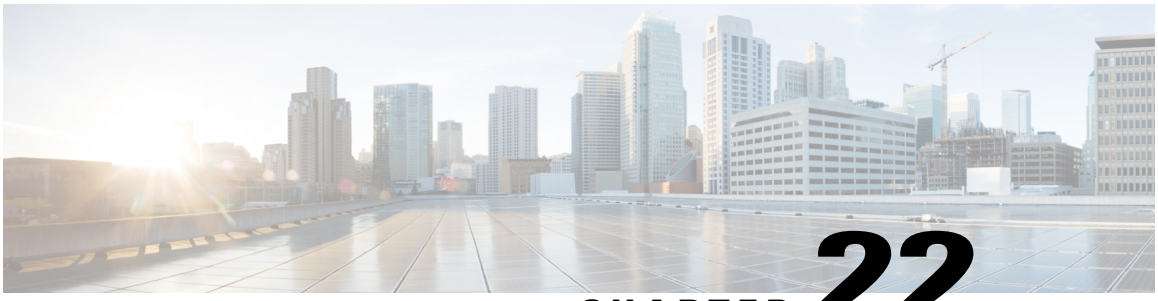
This statistic increments when an Attach or TAU request containing a foreign GUTI is rejected due to restrictions set in the Foreign PLMN GUTI Management Database.

System Schema

The following statistic is also included in the System Schema in support of the Foreign PLMN GUTI feature:

- disc-reason-534: mme-foreign-plmn-guti-rejected(534)

This statistic increments when a session is disconnected due to the restrictions set in the Foreign PLMN GUTI Management Database.



CHAPTER 22

GTP-C Load and Overload Control on MME

Feature Description

Overload of packet core network nodes in the network results in service de-gradation. Overload conditions can occur in various network scenarios. Overload issue can be addressed through improved load distribution over the network.

GTP-C load and overload control feature adds MME support for GTP-C load and overload control mechanism on S11 interface. GTP-C load and overload control is a standard driven (3GPP TS 29.807 V12.0.0 and 3GPP TS 29.274 V d30) feature. For standards compliance information see the Standards Compliance section in this feature chapter.

Important This feature is license controlled. The "EPC Support for GTP Overload Control" license is required for successfully configuring and enabling this feature. Please consult your Cisco Account Representative for information about the specific license.

GTP-C Overload Issues and Resultant effects

A GTP-C overload occurs when the number of incoming requests exceeds the maximum request throughput supported by the receiving GTP-C entity. The GTP-C is carried over UDP transport, and it relies on the re-transmissions of unacknowledged requests. When a GTP-C entity experiences overload (or severe overload) the number of unacknowledged GTP-C messages increase exponentially and this leads to a node congestion or even node collapse. An overload or failure of a node further leads to an increase of the load on the other nodes in the network and in some cases into a network issue.

Listed below are some examples of GTP-C signaling based scenarios which lead to GTP-C overload:

- A traffic flood resulting from the failure of a network element, inducing a signaling spike.

- A traffic flood resulting from a large number of users performing TAU/RAU or from frequent transitions between idle and connected mode.
- An exceptional event locally generating a traffic spike for example a large amount of calls (and dedicated bearers) being setup almost simultaneously.
- Frequent RAT re-selection due to scattered Non-3GPP (for example, Wi-Fi) coverage or a massive mobility between a 3GPP and Non-3GPP coverage. This may potentially cause frequent or massive inter-system change activities.

GTP-C overload may result in any of the following service impacts:

- Loss of PDN connectivity (IMS, Internet and so on) and associated services.
- Loss of ability to setup and release radio and core network bearers necessary to support services, for example GBR bearers for VoLTE.
- Loss of ability to report to the PGW/PCRF user's information changes, for example location information for emergency services and lawful intercept, changes in RAT or QoS.
- Billing errors which result in loss of revenue.

Overview

GTP-C load control and overload control are complimentary concepts which can be supported and activated independently on the network. This feature uses the existing EGTPC infrastructure to gather and distribute load and overload control information across session managers. In broad terms GTP-C load control can be described as a preventive action and GTP-C overload control can be described as a corrective action. A GTP-C entity is termed as overloaded when it operates over and above its signaling capacity resulting in a diminished performance (including impacts to handling of incoming and outgoing traffic).

The advantages of enabling GTP-C load control are listed below:

- Load control allows better balancing of the session load; this prevents an GTP-C overload scenario.
- Load control enables a GTP-C entity (for example SGW or PGW) to send its load information to a GTP-C peer (for example a MME or SGSN, ePDG, TWAN) to adaptively balance the session load across entities supporting the same function (for example SGW cluster) according to their effective load. The load information reflects the operating status of the resources of the GTP-C entity.
- Load control does not trigger overload mitigation actions even if the GTP-C entity reports a high load.

The advantages of enabling GTP-C overload control are listed below:

- Overload control prevents a GTP-C entity from becoming or being overloaded to gracefully reduce its incoming signaling load by instructing its GTP-C peers to reduce sending traffic according to its available signaling capacity to successfully process the traffic.
- Overload control aims at shedding the incoming traffic as close to the traffic source as possible when an overload has occurred.

Operational Benefits of GTP-C Load and Overload Control Support on MME:

- Improved load distribution on SGW and PGW this in turn reduces the occurrence of PGW/SGW overload.

- The MME pro-actively advertises its overload information so that the peer nodes SGW/PGW can reduce the traffic.
- The MME can reduce the traffic towards the peer SGW/PGW if they are overloaded.

Relationships to Other Features

This feature utilizes the existing EGTPC infrastructure to gather and distribute load and overload control information across session managers.

How it Works

This section describes the detailed working mechanism of this feature.

Limitations

- APN level load and overload control is not supported

Standards Compliance

The GTP-C load and overload control feature complies with the following standards:

- 3GPP TS 29.807,version 12.0.0
- 3GPP TS 29.274, version 13.3.0 and beyond

Configuring GTP-C Load and Overload Control on MME

The following configuration procedures are used to configure the GTP-C load and overload control feature.

Configuring GTP-C Load or Overload Control Profile

The **associate** command associates or disassociates supportive services and policies with an MME service. New keywords **gtpc-load-control-profile** and **gtpc-overload-control-profile** are introduced in the **associate** command to configure the GTP-C load control profile and GTP-C overload control profile.

configure
context *context_name*
mme-service *service_name*
associate { { egtp-service *egtp_svc_name* **| egtp-sv-service** *egtp_sv_svc_name* **| foreign-plmn-guti-mgmt-db** *db_name* **| gtpc-load-control-profile** *profile_name* **| gtpc-overload-control-profile** *profile_name* **| henbgw-mgmt-db** *db_name* **| hss-peer-service** *hss_svc_name* **| ipne-service** *ipne_svc_name* **| location-service** *location_svc_name* **| lte-emergency-profile** *profile_name* **| network-global-mme-id-mgmt-db | s102-service** *s102_svc_name* **[context** *context_name* **] | sbc-service** *sbc_svc_name* **| sctp-param-template** *template_name* **| sgs-service** *sgs_svc_name* **| sgtpc-service**

sgtpc_svc_name **} [context** *ctx_name* **] | subscriber-map** *map_name* **| tai-mgmt-db** *database_name* **}**
no associate { egtp-service | egtp-sv-service | foreign-plmn-guti-mgmt-db | gtpc-load-control-profile | gtpc-overload-control-profile| henbgw-mgmt-db | hss-peer-service | ipne-service | location-service | lte-emergency-profile | network-global-mme-id-mgmt-db | s102-service | sctp-param-template | sgs-service | sgtpc-service | subscriber-map | tai-mgmt-db }

Notes:

- The keyword **gtpc-load-control-profile** is used to configure GTP-C Load Control Profile for this MME service.
- The keyword **gtpc-overload-control-profile** is used to configure GTP-C Overload Control Profile for this MME service.
- The *profile_name* is a string of size 1 up to 64.
- These CLI commands are not enabled by default.

Configuring Usage of GTP-C Load Information in SGW/PGW Selection

The gw-selection command configures the parameters controlling the gateway selection process. A new keyword **gtp-weight** is introduced as a part of this feature which is the weight value calculated from the Load Control Information received from the GTP peers.

configure
call-control-profile *profile_name*
[remove] gw-selection {co-location [weight [prefer{ sgw | pgw }]|| gtp-weight | pgw weight | sgw weight | topology [weight [prefer { sgw | pgw }]] }
exit

Notes:

- The option enables the MME selection of SGW and PGW based on the advertised load control information.
- This configuration can be applied selectively to subscribers.
- This CLI is not enabled by default.

Configuring MME Manager and IMSI Manager CPU Utilization to Calculate Overload Factor

This new command allows the user to configure the inclusion of CPU utilization of Session Manager, Demux Manager, IMSI Manager and MME Manager under GTP-C overload control profile for overload factor calculation.

configure
gtpc-overload-control-profile*profile_name*
cpu-utilization {sessmgr-card | demuxmgr-card | imsimgr | mmemgr}
no cpu-utilization
default cpu-utilization
exit

Notes:

- The **default** behavior for the above CLI is to include the average CPU utilization of Sessmgr cards and Demuxmgr card in the overload factor calculation.
- The **no** keyword disables the configuration of CPU utilization of Sessmgr/Demuxmgr/IMSImgr/MMEmgr under GTP-C overload control profile for overload factor calculation.
- The keyword **sessmgr-card** configures the inclusion of average cpu-utilization of SessMgr cards for overload factor calculation.
- The keyword **demuxmgr-card** configures the inclusion of average cpu-utilization of Demux Manager card for overload factor calculation.
- The keyword **imsimgr** configures the inclusion of cpu-utilization of IMSIMgr(s) proclet for overload factor calculation.
- The keyword **mmemgr** configures the inclusion of cpu-utilization of MMEMgr(s) proclet for overload factor calculation.

Sample Configuration

```
configure
  call-control-profile profile_name
    gw-selection topology weight prefer pgw
    gw-selection gtp-weight
exit
operator-policy namepolicy_name
  associate call-control-profile profile_name
exit
lte-policy
  subscriber-mapmap_name
    precedence xmatch-criteria all operator-policy-name policy_name
  exit
exit
context ingress
  mme-serviceservice_name
    bind s1-mme ipv4-address x.x.x.x
    s1-mme sctp portxx
    mme-id group-idxxxxx mme-codex
    plmn-id mcc xxx mnc xxx
    associate egtp-service egtp_mme context ingress
    associate mme-hss-service mme_hss contexthss
    associate subscriber-mapmap_name
    associate gtpc-load-control-profileprofile_name
    associate gtpc-overload-control-profile profile_name
  exit
exit
end
```

Verifying the Configuration

The configuration of this feature can be verified using the following show commands.

Execute the **show configuration** command to verify the configuration, the part of the output related Call Control Profile displays the following parameters based on the configuration:

- **gw-selection: gtp-weight**

The parameter **gtp-weight** identifies GTP-C load based SGW or PGW selection.

Execute the **show configuration** command to verify the configuration, the part of the output related to MME Service Configuration displays the following parameters based on the configuration:

- **associate gtpc-load-control-profile profile_name**
- **associate gtpc-overload-control-profile profile_name**

Execute the **show configuration** command to verify the configuration, the part of the output related to GTP-C overload control profile Configuration displays the following parameters based on the configuration:

- **cpu-utilization: sessmgr-card demuxmgr-card imsimgr mmemgr**

The **cpu-utilization** is used to configure the inclusion of CPU utilization of Session Manager, Demux Manager, IMSI Manager and MME Manager under GTP-C overload control profile for overload factor calculation.

Monitoring and Troubleshooting the GTP-C Load and Overload Control Feature

This section provides information regarding show commands and bulk statistics for this feature.

Troubleshooting

Listed below are the troubleshooting steps for any issues encountered during configuration or functioning of the GTP-C Load and Overload control feature:

Important All configuration parameters newly added will be recovered during Session Manager re-starts. The LCI/OCI information of SGW/PGW peer nodes are recovered during Session Manager restarts.

Step 1:

If the CLI commands required to enable the feature are not visible, ensure that the GTP-C Load and Overload feature control license is present and enabled.

Step 2:

If MME selection of SGW and PGW based on load control information is not working, verify the following:

- Ensure that the load control profile is associated with the MME service, for more information see the section on “Configuring GTP-C Load or Overload Control Profile” in this feature chapter.
- Ensure that the overload control profile is associated with the MME service, for more information see the section on “Configuring GTP-C Load or Overload Control Profile” in this feature chapter.
- Verify if the load and overload feature is associated and feature is enabled, execute the show commands **show mme-service all** and **show egtp-service name** *service_name*.

- Verify if the MME has started learning the LCI/OCI information from peer nodes using following show commands:

show egtpc peers
show egtpc peers sessmgrs
show egtpc peers address *x.x.x.x*
show egtpc statistics sgw-address *x.x.x.x*
show egtpc statistics remote-peer-address *x.x.x.x*
show subscribers summary mme-service *service-name* **sgw-address** *x.x.x.x*
show subscribers summary mme-service *service-name* **pgw-address** *x.x.x.x*
show egtpc statistics egtp-service *service-name*

- Ensure the configuration to consider LCI/OCI information in node selection is enabled. For more information see the section “Configuration to use GTPC load information in SGW/PGW selection” in this feature chapter. Execute the show command **show call-control-profile full all** to verify the same.
- For the GTP dynamic weight (that is, LCI/OCI) to work in case of DNS based node selection, following DNS weight based configuration should be present in the call control profile.
  - In case of SGW selection:

    configure
    call-control-profile *profile_name*
    gw-selection sgw weight
    end

    Please refer to the section " DNS SGW selection with Load Control Information" in this feature chapter.
  - In case of PGW selection:

    configure
    call-control-profile *profile_name*
    gw-selection pgw weight
    end

    Please refer to the section " DNS PGW selection with Load Control Information" in this feature chapter.
  - During Topology based selection:

    configure
    call-control-profile *profile_name*
    gw-selection topology [weight [prefer { pgw|sgw }]]
    end

    Please refer to the section "Topology" in this feature chapter.
  - When Co-location is enabled:

    configure
    call-control-profile *profile_name*
    gw-selection co-location [weight [prefer { pgw|sgw }]]
    end

    Please refer to the section "Co-location" in this feature chapter.

Step 3:

If the MME Selection of SGW using DNS does not result in expected session distribution on the SGW.

- Ensure that Steps 1 and 2 are working as explained earlier in this section.

- Collect the data for following show commands at regular intervals of time to observe if the distribution is happening or not:

  show egtpc peers
  show egtpc peers sessmgrs
  show egtpc peers address *x.x.x.x*
  show egtpc statistics sgw-address *x.x.x.x*
  show egtpc statistics remote-peer-address *x.x.x.x*
  show subscribers summary mme-service *service-name* **sgw-address** *x.x.x.x*

Step 4:

If the MME Selection of PGW using DNS does not result in expected session distribution on the SGW.

- Ensure that Steps 1 and 2 are working as explained earlier in this section.
- Collect the data for following show commands at regular intervals of time to observe if the distribution is happening or not:

  show egtpc peers
  show egtpc peers sessmgrs
  show egtpc peers address *x.x.x.x*
  show egtpc statistics remote-peer-address *x.x.x.x*
  show subscribers summary mme-service *service-name* **pgw-address** *x.x.x.x*
  show egtpc statistics egtp-service *service-name*

Step 5:

If MME Selection of SGW and PGW using topology is not resulting in expected session distribution on SGW/PGW.

- Ensure that Steps 1 and 2 are working as explained earlier in this section.
- Collect the data for following show commands at regular intervals of time to observe if the distribution is happening or not:

  show egtpc peers sessmgrs
  show egtpc peers address *x.x.x.x*
  show egtpc statistics sgw-address *x.x.x.x*
  show egtpc statistics remote-peer-address *x.x.x.x*
  show subscribers summary mme-service *service-name* **sgw-address** *x.x.x.x*
  show subscribers summary mme-service *service-name* **pgw-address** *x.x.x.x*
  show egtpc statistics egtp-service *service-name*

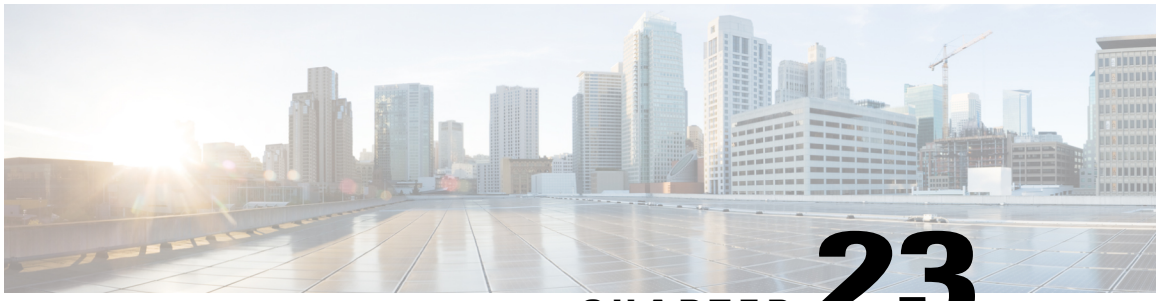
Step 6:

If the MME is not reporting overload control information, follow the steps described below:

- Ensure that Step 1 is working as explained earlier in this section.
- Ensure that the overload control profile is associated with the MME Service. For more information see the section “Configuring GTP-C Load or Overload Control Profile” in this feature chapter.
- Execute the following show commands to verify if the feature is enabled:
  - **show mme-service all**
  - **show egtp-service name egtp_mme**

- Verify the parameters configured through the commands inclusion-frequency, message- prioritization, overload-control-handling, overload-control-publishing, self-protection-behavior, tolerance, throttling-behavior, validity-period and weightage under the GTPC Overload Profile Configuration Mode. Execute the following show command to verify the same:

  show gtpc-overload-control-profile *profile_name*



CHAPTER 23

GUTI Re-allocation

Feature Description

Overview

The Globally Unique Temporary Identity (GUTI) is assigned to the UE by the MME the GUTI is used to support subscriber identity confidentiality. The GUTI has two parts, the Globally Unique Mobility Management Entity Identifier (GUMMEI), which identifies the network, and the M-TMSI, which identifies the device. This feature enables GUTI Re-allocation for an UE based on time and frequency of access attempts per UE.

How It Works

The MME currently performs GUTI allocation during UE attaches. The GUTI once allocated is retained until the DB associated with the UE is purged. This feature introduces MME support to perform GUTI Reallocation for securing the TMSI allocated to UE. GUTI Reallocation is triggered based on configured frequency of access attempts or periodicity.

A configured frequency of "n" requests triggers GUTI Reallocation for every "nth" ATTACH / TAU / SERVICE REQUEST received from the UE. Here 'n' is the sum of the received ATTACH / TAU/ SERVICE Request. A configured periodicity of "t" minutes triggers GUTI Reallocation at every "t" minutes for a UE.

The frequency-based GUTI reallocation is independent of the configured periodicity. However, periodicity-based GUTI reallocation attempts are relative to the last attempted UE GUTI Reallocation time. The last attempted GUTI Reallocation time for a UE is updated whenever a GUTI Reallocation for a UE is attempted irrespective of the trigger (frequency/periodicity).

The MME initiates GUTI Reallocation only if the NAS signaling connection with the UE is present. If the NAS signaling connection is not present the UE shall not be paged. If the NAS signaling connection with the

UE is absent, GUTI reallocation is performed whenever the NAS signaling connection with the UE is established.

Note GUTI Reallocation is not triggered when UE is always in connected mode as, GUTI Reallocation based on periodicity is performed only when the either Attach, periodic TAU, Service request is received by MME and the configured periodicity time has been reached. For a UE that is always in connected mode neither of these events occur. The session are not disturbed during GUTI Reallocation, idle-active transitions are a frequent occurrence in the network, therefore GUTI Reallocation should happen for most UE's at the configured periodicity/frequency during service request procedure.

The Reallocated GUTI is sent in the NAS Attach Accept, NAS TAU Accept and NAS GUTI Relocation Command messages.

Limitations

The MME does not perform GUTI Reallocation if the subscriber is marked for offload or if the subscriber is executing an outbound handover procedure.

The GUTI reallocation retries for UE's which do not adhere to specifications is limited by the MME. MME detaches such UEs after "10" consecutive failure attempts of GUTI Reallocation. This behavior and number of consecutive failures to trigger detach is not configurable.

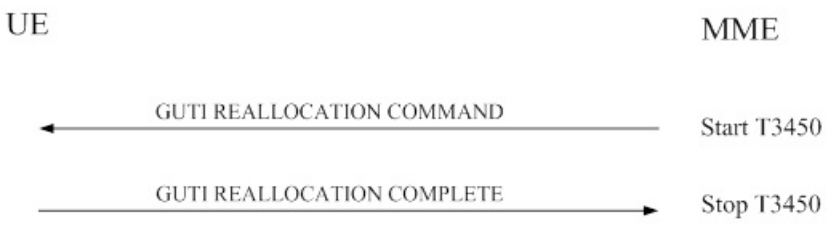
The **frequency** and **periodicity** configured to trigger authentication/GUTI reallocation requires the new session setup message (NAS Attach/TAU) to be processed by the Session Manager instance which has the corresponding MME DB for the subscriber. If the MME DB is not available the **frequency** and **periodicity** triggers will not work. For example, if the mobile identifier in the NAS Attach/TAU message is a foreign GUTI and additional GUTI is not present, the MME does not trigger authentication/GUTI reallocation for the subscriber based on frequency/periodicity.

Reallocated GUTI is not sent in TAU accept for TAU with type TA Update. In this scenario, once the frequency criteria for TAU is met, GUTI reallocation is performed on receiving the next periodic TAU or Service request. This to prevent the case where, TAU complete for an TAU accept with Reallocated GUTI is not received by MME. Wherein upon receiving a paging trigger, MME needs to page the UE in both the TAI lists (before and after TAU) with both the GUTI (previous and reallocated). In the case of SGSN , paging message is sent to the RNC with acknowledged PTMSI and unacknowledged (reallocated) PTMSI. However paging is sent only for the current RAI. Similarly in the case of MME, MME has to send paging message to the eNodeB's with acknowledged GUTI and unacknowledged GUTI (reallocated). But paging needs to be sent in both current TAI list and previous TAI list.

Flows

The following diagram illustrates the messages exchanged during network-initiated GUTI re-allocation:

Figure 14: GUTI Re-allocation



1. The MME sends GUTI REALLOCATION COMMAND message to the UE. The time duration for the T3450 timer starts. This timer starts when the MME initiates a Globally Unique Temporary Identifier (GUTI) reallocation procedure by sending a GUTI REALLOCATION COMMAND message to the UE and stops upon receipt of the GUTI REALLOCATION COMPLETE message.
2. The UE sends a GUTI REALLOCATION COMPLETE message to the MME on completion of the GUTI Re-allocation procedure. The T3450 timer stops once the MME receives the GUTI REALLOCATION COMPLETE message.

Configuring GUTI Re-allocation

The following configuration command is used to configure the periodicity (time interval) / frequency of GUTI Reallocation for a UE:

config
call-control-profile *<profile_name>*
[remove] guti reallocation [frequency *<frequency>* **| periodicity** *<duration>* **]**
end

Notes:

- The keyword **guti** identifies the Globally Unique Temporary UE Identity (GUTI).
- The keyword **reallocation** specifies reallocation of GUTI.
- The **frequency** configured specifies the GUTI reallocation frequency. The frequency is an integer with a range "1" up to "65535" requests.
- The **periodicity** configured specifies GUTI reallocation periodicity. The periodicity is an integer with a range "1" up to "65535" minutes.
- GUTI reallocation is disabled by default. The **remove** keyword is used to remove the configured GUTI reallocation frequency and periodicity specified in the call control profile configuration.

Monitoring and Troubleshooting GUTI Re-allocation

This section provides information regarding show commands and/or their outputs in support of the GUTI reallocation feature in MME.

GUTI Re-allocation Show Command(s) and/or Outputs

show call-control-profile full all

The following new fields are added to the show output to display the configured GUTI Reallocation parameters:

- GUTI Reallocation
- GUTI Reallocation Frequency
- GUTI Reallocation Periodicity

show session disconnect-reasons verbose

The following new disconnect reason is added for GUTI Reallocation:

- mme-guti_realloc_failed-detach

show mme-service statistics

The following new fields are added to the show output to display the configured GUTI Reallocation parameters:

- GUTI Reallocation
- Attempted
- Failures
- Success
- GUTI Reallocation
- Attach Accept
- Retransmission
- TAU Accept
- Retransmission
- GUTI Reallocation cmd
- Retransmission

Below is an example displaying the EMM Statistics listed above:

```
EMM  Statistics:
   .  .  .
GUTI Reallocation:
```

```
Attempted               : 176807
Success                 : 176691
Failures                : 116
```

Below is an example displaying the Total EMM Control Messages listed above:

```
Total EMM Control Messages::
  .  .  .
GUTI Reallocation:
Attach Accept:   180094              Retransmissions: 0
TAU Accept:      892098              Retransmissions: 0
GUTI Reallocation Cmd:   389986      Retransmissions: 0
```

show mme-service db record all

The following new field is added to the show output to display the configured GUTI Reallocation parameters:

- REALLOCATED GUTI

show mme-service db record imsi

The following new fields are added to the show output to display the configured GUTI Reallocation parameters:

- REALLOCATED GUTI
- PLMN
- MME Group ID
- MME Code
- M-TMSI
- GUTI Allocated time

Below is an example displaying the statistics listed above:

```
 show mme-service db record imsi 123456710100158
Friday September 18 09:25:19 EDT 2015
DB RECORD
=========
Sessmgr Instance                                                    : 1
Imsimgr Instance                                                   : 1
MME Service                                                            :
mmesvc
Lookup Keys
-----------
IMSI                          : 123456710100158
Service-id                    : 7
 GUTI
   PLMN                                                          : 123456
   MME Group ID                                                 : 32777
   MME Code                                                        : 2
   M-TMSI                                                       : 3221491713
REALLOCATED GUTI
   PLMN                                                          : 123456
   MME Group ID                                                 : 32777
   MME Code                                                        : 2
   M-TMSI                                                           :
3221491713
Call-ID                                                           : 00004e62
GUTI Allocated time                                  : Fri Sep 18 08:29:16
2015
```

GUTI Re-allocation Bulk Statistics

The following bulk statistics are included in the MME Schema in support of this feature:

The following bulk statistics are included in the MME Schema in support of this feature:

- emm-msgtx-guti-reallocation
- emm-msgtx-guti-reallocation-retx
- emm-msgtx-guti-realloc-attach-accept
- emm-msgtx-guti-realloc-attach-accept-retx
- emm-msgtx-guti-realloc-tau-accept
- emm-msgtx-guti-realloc-tau-accept-retx
- guti-reallocation-attempted
- guti-reallocation-success
- guti-reallocation-failure

For descriptions of these variables, see "MME Schema Statistics" in the *Statistics and Counters Reference*.

CHAPTER 24

Heuristic and Intelligent Paging

This chapter describes the advanced paging features of the MME.

Feature Description

A valid license key is required to enable heuristic and intelligent paging. Contact your Cisco Account or Support representative for information on how to obtain a license.

The MME supports two levels of paging optimization to minimize the paging load in the E-UTRAN access network:

- **Heuristic Paging**

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

- **Intelligent Paging**

  Intelligent Paging further optimizes heuristic paging to allow operators to specify different paging profiles for different streams of traffic (CS or PS traffic types). Each paging profile provides the flexibility to control the pace, volume and type of paging requests sent to eNBs.

How It Works

Heuristic Paging

Each MME maintains a list of "n" last heard from eNodeBs 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.

Using Heuristic Paging, the MME attempts to page the user in stages as described in the "Heuristic Paging Behavior" section that follows.

Default (Non-Heuristic) Paging Behavior

If no license is in place, or if the heuristic paging is not turned on, the MME by default pages all eNodeBs in all TAIs present in the TAI list assigned to the UE.

The number of paging retries attempted for Packet Switch (PS) calls is dictated by the **max-paging-attempts** command under the mme-service configuration. If no configuration exists then by default 3 retries are attempted.

The timeout duration for each retry is dictated by the **t3413-timeout** command under mme-service configuration. If no configuration exists, the default value of 6 seconds is used.

For Circuit Switch (CS) calls, the MME sends only one paging attempt, regardless of the configuration of the **max-paging-attempts** command.

Heuristics Paging Behavior

If heuristics paging is turned on for the mme-service the following heuristics paging behavior can be observed for Circuit Switched (CS) and Packet Switched (PS) events, the Default Heuristics Paging refers to Heuristics paging without an associated paging map:

The default Heuristics paging behavior for CS events like SGS PAGING (Voice ,SMS), MM INFO and so on is listed below:

- Page all eNodeBs in all TAIs present in the TAI list assigned to the UE.

The default Heuristics paging behavior for PS events like DDN, Create Bearer Request, Delete Bearer request ,Update Bearer Request and so on is listed below:

1. Page the last eNodeB from which the UE contacted the MME in the last TAI from which the UE contacted the MME.
2. Page all eNodeBs in the last TAI from which the UE contacted the MME.
3. Page all eNodeBs in all TAIs present in the TAI list assigned to the UE.

When heuristic paging is enabled, the MME tracks the last TAI from which the UE contacted the MME and the last eNodeB from which the UE contacted the MME.

Paging to the last eNodeB (1) and the TAI from which UE was last heard (2) is done only once. **max-paging-attempts** configured in the mme-service is used only to control the number paging attempts to all eNodeBs in all TAIs (3).

Important For paging requests for circuit switch (CS) calls, the MME does not follow this staged paging behavior. Instead, it follows the standards-defined paging mechanism of paging all eNodeBs in all TAIs present in the TAI list assigned to the UE (all-enb-all-tai). Only one attempt is made with no retries.

Intelligent Paging

With Intelligent Paging, the MME can be configured with paging profiles which define different stages of paging (paging maps). These controls determine whether the MME sends a paging-request to either the last TAI or all TAIs. In addition, these controls determine whether the MME sends the paging request to just one eNodeB, a specific number of eNodeBs, or to all eNBs. This enables the MME to control the span and reach of each paging request.

Two modules, configurable under the LTE Policy configuration mode, are introduced to support intelligent paging:

- **Paging-profile** -- This module allows operator to configure different stages of paging in the order of desired execution with parameters that control the pace, volume and behavior of a given paging stage.
- **Paging-map** -- This module allows operator to apply different 'paging-profiles' to different traffic types. When MME service is associated with an instance of this module, MME checks this map object to figure the type of paging-profile to adopt for a given paging trigger.

Important If the MME is associated with a paging-map object that either does not exist or does not have an entry matching the paging-trigger, the MME performs paging as described in *Default Heuristics Paging Behavior*.

Configuring MME Paging Features

Important Use of these Paging features require that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

Configuring Heuristic Paging

The example configuration in this section allows the MME to perform heuristic (optimized), idle-mode paging, reducing the number of messages carried over the E-UTRAN access network.

The following configuration example enables heuristic (optimized) paging on the MME:

```
configure
    context <mme_context_name>
        mme-service <mme_svc_name>
            heuristic-paging
            end
```

Configuring Intelligent Paging

The following sections provide configuration examples to enable intelligent paging on the MME:

Step 1 Create and configure a **paging-profile**.

Step 2 Create and configure a **paging-map**.

Step 3 Enable heuristic paging and assign a paging-map to a specific mme-service.

Creating and Configuring the Paging-Profile

A paging-profile enables operators to configure different stages of paging in the order of desired execution with parameters that control the pace, volume and behavior of a given paging stage.

The following configuration example creates two paging-profiles in the lte-policy configuration mode:

```
configure
    lte-policy
        paging-profile <paging_profile_name1 > -noconfirm
            paging-stage 1 match-criteria all action all-enb-all-tai t3413-timeout 5 max-paging-attempts
 4
            exit
        paging-profile <paging_profile_name2 > -noconfirm
            paging-stage 1 match-criteria all action last-n-enb-last-tai max-n-enb 1 t3413-timeout 5
max-paging-attempts 1
           paging-stage 2 match-criteria all action all-enb-last-tai t3413-timeout 5 max-paging-attempts
 1
            end
```

Creating and Configuring the Paging-Map

A paging-map enables operators to apply different paging-profiles to different traffic types. When an MME service is associated with an instance of this module, the MME checks this map object to figure the type of paging-profile to adopt for a given paging trigger.

The following configuration example creates a paging-profile in the LTE Policy configuration mode:

```
configure
    lte-policy
        paging-map <paging_map_name > -noconfirm
            precedence 1 traffic-type { cs | ps } paging-profile paging_profile_name1
            end
```

Beginning in Release 16.0, the paging-map configuration includes additional configuration options for selecting a paging-profile in order to control the pace, volume and behavior of a given paging state. Within a paging map, precedence can be defined for paging requests based on the following traffic types:

- CS traffic (circuit-switched traffic for Mobile Terminated CSFB) types can be defined according to specific subtypes of **voice**, **sms**, and **other**.

- PS traffic (packet-switched traffic for all data and control messaging that involve packet services as well as IMS Voice) types can be defined according to the QoS **QCI value** from the EPS Bearer ID (EBI) in the Downlink Data Notification (DDN) received on S11 from the S-GW. The ARP priority based paging can be defined for PS traffic.
- **Signaling** (UE-level signaling requests) traffic types can also be defined. This option can be further qualified with the **Detach** and **LCS** (Location Services) traffic subtype options.

These options are shown in the following **precendence** command syntax:

precedence *precedence* **traffic-type { cs [voice | sms | other] | ps [qci** *qci_value* **] | signaling [detach | lcs] } paging-profile** *paging_profile_name*
From release 20.0 onwards the **precedence** command has been enhanced as follows:

precedence *priority* **traffic-type { cs [voice | sms | other] | ps [arp** *arp_value* **| qci** *qci_value* **] | signaling [detach | idr | lcs | node-restoration] } paging-profile** *paging_profile_name*
Refer to the *LTE Paging Map Configuration Commands* chapter of the *Command Line Interface Reference* for more information about this command.

Enable Heuristic Paging with Paging-Map (Intelligent Paging)

The following example enables heuristic-paging and associates a paging-map to the specified MME service.

```
configure
   context <mme_context_name> -noconfirm
      mme-service <mme_svc_name> -noconfirm
         heuristic-paging paging-map paging_map_name
         end
```

Verifying the Paging Configuration

The following command displays the entire paging configuration for the MME service.

show mme-service all
The output of the above command will be similar to the following:

```
[local]asr5x00 show mme-service name mmesvc1
Heuristic Paging        : Enabled
Heuristic Paging Map    : pgmap1
```

Monitoring and Troubleshooting the MME Paging Features

For more information regarding bulk statistics and output fields and counters in this section, refer to the *Statistics and Counters Reference*.

Paging Bulk Statistics

The following bulk statistics are included in the MME Schema to track paging events:

- ps-qci-1-paging-init-events-attempted
- ps-qci-1-paging-init-events-success

- ps-qci-1-paging-init-events-failures
- ps-qci-1-paging-last-enb-success
- ps-qci-1-paging-last-tai-success
- ps-qci-1-paging-tai-list-success
- ps-qci-2-paging-init-events-attempted
- ps-qci-2-paging-init-events-success
- ps-qci-2-paging-init-events-failures
- ps-qci-2-paging-last-enb-success
- ps-qci-2-paging-last-tai-success
- ps-qci-2-paging-tai-list-success
- ps-qci-3-paging-init-events-attempted
- ps-qci-3-paging-init-events-success
- ps-qci-3-paging-init-events-failures
- ps-qci-3-paging-last-enb-success
- ps-qci-3-paging-last-tai-success
- ps-qci-3-paging-tai-list-success
- ps-qci-4-paging-init-events-attempted
- ps-qci-4-paging-init-events-success
- ps-qci-4-paging-init-events-failures
- ps-qci-4-paging-last-enb-success
- ps-qci-4-paging-last-tai-success
- ps-qci-4-paging-tai-list-success
- ps-qci-5-paging-init-events-attempted
- ps-qci-5-paging-init-events-success
- ps-qci-5-paging-init-events-failures
- ps-qci-5-paging-last-enb-success
- ps-qci-5-paging-last-tai-success
- ps-qci-5-paging-tai-list-success
- ps-qci-6-paging-init-events-attempted
- ps-qci-6-paging-init-events-success
- ps-qci-6-paging-init-events-failures
- ps-qci-6-paging-last-enb-success
- ps-qci-6-paging-last-tai-success

- ps-qci-6-paging-tai-list-success
- ps-qci-7-paging-init-events-attempted
- ps-qci-7-paging-init-events-success
- ps-qci-7-paging-init-events-failures
- ps-qci-7-paging-last-enb-success
- ps-qci-7-paging-last-tai-success
- ps-qci-7-paging-tai-list-success
- ps-qci-8-paging-init-events-attempted
- ps-qci-8-paging-init-events-success
- ps-qci-8-paging-init-events-failures
- ps-qci-8-paging-last-enb-success
- ps-qci-8-paging-last-tai-success
- ps-qci-8-paging-tai-list-success
- ps-qci-9-paging-init-events-attempted
- ps-qci-9-paging-init-events-success
- ps-qci-9-paging-init-events-failures
- ps-qci-9-paging-last-enb-success
- ps-qci-9-paging-last-tai-success
- ps-qci-9-paging-tai-list-success
- cs-voice-paging-init-events-attempted
- cs-voice-paging-init-events-success
- cs-voice-paging-init-events-failures
- cs-voice-paging-last-enb-success
- cs-voice-paging-last-tai-success
- cs-voice-paging-tai-list-success
- cs-sms-paging-init-events-attempted
- cs-sms-paging-init-events-success
- cs-sms-paging-init-events-failures
- cs-sms-paging-last-enb-success
- cs-sms-paging-last-tai-success
- cs-sms-paging-tai-list-success
- cs-other-paging-init-events-attempted
- cs-other-paging-init-events-success

- cs-other-paging-init-events-failures
- cs-other-paging-last-enb-success
- cs-other-paging-last-tai-success
- cs-other-paging-tai-list-success
- signaling-detach-paging-init-events-attempted
- signaling_detach-paging-init-events-success
- signaling-detach-paging-init-events-failures
- signaling-detach-paging-last-enb-success
- signaling-detach-paging-last-tai-success
- signaling-detach-paging-tai-list-success
- signaling-lcs-paging-init-events-attempted
- signaling_lcs-paging-init-events-success
- signaling-lcs-paging-init-events-failures
- signaling-lcs-paging-last-enb-success
- signaling-lcs-paging-last-tai-success
- signaling-lcs-paging-tai-list-success

Release 15.0: The following bulk statistics are included in the MME Schema to track paging events. Note that these bulk statistics have been replaced by the bulk statistics above.

- ps-paging-init-events-attempted
- ps-paging-init-events-success
- ps-paging-init-events-failures
- ps-paging-last-enb-success
- ps-paging-last-tai-success
- ps-paging-tai-list-success

Release 20.0

The following bulk statistics are included in the MME schema in for eMPS support :

- s1ap-transdata-pagingpriocs
- s1ap-transdata- pagingpriops
- csfb-ue-prio-voice-total
- csfb-ue-prio-voice-success
- csfb-ue-prio-voice-failures
- csfb-nw-prio-voice-total
- csfb-nw-prio-voice-success

- csfb-nw-prio-voice-failures
- ps-arp-1-paging-init-events-attempted
- ps-arp-1-paging-init-events-success
- ps-arp-1-paging-init-events-failures
- ps-arp-1-paging-last-enb-success
- ps-arp-1-paging-last-tai-success
- ps-arp-1-paging-tai-list-success
- ps-arp-2-paging-init-events-attempted
- ps-arp-2-paging-init-events-success
- ps-arp-2-paging-init-events-failures
- ps-arp-2-paging-last-enb-success
- ps-arp-2-paging-last-tai-success
- ps-arp-2-paging-tai-list-success
- ps-arp-3-paging-init-events-attempted
- ps-arp-3-paging-init-events-success
- ps-arp-3-paging-init-events-failures
- ps-arp-3-paging-last-enb-success
- ps-arp-3-paging-last-tai-success
- ps-arp-3-paging-tai-list-success
- ps-arp-4-paging-init-events-attempted
- ps-arp-4-paging-init-events-success
- ps-arp-4-paging-init-events-failures
- ps-arp-4-paging-last-enb-success
- ps-arp-4-paging-last-tai-success
- ps-arp-4-paging-tai-list-success
- ps-arp-5-paging-init-events-attempted
- ps-arp-5-paging-init-events-success
- ps-arp-5-paging-init-events-failures
- ps-arp-5-paging-last-enb-success
- ps-arp-5-paging-last-tai-success
- ps-arp-5-paging-tai-list-success
- ps-arp-6-paging-init-events-attempted
- ps-arp-6-paging-init-events-success

- ps-arp-6-paging-init-events-failures
- ps-arp-6-paging-last-enb-success
- ps-arp-6-paging-last-tai-success
- ps-arp-6-paging-tai-list-success
- ps-arp-7-paging-init-events-attempted
- ps-arp-7-paging-init-events-success
- ps-arp-7-paging-init-events-failures
- ps-arp-7-paging-last-enb-success
- ps-arp-7-paging-last-tai-success
- ps-arp-7-paging-tai-list-success
- ps-arp-8-paging-init-events-attempted
- ps-arp-8-paging-init-events-success
- ps-arp-8-paging-init-events-failures
- ps-arp-8-paging-last-enb-success
- ps-arp-8-paging-last-tai-success
- ps-arp-8-paging-tai-list-success
- ps-arp-9-paging-init-events-attempted
- ps-arp-9-paging-init-events-success
- ps-arp-9-paging-init-events-failures
- ps-arp-9-paging-last-enb-success
- ps-arp-9-paging-last-tai-success
- ps-arp-9-paging-tai-list-success
- ps-arp-10-paging-init-events-attempted
- ps-arp-10-paging-init-events-success
- ps-arp-10-paging-init-events-failures
- ps-arp-10-paging-last-enb-success
- ps-arp-10-paging-last-tai-success
- ps-arp-10-paging-tai-list-success
- ps-arp-11-paging-init-events-attempted
- ps-arp-11-paging-init-events-success
- ps-arp-11-paging-init-events-failures
- ps-arp-11-paging-last-enb-success
- ps-arp-11-paging-last-tai-success

- ps-arp-11-paging-tai-list-success
- ps-arp-12-paging-init-events-attempted
- ps-arp-12-paging-init-events-success
- ps-arp-12-paging-init-events-failures
- ps-arp-12-paging-last-enb-success
- ps-arp-12-paging-last-tai-success
- ps-arp-12-paging-tai-list-success
- ps-arp-13-paging-init-events-attempted
- ps-arp-13-paging-init-events-success
- ps-arp-13-paging-init-events-failures
- ps-arp-13-paging-last-enb-success
- ps-arp-13-paging-last-tai-success
- ps-arp-13-paging-tai-list-success
- ps-arp-14-paging-init-events-attempted
- ps-arp-14-paging-init-events-success
- ps-arp-14-paging-init-events-failures
- ps-arp-14-paging-last-enb-success
- ps-arp-14-paging-last-tai-success
- ps-arp-14-paging-tai-list-success
- ps-arp-15-paging-init-events-attempted
- ps-arp-15-paging-init-events-success
- ps-arp-15-paging-init-events-failures
- ps-arp-15-paging-last-enb-success
- ps-arp-15-paging-last-tai-success
- ps-arp-15-paging-tai-list-success

Paging Show Command(s) and/or Outputs

This section provides information regarding show commands and/or their outputs in support of the MME Paging features.

Only those counters which relate to paging are shown.

The following command displays a list of all paging-profiles in ordered by the paging-stage.

show lte-policy paging-profile summary
The following command shows information for the specified paging-profile.

show lte-policy paging-profile name <*name* >

```
[local]asr5x00 show lte-policy paging-profile name pg-aggressive
```

```
      Paging Profile : pg-aggressive
            Paging Stage 1 :
                  Paging Action      - Page all TAIs in all ENBs.
                  Match Criteria     - No conditions. Always apply this stage.
                  T3414-Timeout      - 5 sec
                  Max Paging Retries - 4
```

The following command shows a list of all paging-maps configured.

show lte-policy paging-map summary

The following command shows information for the specified paging-map.

show lte-policy paging-map name < *name* **>**

```
      [local]asr5x00 show lte-policy paging-map name pg-map2
      Paging Map : pg-map2
            Precedence 1 : Circuit-Switched (CS); Paging is performed as per paging-profile
 pg2
             Precedence 2 : Packet-Switched (PS); Paging is performed as per paging-profile
 pg4
```

The following command shows the UE Tracking Information for the Last Reported 5 eNodeBs and Last Reported 7 ECGIs for the specified IMSI.

show mme-service db record imsi < *imsi* **>**

The following command shows information about the Paging Initiation Events.

show mme-service statistics

The following groups of PS paging initiation event counters track individual events for each QCI level (1-7). The following sample shows only the fields for QCI-1. Additional groups of fields are provided for QCI-2 through QCI-7.

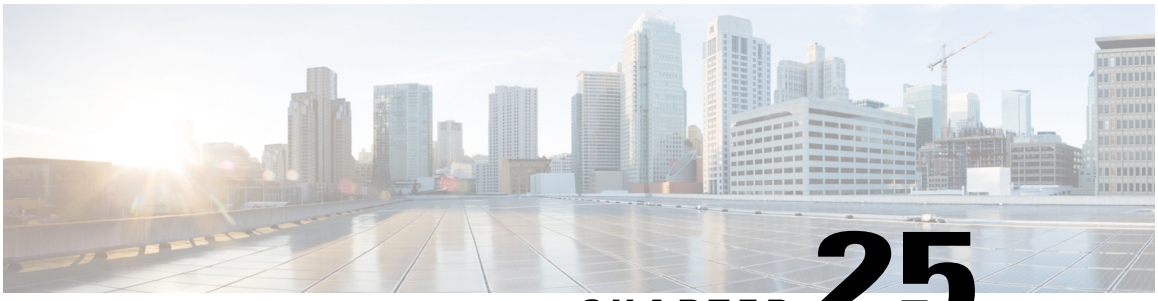
```
Paging Initiation for PS QCI-1 Events:
    Attempted: 0   Success: 0
    Failures: 0
    Success at Last n eNB: 0   Success at Last TAI: 0
    Success at TAI List:  0
```

The following groups of CS traffic paging event counters events based on sub-traffic type: (CS **Voice** Events, CS **SMS** Events, and CS **Other** Events) .

```
Paging Initiation for CS Voice Events:
    Attempted: 0   Success: 0
    Failures: 0
    Success at Last n eNB: 0  Success at Last TAI: 0
    Success at TAI List: 0
Paging Initiation for CS SMS Events:
    Attempted: 0  Success: 0
    Failures: 0
    Success at Last n eNB: 0  Success at Last TAI: 0
    Success at TAI List: 0
Paging Initiation for CS Other Events:
    Attempted: 0  Success: 0
    Failures: 0
    Success at Last n eNB: 0  Success at Last TAI: 0
    Success at TAI List: 0
```

The following groups of Signaling event counters track individual Detach and LCS (Location Services) paging events.

```
Paging Initiation for SIGNALING DETACH Events:
    Attempted: 0  Success: 0
    Failures: 0
    Success at Last n eNB: 0  Success at Last TAI: 0
    Success at TAI List: 0
Paging Initiation for SIGNALING LCS Events:
    Attempted:  0  Success: 0
    Failures:  0
    Success at Last n eNB: 0  Success at Last TAI: 0
    Success at TAI List: 0
```



CHAPTER 25

HSS-based P-CSCF Restoration

The home subscriber server-based (HSS) Proxy Call Session Control Function (P-CSCF) Restoration is an optional mechanism during a P-CSCF failure. It applies only when the UE is using 3GPP access technologies.

This section describes MME support for HSS-Initiated P-CSCF Restoration.

Feature Description

P-CSCF 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

The HSS-based P-CSCF Restoration feature is license controlled. Contact your Cisco Account or Support representative for information on how to obtain a license.

How It Works

The HSS-based P-CSCF restoration feature consists of restoring P-CSCF for the corresponding UE IMS PDN connections in one of the following ways:

- **Basic mechanism** -- This makes usage of a path through HSS and MME to request the release of the IMS PDN connection to the corresponding UE.
- **Optional extension** -- This avoids the IMS PDN deactivation and re-activation. The HSS-based P-CSCF basic mechanism is optionally extended by reusing part of the "Update bearer at P-CSCF failure" mechanism. This extension is based on the possibility for the P-GW to know whether or not the UE supports the "P-CSCF address assignment through PCO." mechanism.

Architecture

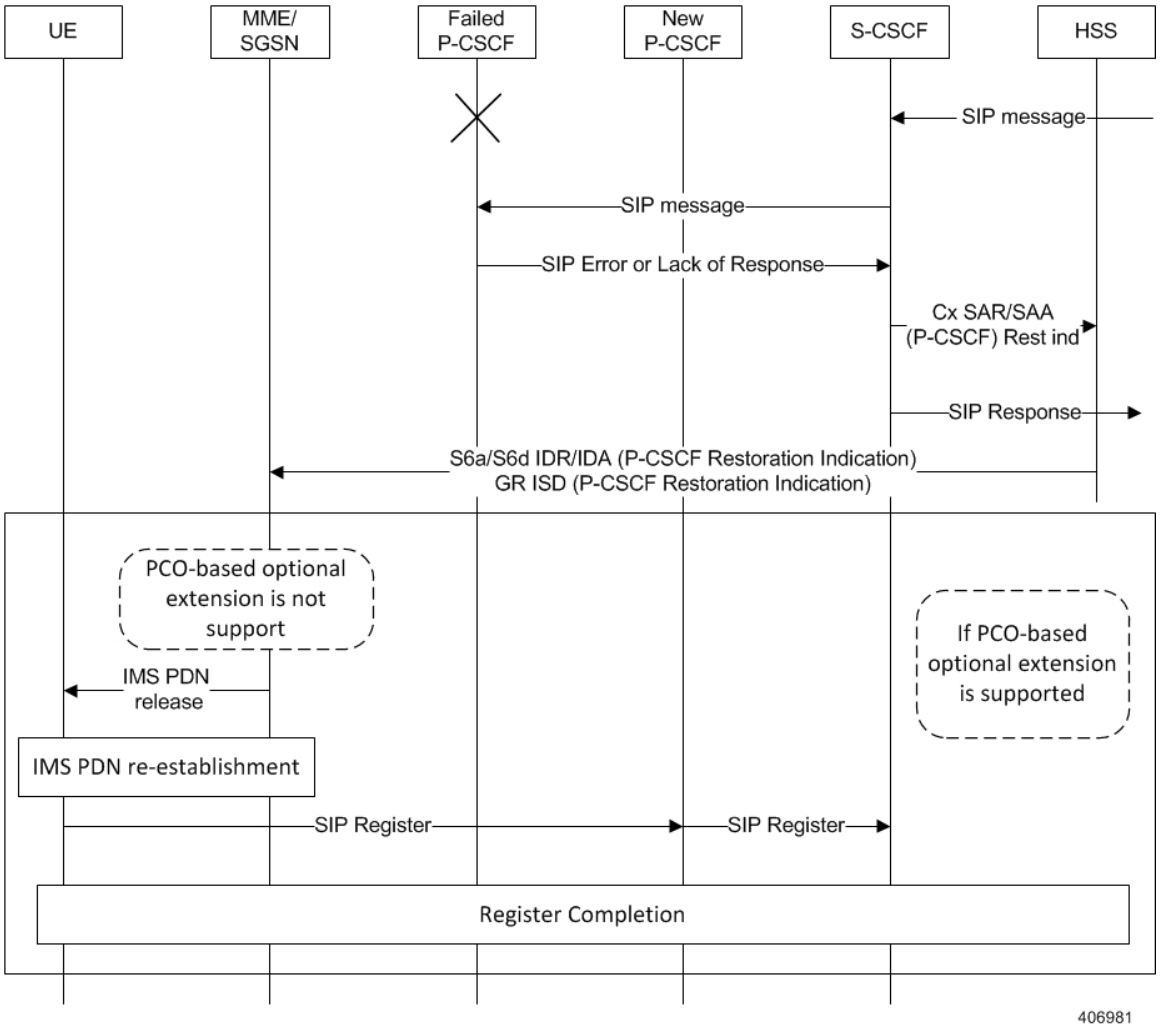
MME provides the following support for HSS-based P-CSCF restoration:

- Advertise support for P-CSCF Restoration on S6a interface towards HSS when configured.
- P-CSCF restoration for IMS PDN's upon receiving s6a IDR message with P-CSCF restoration in IDR flags.
- Identifying IMS PDN based on APN type specified.
- Configuration to select P-CSCF restoration type - PDN Deactivation or PDN Modification.
- Performs PDN Disconnect for IMS PDN deactivation with cause code "reactivation requested" if P-CSCF Restoration type is set to PDN Deactivation.
- "Modify bearer request on S11 interface towards SGW with PCRI indication if P-CSCF Restoration type is set to PDN Modification.
- Detaches UE with cause "reattach required" in case all the UE PDN's need to be deactivated as part of P-CSCF restoration.
- Pages the UE if IDR with P-CSCF restoration is received, while UE is in idle mode.
- Implicitly detach or disconnect the IMS PDN if Paging UE fails and the P-CSCF restoration type is set to PDN deactivation.
- Generate statistics for the number of IMS PDN's Deactivated & Modified for P-CSCF restoration.

Flows

This section provides the MME's call flows for HSS-based P-CSCF Restoration.

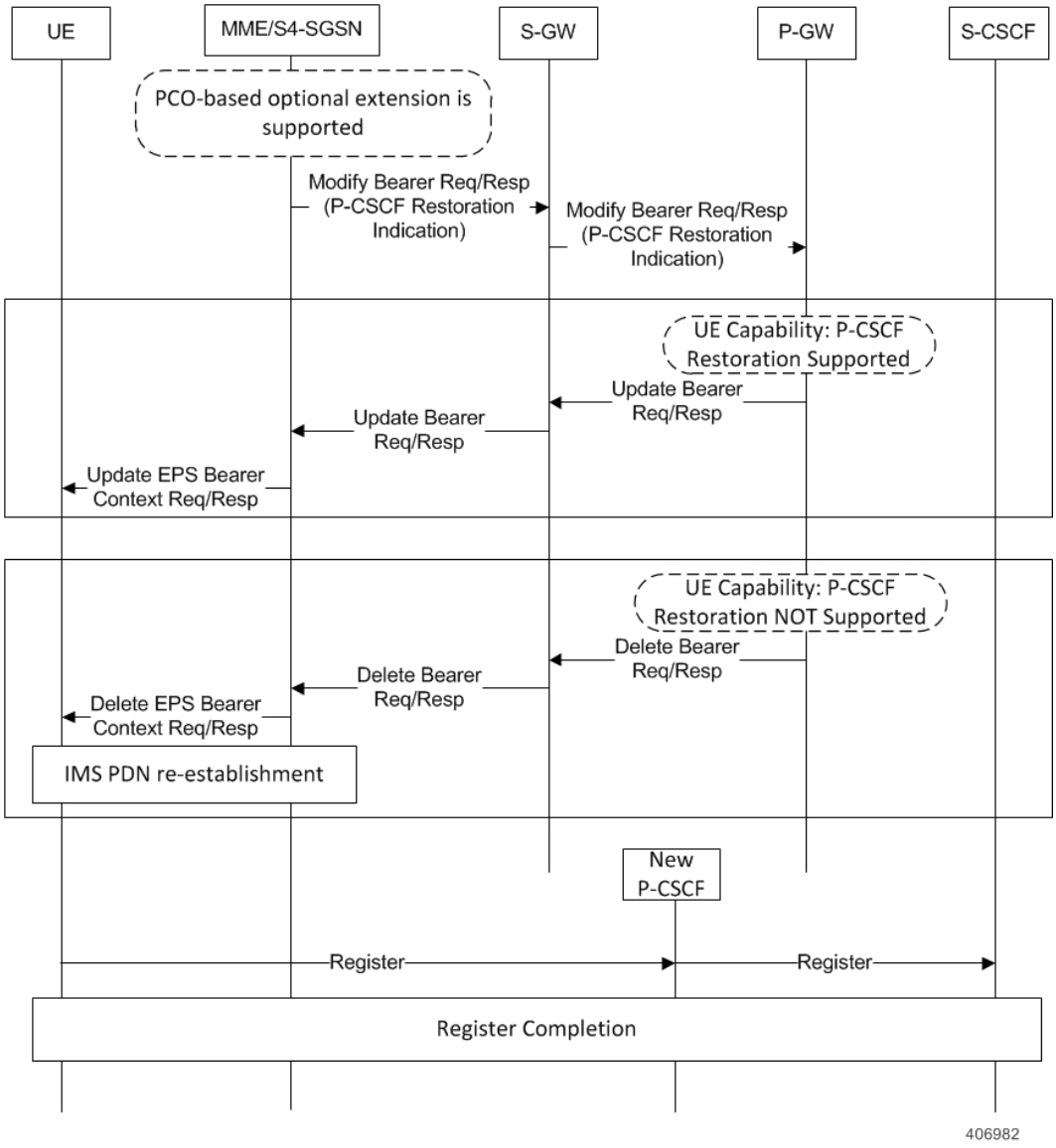
Figure 15: Call flow for HSS-based P-CSCF Restoration



On receiving the P-CSCF Restoration indication from the HSS, the MME/SGSN from the received IMSI identifies the UE and finds the corresponding IMS APN. The support of this feature by the serving SGW/PGW is determined based on the local configuration at the MME. If the optional extension is not supported by the SGW/PGW, the MME releases the identified PDN connection towards the UE by executing PDN disconnection/detach procedure with NAS cause code "reactivation requested/ reattach required". Additionally, the MME/SGSN release the same PDN connection towards the SGW/PGW by sending Delete Session message.

As a result of the release of the IMS PDN connection, the UE activates the IMS PDN connection to select an available P-CSCF and to perform a new initial IMS registration.

Figure 16: Call flow for HSS-based P-CSCF Restoration, continued...



The HSS-based P-CSCF basic mechanism is optionally extended by reusing part of the "Update PDP context/bearer at P-CSCF failure" mechanism. This in order to avoid the need to deactivate and reactivate the IMS PDN connection. PCO-based optional extension is based on the possibility for the P-GW/GGSN to know whether or not the UE supports the "Update PDP context/bearer at P-CSCF failure" mechanism.

The MME sends Modify Bearer to the P-GW for the associated PDN connection with a P-CSCF Restoration indication. The MME provides this indication to the P-GW through the S-GW. When Modify Bearer Request is received by the S-GW with the P-CSCF Restoration indication, this message is forwarded to PGW. PGW sends Update Bearer Request to the MME along with a list of available P-CSCF addresses within PCO IE to update the destination UE.

MME sends an Update EPS Bearer Context Request or Modify PDP Context Request to the UE, including the PCO with the list of available P-CSCF addresses otherwise, upon reception of Delete Bearer Request the MME sends Delete EPS Bearer Context Request to the UE with NAS cause code "reactivation requested". When the PDN connection is released, the UE re-activates the IMS PDN connection and selects an available P-CSCF. If the UE has received Modify EPS Bearer Context Request, the UE as per PCO based P-CSCF Restoration procedures, selects an available P-CSCF from the list for IMS registration. The UE performs a new initial IMS registration.

Configuring HSS-based P-CSCF Restoration

Configuring P-CSCF Restoration and Restoration Method

Setting Up P-CSCF Restoration

The **pcscf-restoration** is a newly added command to enable HSS-based P-CSCF Restoration.

The following CLI configuration enables/disables support for HSS-initiated P-CSCF restoration in the Call Control Profile configuration mode.

configure
call-control-profile *profile_name*
[remove] pcscf-restoration
end

Notes:

- The **pcscf-restoration** command in the above configuration enables HSS-based P-CSCF restoration. When enabled, MME supports P-CSCF Restoration on the S6a interface towards HSS for IMS PDN.
- The **remove** prefix added to the command disables HSS-based P-CSCF Restoration in the MME.
- By default, the above configuration is disabled.
- To select the method for P-CSCF Restoration, use the **pcscf-restoration** keyword in **apn-type ims** command under APN Profile configuration mode.

Setting Restoration Method

The **apn-type ims** command identifies APN as IMS APN, and indicate whether the PGW supports optional extension or MME initiates PDN deactivation for HSS initiated P-CSCF restoration.

The **pcscf-restoration { pco-update | pdn-deactivate }** keywords select the method for P-CSCF restoration. The P-CSCF restoration method is configured under the APN Profile configuration mode.

configure
apn-profile *profile_name*
apn-type ims [pcscf-restoration { pco-update | pdn-deactivate }]
end

Notes:

- The **apn-type ims** command for MME identifies the type of APN. If an IMS APN is present, the Modify Bearer Request will be delayed during Inbound SRNS relocation.

- The **pcscf-restoration** keyword identifies P-CSCF restoration for IMS PDN. This keyword is functional only if the feature license is installed.
- The **pco-update** keyword selects P-CSCF restoration method as PDN Modification through PCO update.
- The **pdn-deactivate** keyword selects P-CSCF restoration method as PDN Deactivation.
- To enable HSS-based P-CSCF Restoration, use the **pcscf-restoration** command under the Call Control Profile mode.

Important If only "apn-type ims" is configured then default P-CSCF restoration method "pdn-deactivate" is enabled.

Verifying the HSS-based P-CSCF Restoration Configuration

Verify the configuration of HSS-based P-CSCF Restoration by entering the following commands:

```
show call-control-profile full all
```

The command above outputs a display similar to the following:

```
Call Control Profile Name  =  cp1
SAMOG Web-Authorization Mutiple Device Support  :  NO
Super Charger  :  Disabled
P-CSCF Restoration  :  Enabled
Sending Radio Access Technology (RAT) IE  :  Enabled
```

The P-CSCF Restoration field indicates if P-CSCF Restoration is enabled or disabled.

show apn-profile full all

The command above generates a display similar to the following:

```
APN Profile Name :  ap1
CI-QOS mapping table  :  Not Configured
APN Type  :  IMS
PCSCF Restoration Type  :  PCO Update
Dedicated bearers
GBR  :  Not Configured
Non-GBR  :  Not Configured
```

The P-CSCF Restoration Type parameter is displayed if the APN type is set to IMS. This parameter indicates if the P-CSCF Restoration method is PCO Update or PDN Deactivate for the current APN profile.

Monitoring and Troubleshooting the HSS-based P-CSCF Restoration

The following sections describe commands available to monitor HSS-based P-CSCF Restoration on the MME.

HSS-based P-CSCF Restoration Show Command(s) and/or Outputs

This section provides information regarding show commands and their outputs in support of HSS-based P-CSCF Restoration

show mme-service statistics

The following fields are displayed on executing this command for this feature:

```
Bearer Statistics:
All Bearers:  0      Connected Bearers: 0
Idle Bearers:  0
HSS P-CSCF Restoration:
PDN Deactivation: 0   PDN Modification:  3
```

The PDN Deactivation counter indicates the number of IMS PDN deactivations attempted due to HSS-based P-CSCF Restoration

Troubleshooting HSS-based P-CSCF Restoration

To troubleshoot the HSS-based P-CSCF Restoration feature, use the following instructions:

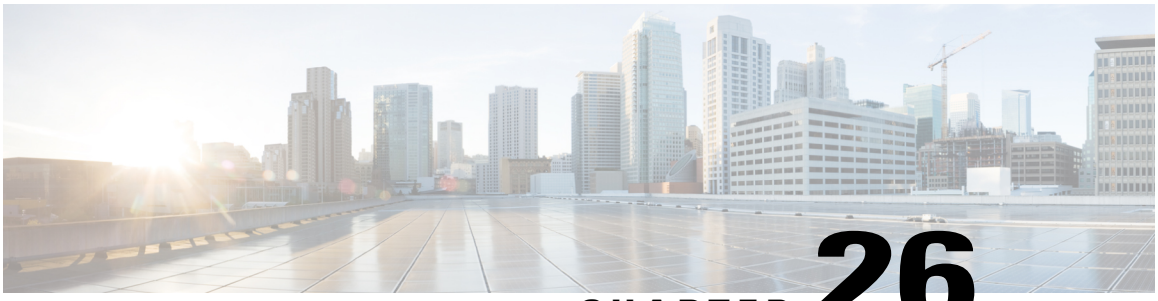
- Ensure call control profile has PCSCF restoration configured.
- Ensure APN profile has APN type configuration and APN profile is associated for the concerned APN NI.
- Check if HSS supports PCSCF restoration and also if it has advertised its support in the S6a messages.
- Ensure if all PGWs serving the APN supports PCSCF restoration through PCO update. If yes then PCSCF restoration method PDN Modification (PCO-update) should be configured. Otherwise PCSCF restoration method PDN deactivate should be configured by default.
- Check the statistics using the following show commands:
  - **show mme-service statistics esm-only**: Displays the counters illustrated below:
    ```
    HSS P-CSCF Restoration:
    PDN Deactivation:  0   PDN Modification: 3
    ```
  - **show session disconnect-reasons verbose**: Displays the counter illustrated below:
    ```
    mme-pcscf-rest-detach(616)  0           0.00000
    ```
  - **show mme-service statistics**: Displays the counters illustrated below:
    ```
    Paging Initiation for SIGNALING DETACH Events:
    Attempted:  0    Success: 0
    Failures:  0
    Success at Last n eNB: 0   Success at Last TAI: 0
    Success at TAI List:              0

    Paging Initiation for SIGNALING Idr Events:
    Attempted: 0    Success: 0
    Failures: 0
    Success at Last n eNB 0    Success at Last TAI: 0
    Success at TAI List: 0
    HSS Initiated PDN Disconnections:
    Attempted: 2    Success: 2
    Failures: 0
    Disconnect Statistics:
    UE detached:  0    PGW detached: 0
    HSS detached: 1    MME detached: 0
    Implicit detach: 0    Local abort:  0
    Authentication failure: 0  Sub parameter failure: 0
    Foreign PLMN rejected: 0    APN not sup PLMN-RAT:  0
    Other reasons: 0
    ```

HSS-based P-CSCF Restoration Bulk Statistics

The following statistics are included in the MME Schema in support of the HSS-based P-CSCF Restoration:

- pcscf-restoration-pdn-deactivations
- pcscf-restoration-pdn-modifications

For descriptions of these variables, see *MME Schema Statistics* in the *Statistics and Counters Reference*.



CHAPTER 26

Idle-mode Signaling Reduction

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.

Feature Description

Idle mode Signaling Reduction (ISR) allows the UE to be registered in UTRAN/GERAN at the same time it is registered in E-UTRAN. ISR requires functionality in both the UE and the network (i.e. in the SGSN, MME, S-GW and HSS) to activate ISR for a UE. The network can decide for ISR activation individually for each UE.

ISR allows the UE to roam between LTE & 2G/3G while reducing the frequency of TAU and RAU procedures caused by UEs reselecting between E-UTRAN and GERAN/UTRAN, when operated together. It not only reduces the signaling between UE and network, but also reduces the signaling between E-UTRAN & UTRAN/GERAN.

When ISR is activated, the UE is registered with both the MME and S4 SGSN. Both the S4 SGSN and the MME have a control connection with the S-GW. The MME and S4 SGSN are both registered at the HSS. The UE stores MM parameters from S4 SGSN (e.g. P-TMSI and RA) and from MME (e.g. GUTI and TA(s)) and the UE stores session management (bearer) contexts that are common for E-UTRAN and GERAN/UTRAN accesses. In an idle state the UE can reselect between E-UTRAN and GERAN/UTRAN (within the registered RA and TAs) without any need to perform TAU or RAU procedures with the network. SGSN and MME store each other's address when ISR is activated.

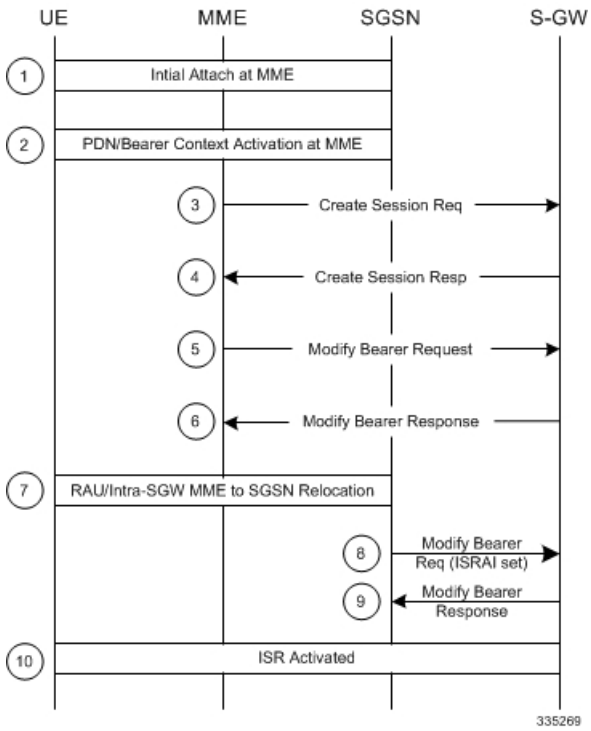
How it Works

ISR Activation

ISR does not entail any changes to the initial attach procedure at the MME or S4 SGSN. ISR is only activated when the UE is registered with both the MME and S4 SGSN. This happens for the first time when the UE has a previous state at either the MME or S4 SGSN and relocates to the other node. This is achieved via TAU/RAU procedures or via inter-RAT procedures. Both the S4 SGSN and the MME then have a control connection with the Serving GW. The MME and S4 SGSN are both registered at the HSS.

The UE stores Mobility Management (MM) parameters from the SGSN (P-TMSI and RA) and from MME (GUTI and TA(s)) and the UE stores session management (bearer) contexts that are common for E-UTRAN and GERAN/UTRAN accesses. In the idle state, the UE can reselect between E-UTRAN and GERAN/UTRAN (within the registered RA and TAs) without any need to perform TAU or RAU procedures with the network. The SGSN and MME store each other's address when ISR is activated.

Figure 17: ISR Activation During MME to SGSN Relocation

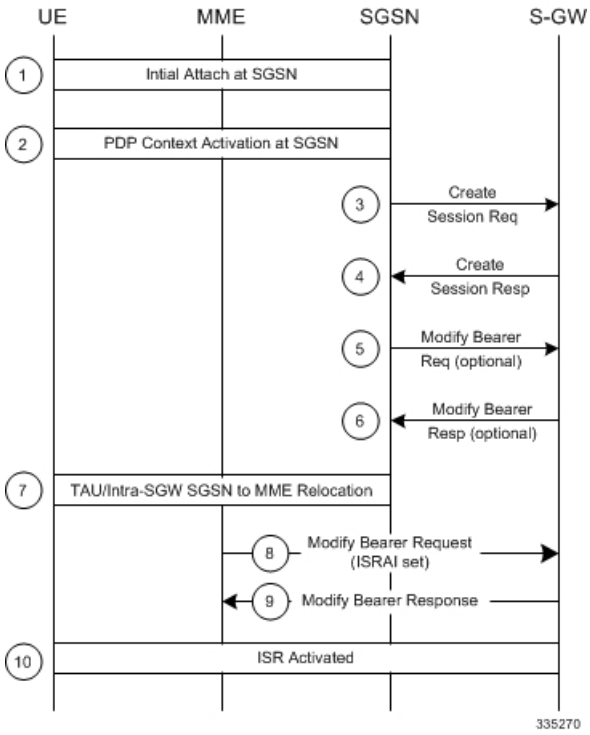


Notes:

- S3 Fwd relocation request/context response would indicate ISR support at MME via indication flag (ISRSI).
- If the SGSN also supports ISR, it activates and indicates so using ISRAI flag to the S-GW in an S4 modify bearer request message.

- The SGSN uses Context Ack/Fwd Relocation Complete response to indicate to MME that ISR has been activated. This ensures that the MME does not delete UE context.
- The MME also expects the HSS to not send a Cancel-Location-request to the MME.

Figure 18: ISR Activation During SGSN to MME Relocation



Notes:

- S3 Fwd relocation request/context response indicates ISR support at SGSN via indication flag (ISRSI).
- If the MME also supports ISR, it activates and indicates so using ISRAI flag to the S-GW in a S11 Modify Bearer Request message.
- The MME uses the Context Ack/Fwd Relocation Complete notification to indicate to the SGSN that ISR has been activated. This ensures that the SGSN does not delete the UE context.
- The MME sends a t3423 timer and sends the appropriate EPS Update result IE to UE in a TAU accept.

ISR Deactivation

The UE and the network run independent periodic update timers for GERAN/UTRAN and for E-UTRAN. When the MME or SGSN do not receive periodic updates, the MME and SGSN may decide independently for implicit detach, which removes session management (bearer) contexts from the CN node performing the implicit detach and it also removes the related control connection from the S-GW. Implicit detach by one CN node (either SGSN or MME) deactivates ISR in the network. It is deactivated in the UE when the UE cannot perform periodic updates in time. When ISR is activated and a periodic updating timer expires, the UE starts

a Deactivate ISR timer. When this timer expires and the UE was not able to perform the required update procedure, the UE deactivates ISR.

All special situations that cause context in the UE, MME and SGSN to become asynchronous are handled by ISR deactivation. The normal RAU/TAU procedures synchronize contexts in MME and SGSN and activate ISR again when wanted by the network.

ISR Behavior with Circuit Switched Fallback

ISR capability impacts some MME messaging when Circuit Switched Fallback (CSFB) is also implemented.

- When receiving a Paging Request from the MSC/VLR, the MME must initiate paging in both the E-UTRAN and the UTRAN/GERAN domains (as a UE in idle mode may be in either cell coverage).
- When the MSC/VLR initiates a Non-EPS Alert Procedure, the MME must inform the peer SGSN of the request. If there is signaling activity in the UTRAN/GERAN domain, the SGSN can inform the MME (via the S3 interface) to allow the MME to indicate activity to the MSC/VLR.
- IMSI-detach is allowed from the SGSN.

Standards Compliance

The ISR capability complies with the following standards for 3GPP LTE/EPS wireless networks:

- 3GPP TS 23401-970
- 3GPP TS 29274-940
- 3GPP TS 23272-990
- 3GPP TS 24301-950

Configuring ISR

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.

Use the following example to enable the ISR feature on the specified MME service

```
config
    context <context_name>
        mme-service <mme_svc_name> -noconfirm
            isr-capability
            exit
```

Verifying ISR Configuration

Use either of the following commands to display information to verify if ISR is enabled.

```
show mme-service all
show mme-service name  <mme_svc_name>
```

The output of this command displays the entire configuration for the MME service specified.

```
[local]asr5x00 show mme-service name mmesvc1
ISR Capability   : Enabled
```

Monitoring and Troubleshooting ISR

ISR Bulk Statistics

The following MME Schema bulk statistics have been introduced for the Idle-mode Signaling Reduction feature:

- isr-activated

The following eGTP-C Schema bulk statistics have been introduced for the Idle-mode Signaling Reduction feature:

- mobility-sent-cspagingind
- mobility-recv-cspagingind
- mobility-sent-alertmmenotf
- mobility-sent-retransalertmmenotf
- mobility-recv-alertmmenotf
- mobility-recv-retransalertmmenotf
- mobility-sent-alertmmeack
- mobility-sent-retransalertmmeack
- mobility-recv-alertmmeack
- mobility-recv-retransalertmmeack
- mobility-sent-alertmmeackaccept
- mobility-sent-alertmmeackdenied
- mobility-recv-alertmmeackaccept
- mobility-recv-alertmmeackdenied
- mobility-sent-ueactivitynotf
- mobility-sent-ueactivitynotf
- mobility-sent-retransueactivitynotf
- mobility-recv-ueactivitynotf
- mobility-recv-retransueactivitynotf
- mobility-sent-ueactivityack
- mobility-sent-retransueactivityack
- mobility-recv-ueactivityack

- mobility-recv-retransueactivityack
- mobility-sent-ueactivityackaccept
- mobility-sent-ueactivityackdenied
- mobility-recv-ueactivityackaccept
- mobility-recv-ueactivityackdenied
- mobility-sent-detachnotf
- mobility-sent-retransdetachnotf
- mobility-recv-detachnotf
- mobility-recv-retransdetachnotf
- mobility-sent-detachack
- mobility-recv-detachack
- mobility-sent-detachackaccept
- mobility-sent-detachackdenied
- mobility-recv-detachackaccept
- mobility-recv-detachackdenied

ISR Show Command(s) and/or Outputs

This section provides information regarding show commands and/or their outputs in support of ISR.

Only those counters which relate to ISR are shown.

show mme-service statistics

Table 11: ISR Deactivation Statistics

Field	Description
ISR Deactivation Statistics	
S3 path failure	The total number of Idle mode Signaling Reduction (ISR) deactivations due to failure in the S3 interface.
SGSN local detach	The total number of Idle mode Signaling Reduction (ISR) deactivations due to SGSN detach notification.
SGW relocation	The total number of Idle mode Signaling Reduction (ISR) deactivations due to S-GW relocation of the session to an MME/SGSN which does not support ISR.
CN Node relocation	The total number of Idle mode Signaling Reduction (ISR) deactivations due to CN Node relocation of the session to an MME/SGSN which does not support ISR.

Field	Description
Implicit detach	The total number of Idle mode Signaling Reduction (ISR) deactivations due to an idle timeout (implicit detach) initiated by either the MME or Peer SGSN.
Other detach procedures	The total number of Idle mode Signaling Reduction (ISR) deactivations due to an idle timeout (implicit detach) initiated by either the MME or Peer SGSN.
Other reasons	The total number of Idle mode Signaling Reduction (ISR) deactivations due to a reason not otherwise classified by one of the other ISR Deactivation Statistics categories.

show mme-service session full

Table 12: ISR Session Information

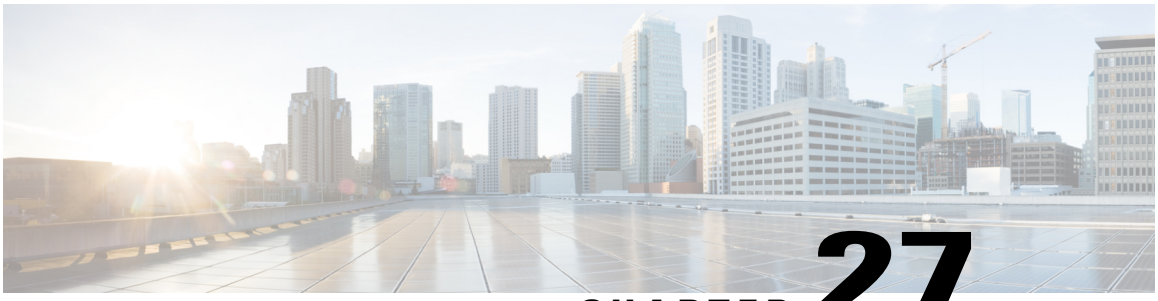
Field	Description
ISR Status	Displays if the session is using Idle mode Signaling Reduction (ISR). Possible configurations are Activated or Deactivated.
Peer SGSN	Displays the IP address of the SGSN which has a context for this UE in support of Idle mode Signaling Reduction (ISR). A Peer SGSN address is only shown when ISR is activated for this session.

show mme-service session summary

Table 13: ISR Session Summary

Field	Description
Total ISR-activated sessions	The current total number of MME sessions which are activated for ISR.

show egtpc sessions
Typically this command shows only one EGTP session (S11) per UE. When an ISR-activated UE is present, this command displays 2 EGTP sessions per UE.



CHAPTER 27

IMSI Manager Overload Control

Feature Description

The IMSI Manager is the Demux process that selects the Session Manager instance based on the Demux algorithm logic to host a new session for 2G/3G/4G subscribers for SGSN/MME. The IMSI Manager maintains the IMSI-SMGR mapping for SGSN (2G/3G) and MME (4G) subscribers. The mappings maintained for all registered subscribers are synchronous with the Session Managers.

When the incoming attach rate is high at the IMSIMGR in a short span of time, the CPU consumption is very high and affects the normal processing activities of the IMSI Manager. At times this can lead to an IMSI Manager crash. Overload control methods are devised through this feature enhancement to keep the IMSI Manager CPU under control.

Important This feature is enabled by default.

IMSI Manager Overload Control

IMSI Manager Overload control is implemented on both SGSN and MME call flows. Attach rate throttling(network overload protection) is implemented in IMSI Manager to cap the rate at which new requests are accepted by SGSN and MME. This feature helps us process the incoming new subscriber requests (for example ATTACH/ISRAU) at a configured rate, therefore the HLR and other nodes are not overloaded. The SGSN and MME have separate pacing queues in the IMSI Manager to monitor the incoming rate of requests and have a separate network overload configuration as well.

For the SGSN, the following requests are paced using the pacing queues:

- Initial ATTACH (with IMSI , L-PTMSI ,F-PTMSI)
- Inter-SGSN RAU
- Empty-CR requests

In the MME, new connections are setup for the following events:

- UE initiated initial Attach
- All types of attach – IMSI, local GUTI, foreign GUTI, mapped GUTI, emergency and so on.
- UE initiated Inter-CN node TAU request requiring context transfer from old MME/SGSN
- TAU request with foreign GUTI or mapped GUTI
- Peer SGSN/MME initiated forward relocation request via Gn/S10/S3

With this feature enhancement when the incoming attach rate is high, the pacing queue becomes full and the further requests are either dropped or forwarded to Session Manager. The Session Manager in turn sends the reject response based on the configuration. When network overload protection action is set as "reject", the IMSI Manager has to forward overflowing requests from the pacing queue to Session Manager through a messenger call to send back error response. The IMSI Manager spends more time on messenger read and write. The IMSI Manager CPU reaches high values when the incoming call rate is very high (both SGSN/MME) though the network overload protection is configured. To ensure that the IMSI Manager CPU is under control, the IMSI Manager reduces certain messenger activities on reaching the default CPU threshold of 70%. This threshold value is fixed and this feature is enabled by default. This value is currently non-configurable. The IMSI Manager drops the overflowing requests from the pacing queue when the CPU crosses 70% mark instead of rejecting the request. Every IMSI Manager instance monitors its CPU usage independently and actions are taken according to the CPU usage.

Relationships to Other Features

Attach throttling feature will have an impact due to this feature enhancement. Once the CPU reaches the threshold of 70%, the messages will be dropped (irrespective of configured action).

Monitoring and Troubleshooting IMSI Manager Overload Control

New statistics are introduced as a part of feature which can be viewed in the Debug mode. The operator can use these statistics to find the number of requests dropped due to overload.

Show Command(s) and/or Outputs

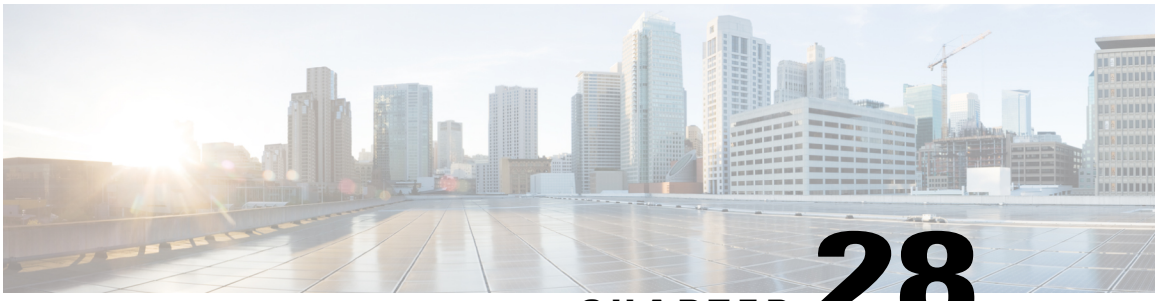
This section provides information regarding show commands and/or their outputs:

show demuxmgr statistics imsimgr all

These counters are available for both MME and SGSN separately.

- Requests dropped due to pacing queue with High Imsimgr CPU

Apart from the statistics listed above, SGSN Network Overload protection statistics which were only available in the show gmm-sm statistics are now available as a part of show demuxmgr statistics imsimgr all. The show output is realigned for better readability. Debug logs are also provided to display the current CPU usage.



CHAPTER 28

IMSI Manager Scaling on the MME

Simply put, IMSI Manager Scaling enables multiple IMSI Managers per MME. To facilitate MME operations on Cisco's higher capacity platforms, such as ASR 5500 and Cisco's Virtual Packet Core (VPC)- Distributed Instance (DI) platform, the MME enables scaling up the number of IMSI Managers supported on ASR 5500 and VPC-DI platforms. Scaling the number of IMSI Managers means the MME's IMSI Manager is not a bottleneck on enhanced platforms.

Feature Description

Overview

The IMSI Manager (IMSIMgr) is the de-multiplexing process that selects the Session Manager (SessMgr) instance to host a new session. The IMSIMgr selects the SessMgr instance based on a demux algorithm logic to host a new session by handling new calls requests from the MME Manager (MMEMgr), EGTPC Mgr, and the (e)SGTPCMgr (handles 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 (e.g., IMSI/GUTI) to the SessMgr instance.

With the addition of support for the expanded capacities of the VPC-DI and ASR5500 platforms, the MME's IMSIMgr had become a bottleneck. With Release 18.0, the **IMSI Manager Scaling** feature increases the number of IMSIMgrs that can be made available on the MME - scaling from 1 to a maximum of 4 in releases prior to 21.0 and a maximum of 8 from release 21.0 onwards. The number is configurable (see *Configuration* section below).

Important IMSIMgr Scaling is only available on the ASR 5500 and the VPC-DI platforms. The maximum number of IMSIMgrs supported on ASR 5000 and SSI platforms remains at "1".

Customers will notice the following when the configured number of IMSIMgrs setting is changed for 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 visualized 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 IMSI Mgr instance.

Relationships to Other Features

The MME's use of the following features has been changed when multiple IMSIMgrs are configured:

- Attach Rate Throttling
- MME per service session limits
- Monitor Subscriber 'next call'
- Congestion Control
- MME traps generated by IMSI Manager

For details about the changes, refer to the *How It Works* section.

How It Works

Workings of IMSIMgr Scaling

It is the MMEMgr/EGTPC Mgr/SGTPC Mgr that selects an IMSIMgr instance to be contacted for session setup. Each subscriber session in the SessMgr maintains the IMSIMgr instance ID that 'hosts' the mapping for this IMSI. This information is required when communicating during audit and session recovery scenarios.

With a single IMSIMgr instance present, there in only one centralized entry point for new calls into the system. By increasing the number of IMSIMgr instances, the new call handling (primarily for Attach and SGs procedures) capacity 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.

The IMSIMgr and SessMgr interactions are the same as those employed when IMSIMgr scaling is not implemented. Once the IMSI is found, the SessMgr performs hash on the IMSI to acquire the "target" IMSIMgr instance ID. Once the IMSI is known, the NOTIFY-IMSI Request will be sent from the SessMgr to the "target" IMSIMgr instance. The "target" IMSIMgr instance updates the mapping table with this "IMSIMgr ID" mapping. This ensures that any further IMSI-based requests from this subscriber will land on the correct SessMgr.

Attach Rate Throttling

With multiple IMSIMgrs, the configured number of allowed Attaches is divided between the configured number of IMSIMgrs. As throttling is now distributed, 100 accuracy cannot be achieved as with a single IMSIMgr, so a minor impact in accuracy based on the incoming rate in every IMSIMgr will result in a limited number of calls being dropped/rejected.

MME Service Session Limits

As a result of IMSIMgr Scaling, a behavior change has been implemented with regard to MME service session limits. Now all IMSIMgr instances will send the current count of sessions per MME service to the MMEMgr via existing response messaging. The MMEMgr shall send the same data received from multiple IMSIMgr instances back to the IMSIMgr in existing request messaging. As a result, each IMSIMgr shall 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. The per service session limit is configured by the command **bind s1-mme max-subscribers** *number* (refer to the *Command Line Interface Reference* for command details).

Monitor Subscriber 'next-call'Option

The monitor subscriber next-call option is used to trace the next incoming call into the system. With multiple IMSIMgr instances, the session controller now sends the next-call details to IMSIMgr instance 1. So, the next incoming call through IMSIMgr instance 1 is monitored.

Congestion Control

All IMSIMgrs will be involved in congestion control and traps will be generated by all IMSIMgrs. The IMSIMgrs are updated with information on critical parameters that lead to congestion control and each IMSIMgr instance sends traps indicating congestion status.

IMSIMgr ID in Traps

Each IMSIMgr instance independently generates traps for each new allowed or disallowed call. The trap information includes the IMSIMgr instance ID.

SessMgr Instance Mapping

From Release 18 and forward, the Diameter Proxy Server queries the MME's IMSIMgr instances to obtain IMSI information in support of SessMgr instance mapping.

Configuring IMSI Manager Scaling

This section documents configuration of IMSI Manager Scaling and configuration for related functionality.

Configuring Support for Multiple IMSIMgrs

The commands illustrated below configure the IMSI Managers parameters. In support of the IMSI Manager Scaling feature, the **max** keyword has been added to set the maximum number of IMSIMgrs that can be spawned on the MME.

Important The **max** keyword is only visible when the MME is running on an ASR 5500 or a VPC platform.

```
config
   task facility imsimgr { avoid-sessmgr-broadcast | max <number_imsimgrs> | sessmgr-sessions-threshold
high-watermark <high_value> low-watermark <low_value> }
   end
```

Notes:

- **max** *number_imsimgrs* must be an integer from 1 to 4 for release prior to 21.0. From release 21.0 onwards the maximum number of IMSI Managers per chassis is enhanced to “8”. The table below lists the default and maximum values for each platform:

Platform and card type	Default number of IMSI managers per chassis	Maximum number of IMSI managers per chassis
ASR5000 PSC/PSC2/PSC3	1	1
ASR5500 with DPC	4	4
ASR5500 with DPC2	8 **Note** For releases prior to 21.0, the default number of IMSI managers per chassis was "4"	8 **Note** For releases prior to 21.0, the default number of IMSI managers per chassis was "4"
VPC-SSI LARGE/MEDIUM	1 1	1 1
VPC-SSI SMALL/FORGE	1	1
SCALE LARGE/MEDIUM	4	4
ASR5700	4	4

- For further information on the other command keywords and the use of the command prefixes, refer to the *Command Line Interface Reference* for release 18.0 or higher.

Important **max** is a **boot-time** configuration setting. It should be added in the configuration file before any MME related configuration is created or any IMSI Manager is started. Run-time (dynamic) configuration of this parameter is stored but not effective until after the next **reboot**. Any attempt at dynamic configuration of this parameter results in a display of the following error message:

IMSImgrs already started. So modify the configuration file and reboot the system with updated configuration.

Verifying the IMSI Mgr Scaling Configuration

Either of the following commands can be used to display/verify the number of IMSIMgrs configured per chassis.
show task resources facility imsimgr all
show configuration

Note:

The task facility imsimgr max field has been added to the output of the **show configuration** command.

Configuring IMSIMgr Audit

With the ability to configure the MME to support more than one IMSIMgr instance, it becomes important to be able to selectively monitor each IMSIMgr instance. With the following command issued from the **Exec** mode, the operator can initiate an audit request for just one IMSIMgr instance at a time:

mme imsimgr instance *instance_id* **audit-with sessmgr { all | instance** *instance_id* **}**
Notes:

- **imsimgr instance** *instance_id*: Enter an integer from 1 to 4 to identify the specific IMSIMgr instance for which the audit is to be performed.
- **all | instance** *instance_id*: Select all to initiate an audit for all SessMgr instances or select instance and for *instance_id* enter an integer from 1 to 1152 to identify a specific SessMgr for the audit.

Monitoring and Troubleshooting the IMSIMgr Scaling

Displaying IMSIMgr Instance Information

The following commands generate output that displays information about IMSIMgr Instances:

show subscribers mme-only full all - This command displays IMSIMgr instance information for subscriber session(s).

show mme-service session full all - This command displays IMSIMgr instance information for MME service session(s).

show mme-service db record call-id - This command displays IMSIMgr instance information based on call-id records.

Displaying IMSIMgr Selection Counter Information

The following commands generate output that displays selection counter information for an IMSIMgr instance:

show demux-mgr statistics sgtpcmgr instance *instance* - This command updates to display IMSI Mgr selection counter information.

show demux-mgr statistics egtpegmgr all - This command updates to display IMSI Mgr selection counter information.

show session subsystem facility mmemgr instance *instance* - This command updates to display IMSIMgr selection counter information.

Displaying IMSIMgr Instance Information in the SNMP Trap

Use the following command to display IMSIMgr instance specific fields in the SNMP trap:

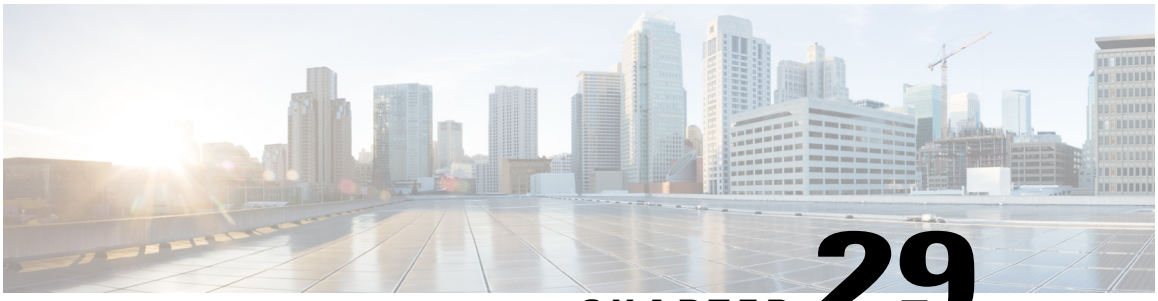
show snmp trap history - SNMP trap now includes the IMSIMgr instance information

- Internal trap notification 1249 Imsimgr instance: 1 (MMENewConnectionsDisallowed) - MME new connections disallowed, initial reason test

- Internal trap notification 1249 Imsimgr instance: 1 (MMENewConnectionsDisallowed) - MME new connections allowed

Bulk Statistics

Currently, there are no bulk statistics used to track IMSIMgr instance-specific information.



CHAPTER 29

Integrity and Confidentiality Algorithms for UE

This chapter describes the implementation of Integrity and Confidentiality Algorithms for UEs in Liminted Service Mode (LSM), and UEs that cannot be authenticated by the MME, to establish emergency calls.

Feature Description

In this feature, UEs that are in limited service mode (LSM) and UEs that cannot be authenticated by the MME are allowed to establish emergency calls.

MME uses EEA0 (Integrity) and EIA0 (Ciphering) algorithms for emergency attach requests even if the UE does not advertise the support of these algorithms in the request message, to successfully process the VoLTE emergency calls. These algorithms successfully process the VoLTE calls irrespective of the validation level configured for a UE.

The MME provides options to authenticate emergency attaches using the following CLI:

ue-validation-level { auth-only | full | imsi | none }

Using the above command syntax, it is possible to configure the MME to allow or disallow unauthenticated UEs in LSM to establish bearers for emergency calls. To establish bearers for an emergency call for unauthenticated UEs in LSM, the MME allows NAS protocol to use EIA0 and EEA0 as the integrity and ciphering algorithm respectively.

If the MME allows an unauthenticated UE in LSM to establish bearers for emergency calls on receiving an emergency attach request message from the UE, the MME:

- Selects an algorithm based on the UE's announcement only if the MME supports the requested algorithm. If the MME does not support the requested algorithm or if there is no algorithm announced, then the EEA0 and EIA0 algorithms are used.
- Set the UE EPS security capabilities to only contain EIA0 and EEA0 when sending these to the eNB in the following messages:
  - S1 UE INITIAL CONTEXT SETUP
  - S1 UE CONTEXT MODIFICATION REQUEST

- S1 HANDOVER REQUEST

Note As a result, the MME only sends a UE with EPS security capability containing EIA0 and EEA0 to the eNB when selecting EIA0 for NAS integrity protection because the eNB is only capable of selecting EIA0 for AS integrity protection and EEA0 for AS confidentiality protection. In general, if EIA0 is used for NAS integrity protection, then EIA0 will always be used for AS integrity protection or vice-versa

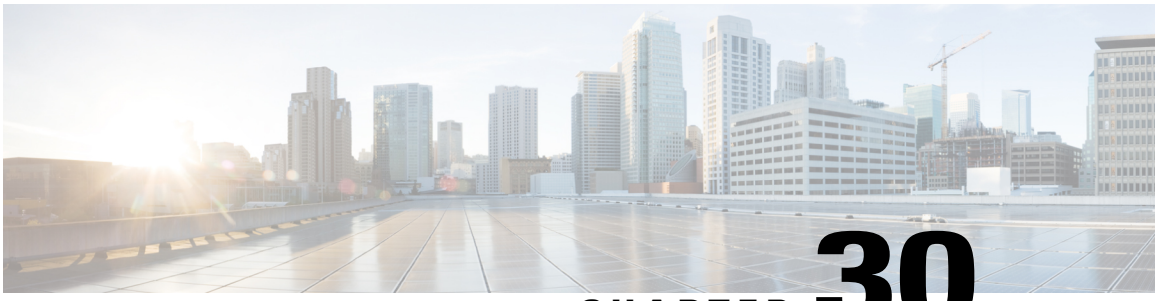
The rules for when the MME selects the EIA0 for NAS integrity protection, and when the UE accepts a NAS security mode command selecting EIA0 for NAS integrity protection depends on whether the UE and MME can be certain that no EPS NAS security context can be established. For more information on these rules, refer to *3GPP 33.401 specifications* document.

Configuration Information

The MME provides options to authenticate emergency attaches using the following CLI:

ue-validation-level { auth-only | full | imsi | none }

- The ***auth-only*** keyword specifies that only authenticated UEs are allowed to use the emergency bearer services.
- The ***full*** keyword specifies that only UEs that have been authenticated, and have successfully passed subscription and location validation, are allowed to use the emergency bearer services.
- The ***imsi*** keyword specifies that UEs with an International Mobile Subscriber Identity are allowed to use the emergency bearer services regardless of authentication. Even if authentication fails, the UE is granted access to use emergency bearer services.
- The ***none*** keyword specifies that all UEs are allowed to use the emergency bearer services. This keyword is used as a default option.



CHAPTER 30

IPNE Service

With Release 18, the MME supports IP Network Enabler (IPNE).

Important This feature, with its CLI commands, counters, and statistics, are all under development for future use and the information listed here is recommended for testing and lab use only. When the feature is ready for deployment then additional information will be added to this chapter.

Feature Description

IP Network Enabler (IPNE) is a Mobile and IP Network Enabler (MINE) client component that collects and distributes session and network information to MINE servers. 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.

The information is shared between the MINE server and IPNE service in the form of XML data. The core object in the IPNE service is the XMPP protocol engine. There is one XMPP protocol engine instance for each configured MINE server peer. The engine implements the XMPP protocol using FSM.

All information that is shared is derived from the context at that instance in time. An IPNE service level scheduler is also implemented to rate-control the feed and notification activities on all the handles to avoid overload which would affect call processing and data path performance.

With support of the IPNE interface and IPNE Service, the MME is able to export the following information to the CSB (Cisco Service Bus):

- UE Location Information
- UE Mobility Information

The ability to export to the CSB makes it possible for operators to design and/or implement solutions and services for network optimization, congestion, troubleshooting and monetization with the information exported from the MME.

IPNE is a licensed Cisco feature. Contact your Cisco account representative for information on licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section in the *System Administration Guide.*

How It Works

IPNE

When the MME service is associated with an IPNE service, then the MME service communicates with the IPNE service through the Session Manager over a SINE interface. The IPNE service communicates with CSB over XMPP protocol.

Information is exchanged between the modules in the form of clp handles. For each session one IPNE handle is created.

Configuring MME Use of IPNE

There are multiple components that need to be configured to enable the MME to utilize the IPNE service:

- IPNE service
- IPNE endpoint
- association with MME service

Configuring IPNE Service

The IPNE service is a separate service configuration.

Important We recommend that you configure the IPNE service in the same context in which the MME service has been configured.

```
config
    context context_name
        ipne-service ipne_svce_name
        end
```

Notes:

- *ipne_service* - Enter 1 to 63 alphanumeric characters to create a *unique* IPNE service name within the context and to enter the IPNE Service configuration mode. Entering the mode provides access to the commands, such as **ipne-endpoint**, needed to configure the IPNE service parameters.
- **no** - As a prefix of the command disables the feature when it has been enabled with this command and removes the IPNE service definition from the MME's configuration. If an IPNE service is to be removed

and the service has actives handles, then the handles are deleted using a timer-based approach and then the IPNE service is removed.

Configuring the IPNE Endpoint

After the IPNE service is created, the IPNE endpoint definition should be added to the configuration. An IPNE endpoint is a combination of a local IP address, a peer address and, optionally, a port. Entering the **ipne-endpoint** command also provides access to the commands in the IPNE Endpoint configuration mode that are used to define the operational parameters required by the endpoint.

config
context *context_name*
ipne-service *ipne_svce_name*
ipne-endpoint
bind { ipv4-address | ipv6 address } *ip_address*
peer { ipv4-address | ipv6 address } *ip_address*
end
no { bind | peer }

Notes:

- **{ ipv4-address | ipv6-address }** *ip_address*: Identify the type of IP address - either IPv4 or IPv6 - and then enter either an IPv4 dotted-decimal or an IPv6 colon-separated hexadecimal notation.
- As part of the **bind** command, the IP address identifies the IPNE client socket as the local address.
- As part of the **peer** command, the IP address identifies the MINE server as the peer address.
- **no** - Include as a prefix of either the **bind** or **peer** command to remove the bind address or the peer address from the IPNE endpoint configuration.

Configuring the Association with MME Service

A special **ipne-service** keyword has been added to the **associate** CLI to associate the created IPNE service with the MME service:

configure
context *context_name*
mme-service *mme_srvc_name*
associate ipne-service *ipne_srvc_name*
no associate ipne-service
end

Notes:

- *ipne_srvc_name* - Enter 1 to 63 alphanumeric characters to identify the *unique* IPNE service name that is within the same context as the MME service configuration.
- **no**- Include as a prefix of the command to disassociate the IPNE service definition from the MMEs service configuration.

Monitoring and Troubleshooting the IPNE Service

Show Command(s) and/or Outputs

This section provides information regarding show commands and/or their outputs in support of using the IPNE service on the MME.

show ipne peers { all | service | summary }

This command generates a display of information for the IPNE service(s) and the TCP connection status for associated Session Manager(s). The following are sample displays:

```
[local]asr5000 show ipne peers all
SESSMGR :  1
Service Name: ipne-service         Contex id: 3
Version : n/a
Local Address  : 192.168.120.1:45161
Peer Address : 192.168.120.7:5222    State : [OPEN 0/1] [TCP]
```

```
[local]asr5000 show ipne peers summary
Service Name: ipne-service Contex id: 3
Version : n/a
Local Address : 192.168.120.1:45161
Peer Address : 192.168.120.7:5222 State : [OPEN 144/144] [TCP]
```

Notes:

- **all** - Lists all of the peers of each IPNE service and the state of the TCP connections for every SessMgr. This command with **all** option is part of the support details (SSD) procedure.
- **service** - Requires the inclusion of an IPNE service name and displays information only for that service.
- **summary** - Generates a display similar to the **all** display but provides only summary TCP connection information for the SessMgrs.

show ipne statistics { all | service | summary }

This command generates a display of information regarding the number of IPNE handles of each IPNE service and count information for query/response/subscription/feed messages for the SessMgrs. The command generates a display similar to the following:

```
[local]asr5000 show ipne statistics all
SESSMGR :  1
Service Name: ipne-service         Context id: 3
Total handles: 0
Local Address  : 192.168.120.1:0
Peer Address : 192.168.120.7:5222
Total query          : 0
Total query response : 0            Success : 0            Failure : 0
Total update         : 0
Total update response: 0            Success : 0            Failure : 0
Total subscription   : 0            Add     : 0            Delete  : 0
Total feed           : 0            Add     : 0            Delete  : 0
Total notification   : 0
Total XML parser error: 0
IPNE messages discarded on tx queue:
```

```
Total discards       : 0
 Total Feed           : 0            Notify  : 0            Response :0
[local]asr5000 show ipne statistics summary
 Service Name: ipne-service Context id: 3
 Total handles: 0
 Local Address : 192.168.120.1:0
 Peer Address : 192.168.120.7:5222
 Total query : 0
 Total query response : 0      Success : 0      Failure : 0
 Total update : 0
 Total update response: 0      Success : 0      Failure : 0
 Total subscription : 0        Add : 0          Delete : 0
 Total feed : 0                Add : 0          Delete : 0
 Total notification : 0
 Total XML parser error: 0
 IPNE messages discarded on tx queue:
 Total discards : 0
 Total Feed : 0      Notify : 0      Response : 0
```

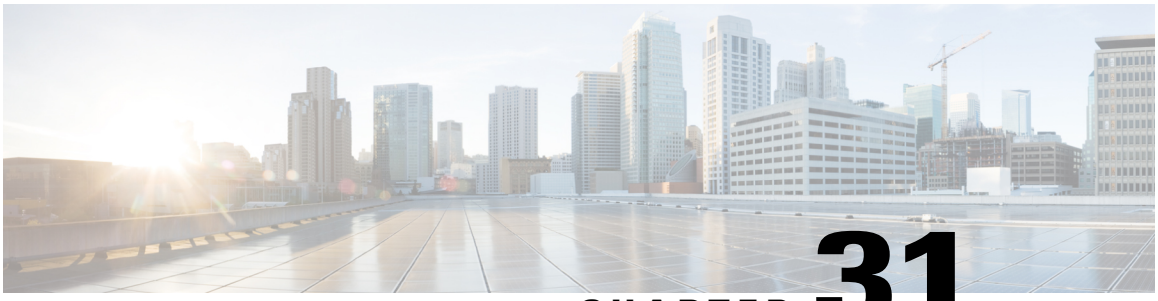
Notes:

- **all** - Lists all of the peers of each IPNE service and the state of the TCP connections for every SessMgr. This command with the **all** option is part of support details (SSD) procedure.
- **service** - Requires the inclusion of an IPNE service name and displays information only for that service.
- **summary** - Generates a display similar to the **all** display but provides only summary TCP connection information for the SessMgrs.

show bulkstats variables mme

Entering this command causes the system to display all of the bulk statistic variables in the MME schema. The 6 bulk statistic variables listed below have been added to the MME schema to enable the operator to track messaging related to IPNE-paging. For descriptions of the bulk statistic variables, refer to the *Statistics and Counters Reference* for StarOS Release 18 or higher.

- signaling-ipne-paging-init-events-attempted
- signaling-ipne-paging-init-events-success
- signaling-ipne-paging-init-events-failures
- signaling-ipne-paging-last-enb-success
- signaling-ipne-paging-last-tai-success
- signaling-ipne-paging-tai-list-success



CHAPTER 31

Limiting the Number of SGWs Tried

This feature enables the operator to configure the number of pooled SGWs to be tried.

Feature Description

With Releases 18.6, 19.4, 20.0 and higher, the operator can configure the MME to enable limiting the number of SGWs tried when the MME is attempting to find an available SGW during Attach or Handover procedures. If the feature-specific **sgw-retry-max** command is configured, as described in the *Configuring a Limit to the Number of SGWs Tried* section (see below), then:

- the MME's default retry behavior is ignored, and
- the MME limits the retries with different SGWs from the DNS pool to only retry a maximum of the configured number of times.

Default Behavior

If this feature is not enabled or is disabled, the MME uses or falls back to the default behavior which is in compliance with 3GPP TS 29.274, Section 7.6. The MME sends Create-Session-Request message to one SGW in the pool. If the SGW node is not available, the MME picks the next SGW from the pool and again sends a Create-Session-Request message. The MME repeats this process. For an Attach procedure, the MME tries up to five (1 + 4 retries) different SGWs from the pool. In the case of a HO procedure, the MME will try every SGW in the entire pool of SGWs sent by the DNS. If there are no further SGW nodes available in the DNS pool or if the guard timer expires, then MME stops trying and sends a Reject with cause "Network-Failure" towards the UE and the UE must restart the Attach/Handover procedure.

Benefits

The amount of signaling at Attach or Handover can be reduced.

The amount of time to find an available SGW can be reduced.

How It Works

The operator has access to a feature-specific CLI command **sgw-retry-max** to enable this feature and override the default behavior. **sgw-retry-max** configures the maximum number of SGWs to be *retried* from the DNS pool list during either Attach or Handover procedures. So the limit to the number of tries will be 1 + limit set.

For either Attach or Handover procedures, the MME sends Create-Session-Request message to one SGW in the pool. If the SGW node is not available, the MME picks the next SGW from the pool and retries. It again sends a Create-Session-Request message. At most, the MME retries only as many times as the number of retries configured with the **sgw-retry-max** command. If no SGW responds or only responds negatively and the MME reaches the configured limit for retries, then MME stops trying and sends the UE a Reject with cause "Network-Failure". At this point, the UE must restart the Attach/Handover procedure.

This feature-specific command is available for provisioning in both the MME service configuration and the Call-Control Profile configuration. To enable the feature, the feature-specific command must be configured under MME service configuration. We recommend provisioning under both modes. If **sgw-retry-max sgw-retry-max** command is configured under both MME service and Call-Control Profile, then the configuration under Call-Control Profile takes precedence.

The configuration under the Call-Control Profile provides the operator with additional control over "roamers" and "homers". For example, if **sgw-retry-max** under Call-Control Profile is set to 2 and if **sgw-retry-max** under MME service is set to 4, then if a "homer" subscriber Attaches, the MME retries 2 times but for all the subscribers other than "homers" the MME retries 4 times.

The feature is disabled with the entry of **no sgw-retry-max no sgw-retry-max** in the configuration. The MME reverts to the use of the default behavior.

Important To change the Reject cause code sent by the MME, use the **local-cause-code-mapping gw-unreachable** command in the Call-Control Profile configuration mode. Refer to the *Call-Control Profile Configuration Mode Commands* section in the *Command Line Interface Reference* for details.

Configuring a Limit to the Number of SGWs Tried

Enabling the Feature in the MME Service

Using the following configuration enables this feature in the MME service configuration. This feature sets the maximum number of SGW selection *retries* to be attempted during Attach/HO/TAU. This means, the total number of tries would be 1 (the initial try) + the **sgw-retry-max** value (the maximum number of retries).

```
configure
    context ctxt_name
        mme-service service_name
            sgw-retry-max max_number
            end
```

Notes:

- *ctxt_name* - Identifies the context in which the MME service configuration resides. Enter a string of 1 through 79 alphanumeric characters

- *service_name* - Identifies the previously configured MME service. Enter a string of 1 through 79 alphanumeric characters.
- *max_number* - Sets the maximum number of retries possible. Enter an integer from 0 to 5. If 0 (zero) is configured, then the MME sends Create-Session-Request to the 1st SGW and if that SGW does not reply, the MME does not select any further SGW to retry. The MME then rejects the ongoing procedure (Attach/HO/TAU) and sends a Reject message.
- Entering this command enables the feature which overrides the default behavior.
- To disable this feature, enter **no sgw-retry-max** . The MME falls back to the default behavior.

Enabling the Feature for Call-Control Profile

Using the following configuration enables this feature in the Call-Control Profile configuration. This feature sets the maximum number of SGW selection *retries* to be attempted during Attach/HO/TAU. This means, the total number of tries would be 1 (the initial try) + the **sgw-retry-max** value (the maximum number of retries).

configure
call-control-profile *profile_name*
sgw-retry-max *max_number*
end

Notes:

- *profile_name* - Identifies the previously configured Call-Control Profile. Enter a string of 1 through 64 alphanumeric characters.
- *max_number* - Sets the maximum number of retries possible. Enter an integer from 0 to 5. If 0 (zero) is configured, then the MME sends Create-Session-Request to the 1st SGW and if that SGW does not reply, the MME does not select any further SGW to retry. The MME then rejects the ongoing procedure (Attach/HO/TAU) and sends a Reject message.
- Entering this command provides the operator with greater control over "roamers" and "homers". For example, if **sgw-retry-max** under Call-Control Profile is set to 2 and if **sgw-retry-max** under MME service is set to 4, then if a “homer” subscriber Attaches, the MME retries 2 times but for all the subscribers other than “homers” the MME retries 4 times.
- If the **sgw-retry-max** command is configured under both MME service and Call-Control Profile, then the configuration under Call-Control Profile takes precedence.
- To remove this configuration from the Call-Control Profile, enter **no sgw-retry-max** .

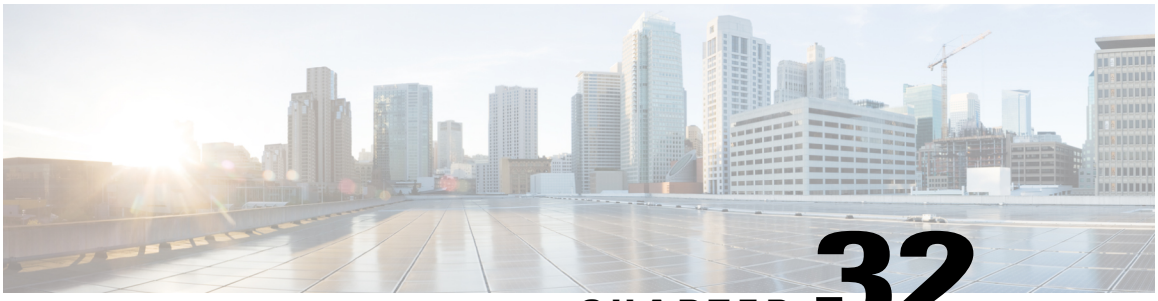
Verifying the Feature Configuration

Use the **show configuration** command to generate output that displays the values configured with **sgw-retry-max** . The following illustrates the sections of the output that will indicate the sgw-retry-max configuration for either or both MME service and Call-Control Profile:

(please note that variables shown are for clarification and are not suggested or real)

```
[local]hostname# show configuration
... ...
 mme-service mmesvc
... ...
   bind s1-mme ipv4-address 192.xx.xx.2
   msc default ip-address 192.xx.xx.56
   sgw-retry-max 2
```

```
  exit
... ...
... ...
 call-control-profile ccp
... ...
   s1-reset detach-ue
   sgw-retry-max 3
  exit
```



CHAPTER 32

Load Balancing and Rebalancing and VoLTE Offloading

Feature Description

The sections below describe the load balancing and rebalancing functionality available on the MME. The MME also supports VoLTE Offloading.

Load Balancing

Load balancing on the MME 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 Rebalancing

The MME load rebalancing functionality permits UEs that are registered on an MME (within an MME pool area) to be moved to another MME in the pool. 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.

The eNodeBs may have their load balancing parameters adjusted beforehand (e.g., the weight factor is set to zero if all subscribers are to be removed from the MME, which will route new entrants to the pool area into other MMEs).

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.

Relationships to Other Features

MME load balancing can be used in conjunction with congestion control. For more information on congestion control, refer to the *Congestion Control* section in the Mobility Management Entity Overview chapter of the *MME Administration Guide*.

How it Works

Load Balancing

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 set by the operator according to the capacity of an MME node relative to other MME nodes. The **relative-capacity** mme-service level command is used to specify this relative weighting factor.

Once set, the Relative MME Capacity IE is included in the S1AP S1 SETUP RESPONSE message from MME to relay this weight factor. If the relative MME capacity is changed after the S1 interface is already initialized, then the MME CONFIGURATION UPDATE message is used to update this information to the eNodeB.

Load Rebalancing

The MME uses the **mme offload mme-service** exec level command to enable the operator to offload UEs for a particular mme-service for load rebalancing among MMEs in a MME pool area. The command enables the operator to specify a percentage of UEs to offload, and the desired time duration in which to complete the offload.

The operator can also include the keyword option **disable-implicit-detach**. By default, if the UE context is not transferred to another MME within 5 minutes, the UE will be implicitly detached. This option disables this implicit detach timer.

To offload ECM-CONNECTED mode UEs, the MME initiates the S1 Release procedure with release cause "load balancing TAU required".

To offload UEs which perform TA Updates or Attaches initiated in ECM-IDLE mode, the MME completes that procedure and the procedure ends with the MME releasing S1 with release cause "load balancing TAU required".

To offload UEs in ECM-IDLE state without waiting for the UE to perform a TAU or perform Service request and become ECM CONNECTED, the MME first pages the UE to bring it to ECM-CONNECTED state.

Call Handling and Other Messaging Considerations

New calls are processed normally (as per the new call policy configuration). The offloading process does not reject INIT UE messages for new subscribers. To prevent new calls from entering this MME, set the **relative-capacity** on this mme-service to 0.

When Init UE messages are received for an existing offloaded subscriber, the ue-offloading state is set as MARKED and the offload procedure continues until the UE is offloaded.

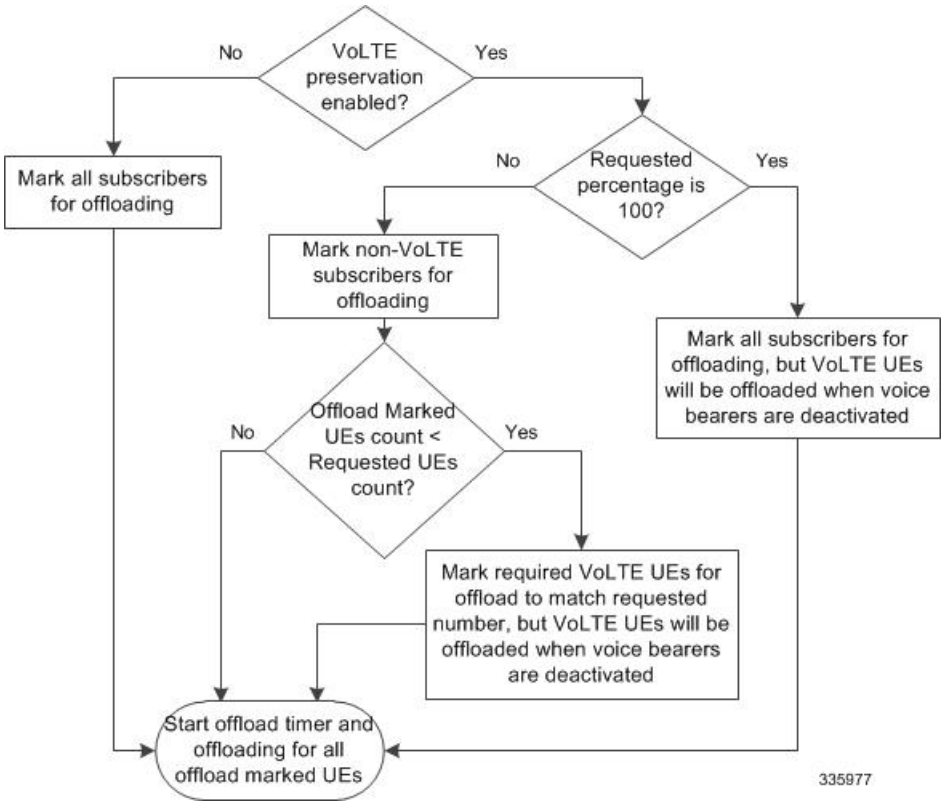
Once a UE is offloaded, messages such as EGTP events, Create bearer, Update bearer, Idle mode exit, and Paging trigger are be rejected. HSS initiated events also will be rejected for offloaded UEs.

Detach events are processed as usual.

Important Emergency attached UEs in Connected or Idle mode are not considered for offloading.

VoLTE Offloading

The **mme offload** command is enhanced with the keyword **preserve-volte-subscribers** , this keyword enables preservation of subscribers with voice bearers (QCI=1) from offloading until the voice bearers are deactivated. In any MME service both VoLTE and Non-VoLTE subscribers are present. The offload command now has options to configure the percentage of total subscribers to be offloaded and to preserve VoLTE subscribers from offloading until voice calls are terminated. With this feature enhancement if VoLTE preservation is not enabled, all subscribers are marked for offloading. But when the keyword **preserve-volte-subscribers** is enabled, Non-VoLTE subscribers are first marked for offloading based on configured offload-percentage. If the configured offload-percentage is greater than the available Non-VoLTE subscribers, VoLTE subscribers are also marked for offloading but the VoLTE UEs will be offloaded only when voice bearers are deactivated.



Configuring Load Balancing and Rebalancing

Configuring Load Balancing

Set the relative capacity of an MME service to enable load balancing across a group of MME services within an MME pool.

Use the following example to set the relative capacity of this MME service. The higher the value, the more likely the corresponding MME is to be selected.

```
config
    context context_name
        mme-service mme_svc -noconfirm
            relative-capacity rel_cap_value
            exit
```

Notes:

- **relative-capacity** *rel_cap_value* -- This command specifies a weight factor such that the probability of the eNodeB selecting this MME is proportional to this value in relation to other MMEs in a pool. *rel_cap_value* define the relative capacity by entering an integer from 0 to 255. The default relative capacity for an MME service is 255.
- The weight factor of the MME is sent from the MME to the eNodeB via S1-AP messages using the Relative MME Capacity S1AP IE in the S1AP S1 Setup Response. If the relative MME capacity is

changed after the S1 interface is already initialized, then the MME Configuration Update message is used to update this information to the eNodeB.

Verifying Load Balancing

Enter the **show mme-service all** causes the MME to generate a display similar to the following to indicate the configured relative capacity:

```
[local]asr5000# show mme-service all
Relative Capacity:      50
```

Performing Load Rebalancing (UE Offloading)

Start Offloading

The following example command rebalances (offloads) 30 percent of all UEs from the specified MME service (to other MME services in the MME pool) over the course of 10 minutes.

mme offload mme-service mme_svc time-duration *10* **offload-percentage** *30* **-noconfirm**
This command can also be entered with the **disable-implicit-detach** option. By default, if the UE context is not transferred to another MME within 5 minutes, the UE will be implicitly detached. This option disables this implicit detach timer.

mme offload mme-service *mme_svc* **time-duration** *10* **offload-percentage** *30* **disable-implicit-detach -noconfirm**

Stop Offloading

To stop the offloading process, issue the command with the **stop** keyword option.

mme offload mme-service *mme_svc* **stop -noconfirm**

Verifying Load Rebalancing (UE Offloading)

The following command shows the offload configuration as well as the status of the rebalancing.

show mme-service name *svc_name* **offload statistics**

```
[local]asr5000 show mme-service name mme1 offload statistics
Current Offload Status: In Progress
Implicit Detach Status: Enabled
Time Duration Requested: 600 secs
Percentage of Subscribers Requested: 30
Total Number of Subscribers: 0
Total Number of Subscribers to be Offloaded: 0
Total Number of Subscribers Offloaded: 0
Total Number of Subscribers Received Context Transfer: 0
Remaining Time:  0 secs
```

Where the Current Offload Status field will report one of the following:

- **Not Started** No UEs marked for offloading and no UEs currently being offloaded.
- **In Progress** MME is currently offloading marked UEs.
- **Completed** Offload procedure is completed or has been terminated by operator using **stop** keyword.

These counters are reset each time an offload procedure is initiated, or when the following command is entered:

clear mme-service statistics offload

Configuring VoLTE Offloading

The following configuration command is used to configure preservation of VoLTE subscribers from offloading during active calls (QCI=1); the offload command is enhanced with the key word**preserve-volte-subscribers** :

mme offload mme-service *mme_svc_name* **{ time-duration** *minutes* **offload-percentage** *percent* **[disable-implicit-detach | preserve-volte-subscribers]] | stop } [- noconfirm]**
By default, the subscribers with voice bearer with QCI = 1 will not be preserved during MME offloading. Configuring the keyword **preserve-volte-subscribers** enables preservation of subscribers with voice bearer.

The following example command re-balances(offloads) 30 percent of Non-VoLTE subscribers from the specified mme-service (to other mme-services in the MME pool) over the course of 30 minutes with VoLTE preservation.

mme offload mme-service *mmesvc* **time-duration** *30* **offload-percentage** *30* **preserve-volte-subscribers**

Verifying VoLTE Offloading

The following show command display is used to verify if VoLTE preservation is enabled and the number of VoLTE subscribers preserved during offloading:

show mme-service name *svc_name* **offload statistics**

```
Current Offload Status : Completed
Implicit Detach Status : Disabled
Preserve VoLTE subscribers Status : Enabled
Time Duration Requested : 60 secs
Percentage of Subscribers Requested : 1
Total Number of Subscribers : 0
Total Number of Subscribers Marked for Offloading: 1
Total Number of Subscribers Offloaded : 0
Total Cumulative Number of Subscribers Offloaded: 2
Total Number of VoLTE Subscribers Preserved : 0
Total Cumulative Number of VoLTE Subscribers Preserved:7
Total Number of Subscribers Received Context Transfer: 0
Remaining Time : 0 secs
```

Monitoring and Troubleshooting

The following sections describe commands available to monitor and troubleshoot this feature on the MME.

Show Command(s) and/or Outputs

This section provides information regarding show commands and their outputs in support of load rebalancing (UE offload).

The following show command displays current statistics for the Load Rebalancing feature.

show mme-service name *mme_svc* **offload statistics**

Table 14: show mme-service name <mme_svc_name> offload statistics

Field	Description
Current Offload Status	Current offload status of the specified mme-service. Possible values are Not Started, In Progress and Completed.
Implicit Detach Status	The Implicit Detach Status specified in the **mme offload** command. When enabled, if the UE context is not transferred to another MME within 5 minutes then it will be implicitly detached.
Preserve VoLTE subscribers Status	Is displayed as "Enabled" when the keyword **preserve-volte-subscribers** is configured in the mme offload command. The status is displayed as "Disabled", when VoLTE preservation is not configured. By default VoLTE preservation is disabled.
Time Duration Requested	The time-duration value specified in the **mme offload** command (in seconds). This is the maximum allowed time for the offload procedure to complete.
Percentage of Subscribers Requested	The offload-percentage specified in the **mme offload** command (specified as a percentage of all UEs on this mme-service).
Total Number of Subscribers	The total number of UEs on the specified mme-service.
Total Number of Subscribers Marked for Offloading	Displays the total number of subscribers marked for offloading during the current MME offload.
Total Number of Subscribers to be Offloaded	Total number of UEs on the specified mme-service selected for offloading.
Total Number of Subscribers Offloaded	The total number of UEs which have been successfully offloaded from this mme-service (UE offloading State/Event = Done).
Total Cumulative Number of Subscribers Offloaded	Displays the cumulative count of subscribers offloaded.
Total Number of VoLTE Subscribers Preserved	Displays the number of preserved VoLTE subscribers during and after MME offload.
Total Cumulative Number of VoLTE Subscribers Preserved	Displays the total numbers of subscribers preserved before starting the offload timer when the **mme offload** command is executed.
Total Number of Subscribers Received Context Transfer	Total number of UEs which has been successfully context transferred to another MME.

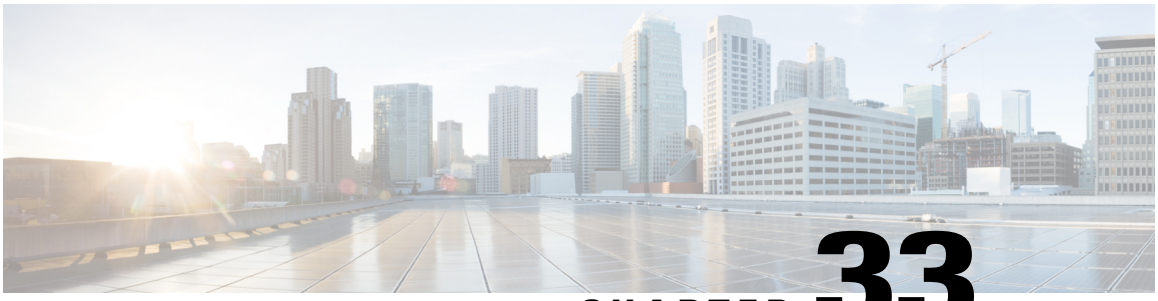
Field	Description
Remaining Time	The number of seconds remaining to complete the offload procedure.

The following command also provides information relating to load balancing:

show mme-service session full all
Only the output field which relates to load rebalancing is shown.

Table 15: show mme-service session full all

Field	Description
UE Offloading	Displays the UE offload state. Possible values are None, Marked, In-Progress and Done.



CHAPTER 33

Local Emergency Numbers List

Feature Description

Local Emergency Numbers List contains a list of emergency numbers that a caller uses to contact emergency services for assistance. Local Emergency Numbers List might differ from one country to another. The emergency numbers are usually configured as a three digit number for quick dialing.

The Local Emergency Numbers List contains additional emergency numbers used by the serving network. This list can be downloaded by the network to the User Equipment (UE) at successful registration as well as subsequent registration updates.

Important The UE uses the stored Local Emergency Numbers List received from the network in addition to the emergency numbers stored on the USIM or UE to detect if the number dialed is an emergency number.

A valid license key is required to enable this feature. Contact your Cisco Account or Support representative for information on how to obtain a license. This license was not enforced in earlier releases.

How It Works

When a User Equipment is activated, the network sends a Local Emergency Numbers List to the UE through the ATTACH ACCEPT or the TRACKING AREA UPDATE ACCEPT messages. The user equipment stores the Local Emergency Numbers List provided by the network. The Local Emergency Numbers List, stored in the user equipment, is replaced on each receipt of the Emergency Number List IE.

The emergency number(s) received in the Emergency Number List IE, which is stored in the UE are valid only in the networks that belong to the same country. If the user equipment registers to a PLMN in a country different from that of the PLMN that sent the list, then the new network replaces the existing Local Emergency Numbers List IE list in the UE.

If the ATTACH ACCEPT or the TRACKING AREA UPDATE ACCEPT message does not contain the Local Emergency Numbers List, then the existing Local Emergency Numbers List in the UE is retained.

The Local Emergency Numbers List is deleted when the UE or USIM is switched off. The user equipment stores up to ten local emergency numbers received from the network. The operator can view the Attach Accept message and the TAU message by running the monitor protocol in the CLI command prompt.

Limitations

The UE can download and store a maximum of only ten local emergency numbers from the network. Therefore, the MME supports the configuration of only ten local emergency numbers for a single UE.

Standards Compliance

The Local Emergency Number List IE feature complies with the following standards:

- 3gpp TS 24.301, Version 11.10.0, Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS)
- 3gpp TS 24.008, Version 11.10.0, Mobile radio interface Layer 3 specification Core network protocols

Configuring Local Emergency Number List IE

This section documents configuration of Local Emergency Numbers List IE and configuration for related functionality.

Configuring Local Emergency Numbers

The Local Emergency Number List is configured under the lte-emergency-profile in the MME Service Configuration mode.

The following CLI commands are used to configure the Local Emergency Numbers in a particular network. By default, the emergency number list is sent through ATTACH ACCEPT messages.

The configuration given below allows the operator to send the Local Emergency Numbers through Attach or TAU messages.

config
lte-policy
lte-emergency-profile *profile_name*
local-emergency-num *emergency_number* **{ ambulance | custom** *custom_name* **| fire | marine-gaurd | mountain-rescue | police }**
end

The configuration given below allows the operator to send the Local Emergency Numbers through TAU Accept messages during Inter-MME-TAU messages or all TAU messages.

config
lte-policy
lte-emergency-profile *profile_name*
local-emergency-num-ie
end

Notes:

- The **local-emergency-num** keyword configures the Local Emergency Numbers to be sent in Attach or TAU responses.
- *emergency_number* is a number assigned to a type of emergency number (ambulance, marine, and so on) with a string of size 1 to 10.
- *custom_number* is specific to the **custom** local emergency number . *custom_number* is an hexadecimal number from 0x1 to 0xFF
- The **no** command prefix removes the specified Local Emergency Numbers from the list. The **no** keyword also removes its following options in the **local-emergency-num-ie** configuration.
- The **local-emergency-num-ie** keyword with the **inter-mme-tau** option allows the configured local emergency number list to be sent in a TAU Accept during Inter-MME-TAUs, that is, when the UE switches from a 2G network to 3G network, from a 3G network to 4G network or from a 4G network to 4G network handover (for both idle and connected mode).
- The **local-emergency-num-ie** keyword with the **tau** option allows the configured local emergency number list to be sent in a TAU Accept message during all TAUs (for example, periodic TAUs and so on).

Verifying the Local Emergency Numbers List IE Configuration

The following sections describe commands available to verify Local Emergency Numbers List IE on the MME.

show lte-policy lte-emergency-profile summary

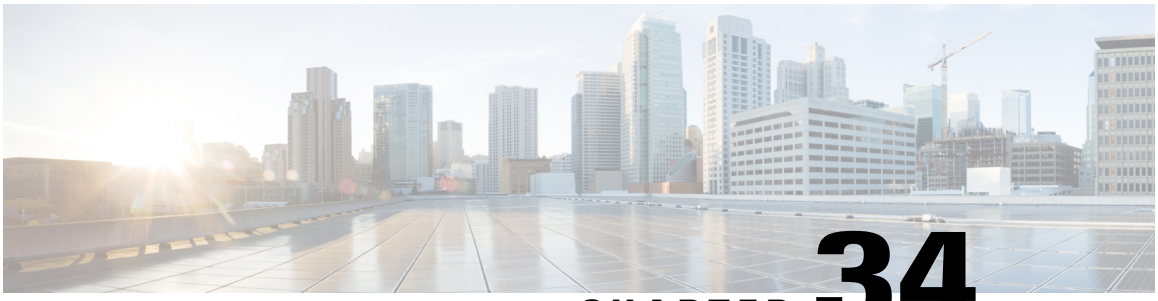
On executing this command the following fields are displayed for this feature:

```
Lte Emergency Profile emergency-prof1
Lte Emergency Profile emergency-prof2
show lte-policy lte-emergency-profile name <profile_name>
```

show lte-policy lte-emergency-profile name

On executing this command the following fields are displayed for this feature:

```
local-emergency-num  123  fire
local-emergency-num  112  police
local-emergency-num  110  ambulance
local-emergency-num  118  custom 0x1f
local-emergency-num-ie inter-mme-tau
```



CHAPTER 34

Location Services

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.

Location Services - Feature Description

The Location Services (LCS) feature enables the EPC MME and the GPRS/UMTS SGSN to use the SLg (MME) or Lg (SGSN) interface which provides the mechanisms to support specialized mobile location services for operators, subscribers, and third party service providers. Use of this feature and the SLg/Lg interface is license controlled.

The location information is reported in standard geographical co-ordinates (longitude and latitude) together with the time-of-day and the estimated errors (uncertainty) of the location of the UE. For external use, the location information may be requested by and reported to a client application associated with the UE, or a client within or attached to the core network. For internal use, the location information can be utilized by the SGSN for functions such as location assisted handover or to support other features.

Location information is intended to be used for

- location-based charging (e.g., home-location billing, roaming-location billing),
- location-based services (e.g., lawful interception, emergency calls),
- positioning services offered to the subscribers (e.g., mobile yellow pages, navigation applications on mobiles), and
- by the operator for service provider services such as network planning and enhanced call routing.

How Location Services Works

The MME LCS responsibilities are to manage LCS positioning requests. The LCS functions of the MME are related to LCS co-ordination, location requests, and operation of the LCS services.

The operation begins with a LCS Client requesting location information for a UE from the LCS server. The LCS server will pass the request to the MME in the core network. The MME in the core network then:

1. verifies that the LCS Client is authorized to request the location of the UE or subscriber
2. verifies that location services are supported by the UE
3. establishes whether it (the MME) is allowed to locate the UE or subscriber, for privacy or other reasons
4. requests the access network (via S1 interface) to provide location information for an identified UE, with indicated QoS
5. receives information about the location of the UE from the Access Network and forward it to the Client

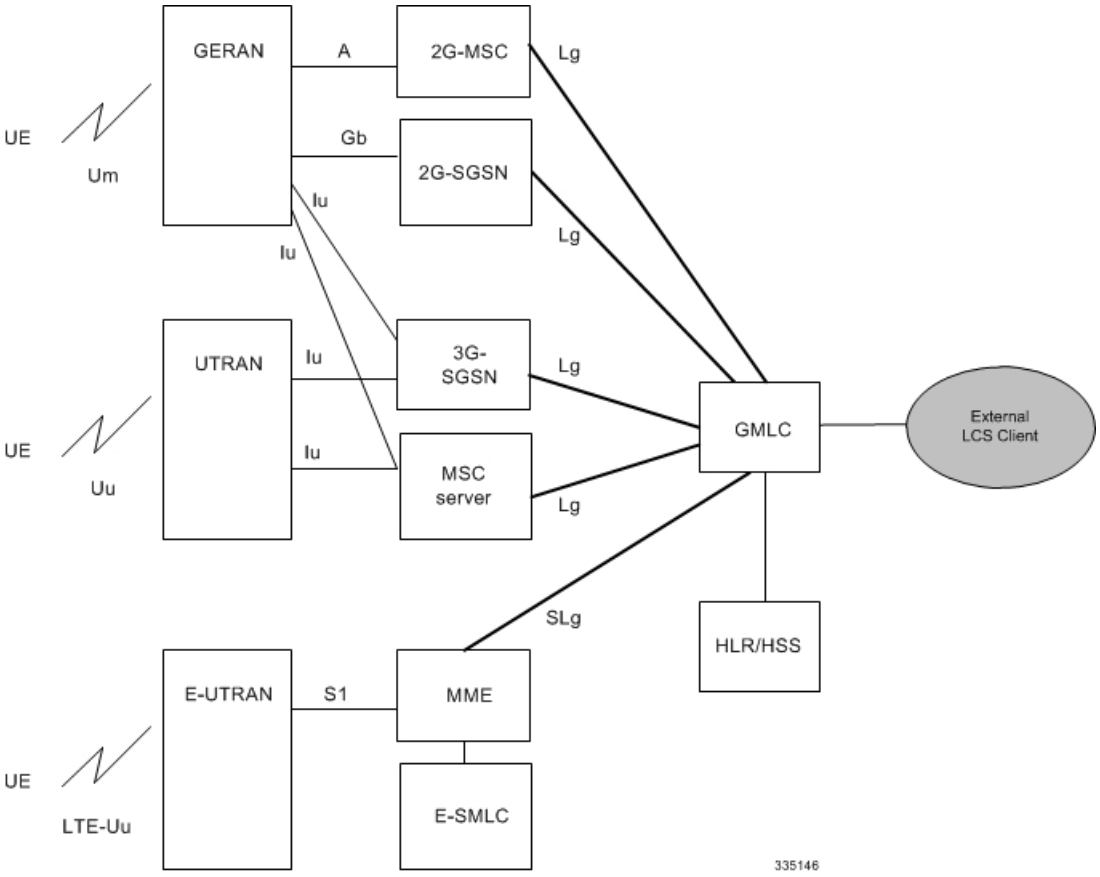
Architecture

The MME is accessible to the Gateway Mobile Location Center (GMLC) via the SLg interface.

The MME is accessible to the Evolved Serving Mobile Location Center (E-SMLC) via the SLs interface.

The SGSN is accessible to the GMLC via the Lg interface.

Figure 19: LCS Architecture



The MME informs the HLR/HSS about a UE's location services capabilities for an EPC network.

Supported Functionality

Development of MME support for LCS functions continues. The following lists the LCF functions that have been added, in the order they have been added:

- Immediate Mobile-Terminating Location Requests (MT-LI) [TS 3GPP 23.271].
- MT-LR procedures from the GMLC with client types of: Emergency Services, Value Added Services, PLMN Operator Services, and Lawful Intercept Services.
- Network Induced (NI-LR) procedures for Emergency PDN Connect and Emergency Attach, and Inbound relocation with emergency PDN (through TAU or SRNS).
- Circuit Switch Fallback (CSFB): When a UE is combined attached to the MME, and the CSFB registration is not for SMS-only services, the MME shall page UE on receipt of an SGs page with LCS Client identity.
- From Release 16.1 onwards, MME supports SLs interface: This 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 tunneling 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 3GPP TS 29.171 for more information.

- Supports UE signaling procedures for LCS. Refer to 3GPP TS 23.271 for more details.
- Supports UE and eNodeB signaling for LTE Positioning Protocol (LPP) and LTE Positioning Protocol A (LPPa). Refer to 3GPP TS 36.355 and 36.455 for more details.
- From Release 17.3.2 onwards, the MME supports sending the EMERGENCY_CALL_RELEASE event in a subscriber location report (SLR) request message, to the GMLC to notify the GMLC of the call release, when an emergency call is released or when an emergency PDN is disconnected at the MME. 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. Refer to 3GPP TS 29.172 for more information.
- From Release 17.4 onwards, the MME supports sending the EMERGENCY_CALL_HANDOVER event, in a Subscriber Location Report (SLR) request message, to the configured GMLC, to notify the GMLC of the handover when an emergency call does an outbound handover from the MME. The SLR, sent when the outbound handover procedure completes, includes the UE Identity (UE's MSISDN, IMSI, and IMEI), the target service node ID (either MSC ID for SRVCC HO or SGSN ID for GnGp HO) if available, and the event type as handover. This ensures that the GMLC is aware that the subscriber has moved from the source MME and ensures location continuity for IMS emergency calls during SRVCC (PS to CS) handovers. For location continuity during SRVCC handover, the MME supports including the MSC ID in the target service node ID. However, since the MME does not have the expected target service node ID (MSC ID), the MSC ID must be mapped to the serving MSC IP-address information (part of the MME Service configuration) to derive the needed ISDN number (see *Map the MSC ID* in the Configuration section). The MME also includes the MSC identity in the target service node IE (per TS 29.172) as part of the Provide Subscriber Location Response (PSL), if an MT-LR procedure was in progress during SRVCC handover of an emergency call.

DSCP Marking for SLs Interface

SLs interface allows Differentiated Services Code Point (DSCP) marking functionality. DSCP marking helps in packet traffic management. DSCP marking can be performed on both IPv4 and IPv6 packets leaving the SLs interface.

Either the pre-defined DSCP values can be used for marking, or any arbitrary value ranging from 0x01 to 0x3F can be assigned. The default DSCP value is 0x00 or be (Best Effort). The default DSCP value is automatically set when the configuration is disabled.

config
context *context_name*
sls-service *service_name*
[no] ip qos-dscp *dscp_value*
end

- ip defines the Internet Protocol parameters for the packets leaving through the SLs interface.
- qos-dscp designates the Quality of Service - Differentiated Services Code Point value to the packet leaving through the SLs interface.
- *dscp_value* is a value assigned to the packet for DSCP marking. The value can be a pre-defined DSCP value or an arbitrary value ranging from 0x01 to 0x3F.

Limitations

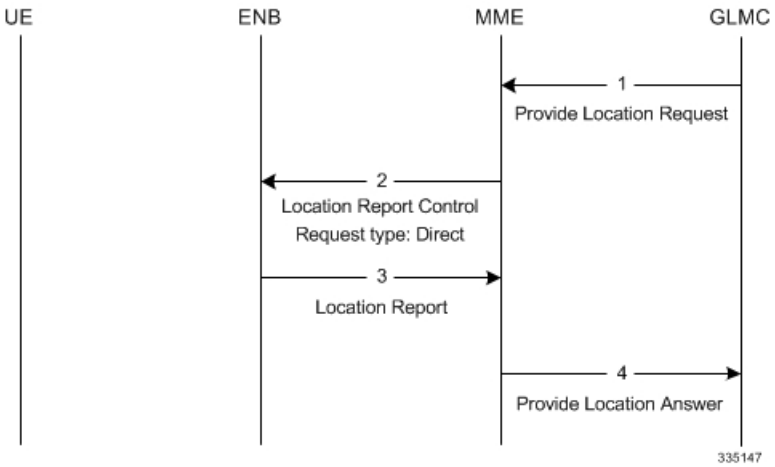
Currently, MME support is limited to:

- A single location request at a time for the target UE. Concurrent location requests are not supported.
- Location reporting granularity is at the E-UTRAN Cell Global Identifier (EGCI) level only. Note: With SLs interface support, location estimate in universal co-ordinates is supported (Refer to 3GPP TS 29.172).
- The MME does not bind all the call events for an emergency call to a specific GMLC peer. As a result, if multiple GMLC peers are configured, the call events for a single emergency call can be sent to any of the configured GMLC peers.

Flows

Mobile Terminated Location Requests

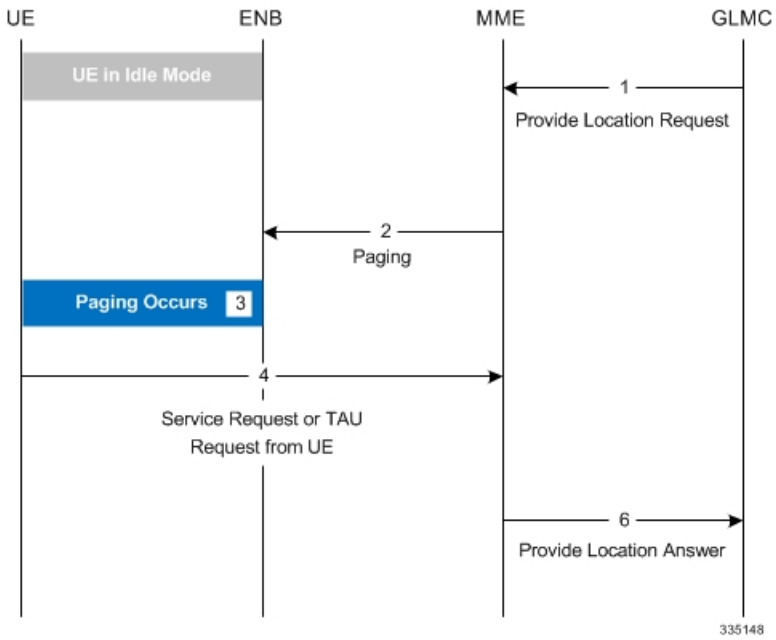
Figure 20: 4G LCS - MT-LR Call Flow - Connected Mode



1. The MME receives a Provide Location Request from the GMLC. The UE is in Connected mode.
2. The MME sends Location Report Control message with request-type as 'Direct'.
3. The eNodeB (ENB) sends the current location of the UE (ECGI) in the Location report message.

4 The MME sends Provide Location Answer to GMLC with ECGI received in the location Report Message

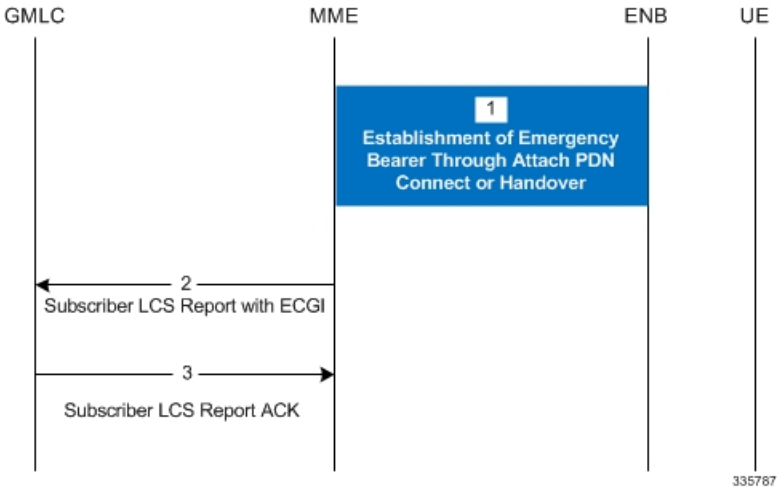
Figure 21: 4G LCS - MT-LR Call Flow - Idle Mode



1 The MME receives a Provide Location Request from the GMLC. The UE is in idle mode.
2 The MME pages the UE.
3 If the UE does not respond to the page, the MME responds with the last known location and sets the age of location report accordingly if the Location Type requested by the GMLC was "current or last known location".
4 If paging is successful, the UE responds with Service request/TAU request.
5 The MME uses the ECGI in the S1 message and sends Provide Location Answer message to the GMLC.

Network Induced Location Requests

Figure 22: 4G LCS - NI-LR Call Flow



1. The UE establishes Emergency bearers with MME. This could be a Emergency Attach or establishment of an Emergency PDN. Handover of an Emergency call from one MME to the other is also possible.
2. If the MME is configured to support Location service for emergency calls, the latest ECGI is sent in the Subscriber Location Report message to the configured GMLC.
3. The GMLC, on processing the Subscriber location report, sends the Subscriber location ACK. Note: A Negative ACK will not have any effect.

EPC Mobile Terminating Location Request (EPC-MT-LR)

Refer to 3GPP TS 23.271 v10.4.0, Section 9.1.15

EPC Network Induced Location Request (EPC-NI-LR)

Refer to 3GPP TS 23.271 v10.4.0, Section 9.1.17

EPC Post Positioning Notification and Verification Procedure

Refer to 3GPP TS 23.271 v10.4.0, Section 9.1.18

Mobile Originating Location Request, EPC (EPC-MO-LR)

Refer to 3GPP TS 23.271 v10.4.0, Section 9.2.6

UE Assisted and UE Based Positioning and Assistance Delivery

Refer to 3GPP TS 23.271 v10.4.0, Section 9.3a.1

Network Assisted and Network Based Positioning Procedure

Refer to 3GPP TS 23.271 v10.4.0, Section 9.3a.2

Obtaining Non-UE Associated Network Assistance Data

Refer to 3GPP TS 23.271 v10.4.0, Section 9.3a.3

Handover of an IMS Emergency Call

Refer to 3GPP TS 23.271 v10.4.0, Section 9.4.5.4 with the following provision: The MSC ID (expected target serving node ID) is not known to the MME so the MSC ID must be mapped (using CLI configuration, see *Map the MSC ID* in the *Configuration* section) to derive the ISDN number that is sent to the GMLC to support location continuity of SRVCC handover. This support added in 17.4.

Standards Compliance

The Location Services feature complies with the following standards:

- TS 3GPP 23.271, v10.4.0
- TS 3GPP 23.272, v10.9.0
- TS 3GPP 24.080, v10.0.0
- TS 3GPP 24.171, v9.0.0
- TS 3GPP 29.172, v10.1.0

Configuring Location Services (LCS)

This section provides a high-level series of steps and the associated configuration examples to configure Location Services on the MME.

The commands could be issued in a different order, but we recommend that you follow the outlined order for an initial LCS configuration. All listed configuration steps are mandatory unless otherwise indicated.

Important For all the required configuration commands to be available and to implement the configuration, the MME must have loaded the license for the Lg interface.

Step 1 Create a location service configuration on the MME.

Step 2 Associate the location service with the appropriate Diameter endpoint (origin host - MME and destination host - GMLC) for SLg interface .

Step 3 Associate the MME service with this location service.

Step 4 Associate the LTE Emergency Policy with this location service.

Step 5 Map the MSC ID and the MSC's IP-address.

Step 6 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide*.

Step 7 Verify the configuration for each component by following the instructions provided in the *Verifying the Feature Configuration* section.

Creating and Configuring a Location Service

In this section, configure the endpoints for the origin (the MME) and the destination host (the GMLC). A location service must be created within a context. Up to 16 separate location services can be created.

Important The origin host (the MME) configured in the endpoint for SLg interface must match the origin host configured in the endpoint for S6a interface.

```
config
    context context_name -noconfirm
        location-service location_svc_name -noconfirm
            associate diameter endpoint endpoint
            end
```

Notes:

- This series of commands creates a Location Service and associates the service with a diameter endpoint for the SLg interface.
- If multiple GMLC peers are configured, the call events for a single emergency call can be sent to any of the configured GMLC peers. If there are concerns about sending reports to different GMLCs, then configure only one peer GMLC as the SLg endpoint.

Associate the MME Service with the Location Service

Once the location service is created and configured, the MME service must be associated with it. The steps below assume the MME service has already been created.

config
context *context_name* **-noconfirm**
mme-service *mme_svc_name*
associate location-service *location_svc_name*
end

Notes:

- This series of commands associates an MME service with the new location service.

Associate the LTE Emergency Profile with the Location Service

Once the location service is created and configured, the LTE Emergency Profile must be associated with it. The steps below assume the LTE Emergency Profile has already been created.

This procedure enables the MME to provide location information of an emergency call to the GMLC.

config
lte-policy
lte-emergency-profile *profile_name*
associate location-service *location_svc_name*
end

Notes:

- This series of commands associates the LTE Emergency Profile with the new location service.

Map the MSC ID

This configuration creates a mapping between the MSC ISDN number and the MSC's IP-address (either IPv4 or IPv6) to ensure location continuity for SRVCC handover. This mapping is required to include the MSV ID in the target service node IE for the Emergency_Call_Handover event.

configure
context *context_name*
mme-service *service_name*
msc-mapping ip-address { *IPv4_address* **|** *IPv6_address* **} isdn** *isdn_number*
no msc-mapping ip-address { *IPv4_address* **|** *IPv6_address* **}**
end

Notes:

- The MSC IP address, key part of the mapping definition, is used to identify a specific mapping definition.
- *isdn_number*: Enter a numeric string upto 15 digits long.
- no msc-mapping ip-address: Identifies a specific MSC IP address mapping definition to remove from the MME Service configuration.
- MME Service supports a maximum of 24 MSC mappings.

- Use the show mme-service command to view configured mapping. the following is a sample of what the MSC mapping information would look like:

```
MSC IP-Address and ISDN Mapping
192.168.61.2          :     123456789012345
192.168.61.3          :     123456789012346
```

Verifying the LCS Configuration

The following command displays configuration information for all Location services configured on the MME.

show location-service service all
The following command displays the location service to which each MME service is associated.

show mme-service all
The following command displays the location service to which the specified LTE Emergency Profile is associated.

show lte-policy lte-emergency-profile *profile_name*
The following command displays a list of all services configured on the system, including location services (listed as Type: lcs).

show services all

Monitoring Location Services (LCS)

This section lists the bulk statistics and show commands that display operational statistics relating to Location services.

LCS Bulk Statistics

LCS service related bulk statistics are provided within the **LCS** schema.

Use the following command to display a list of all variables available within this schema:

show bulkstats variables lcs
For more information about these statistics, refer to the **LCS Schema** chapter of the *Statistics and Counters Reference*.

LCS Show Commands

The following command displays statistics for all LCS activity on the MME.

show location-service statistics all
Use the following command to clear the LCS statistics for a specific Location service.

clear location-service statistics service *location_svc_name*
The following command displays LCS statistics for a specific MME service.

show mme-service statistics service mme-service *mme_svc_name*
Use the following command to clear MME service statistics for a specific MME service.

clear mme-service statistics mme-service *mme_svc_name*

Event Logging

Event logging for the LCS (SLg interface) can be enabled using the following command:

logging filter active facility location-service level *severity_level*
Refer to the *System Logs* chapter of the *System Administration Guide* for more information about event logging.

Configuring the SLs Interface

Creating and Configuring the SLs Service

An SLs service must be created within a context. This service provides an interface from the MME to one or more E-SMLCs.

config
context *context_name* **-noconfirm**
sls-service *sls_svc_name* **-noconfirm**
bind ipv4-address *ipv4_address_value1* **ipv4-address** *ipv4_address_value2* **port** *sctp_port_num* **sctp-template** *sctp_param_template_name*
esmlc esmlc-id *esmlc_id_value* **ipv4-address** *ipv4_address_value1* **port** *sctp_port_num* **weight** *weight*
t-3x01 low-delay *seconds* **delay-tolerant** *seconds*
t-3x02 *seconds*
max-retransmissions reset *retries*
end

Notes:

- Up to 4 separate SLs services can be created on the system. The SLs service name must be unique across all contexts.
- The SLs service must be bound to at least 1 IP address. Up to 2 IPv4 or 2 IPv6 addresses can be specified for multi homing purposes. A valid SCTP Parameter Template must be defined in order for the SLs service to start. The default SCTP port is 9082.
- Up to 8 E-SMLC entries can be configured per SLs service. Up to 2 IPv4 or 2 IPv6 addresses can be specified for each E-SMLC for multi homing purposes. The MME performs a weighted round robin selection of E-SMLC based on the defined weight factor of 1 through 5, where 1 represents the least available relative capacity of the E-SMLC and 5 represents the greatest. The default SCTP port is 9082. A given E-SMLC can serve multiple SLs services on the same MME or even SLs services across separate MMEs.
- The **t-3x01** timer, **t-3x02** timer and **max-retransmission reset** command are all optional configurations.

Associating the SLs Service with the Location Service

The SLs service provides an interface to the E-SMLC for the location service. The SLs service is not a critical parameter for location services. If this association is removed, there is no impact to existing transactions and future transactions will not use the Sls service.

```
config
    context context_name -noconfirm
        location-service loc_svc_name -noconfirm
            associate sls-service sls_svc_name
            end
```

Configuring LCS QoS for Emergency Sessions

This new command defines the location service QoS settings to be used for this emergency profile.

```
config
    lte-policy
        lte-emergency-profile profile_name
            lcs-qos horizontal-accuracy variable vertical-accuracy variable
            end
```

Notes:

- Horizontal and vertical positioning accuracy values must be entered as an integer from 0 to 127, where 0 is the most accurate.
- Configuration of these settings is optional. For Emergency Services, the MME will always set the Response Time to Low Delay. If QoS is configured, the horizontal accuracy is mandatory. If a vertical accuracy is specified in this command, the MME will set the Vertical Requested flag. The LCS-Priority IE on SLs interface is always set to Highest-Priority for NI-LR call flows.

Verifying the SLs Service Configuration

The following command displays configuration information for all SLs services on the MME:

show sls-service service all
The following command displays configuration errors and warnings related to all SLs services on the MME:

show configuration errors section sls-service verbose
The following command displays to which SLs service the location service is associated:

show location-service service all
The following command displays the configured Location Service (LCS) Quality of Service (QoS) for the specified LTE emergency profile:

show lte-policy lte-emergency-profile name

Monitoring SLs Services

This section lists the SNMP traps, bulk statistics and show commands that display operational statistics relating to SLs services.

SNMP Traps

The following traps are available to track status and conditions relating to the SLs service.

- **starSLSServiceStart**: An SLS Service has started.
- **starSLSServiceStop**: An SLS Service has stopped.

The following traps are available to track status and conditions of individual E-SMLC associations.

- **starESMLCAssocDown**: An ESMLC Association is down.
- **starESMLCAssocUp**: An ESMLC Association is up. This notification is only generated for an Association which has previously been declared down.

The following traps are available to track status and conditions of all E-SMLC associations.

- **starESMLCAllAssocDown**: All the ESMLC Associations are down.
- **starESMLCAllAssocDownClear**: At least one ESMLC associations is up. This notification is only generated for all the Association which have previously been declared down.

SLs Bulk Statistics

SLs service related bulk statistics are provided within the **SLs** schema.

Use the following command to display a list of all variables available within this schema:

show bulkstats variables sls
For more information about these statistics, refer to the **SLs Schema** chapter of the *Statistics and Counters Reference*.

SLs Service Show Commands

The following command displays SLs service statistics and/or related SCTP statistics. These statistics can be filtered based on SLs service name or E-SMLC id.

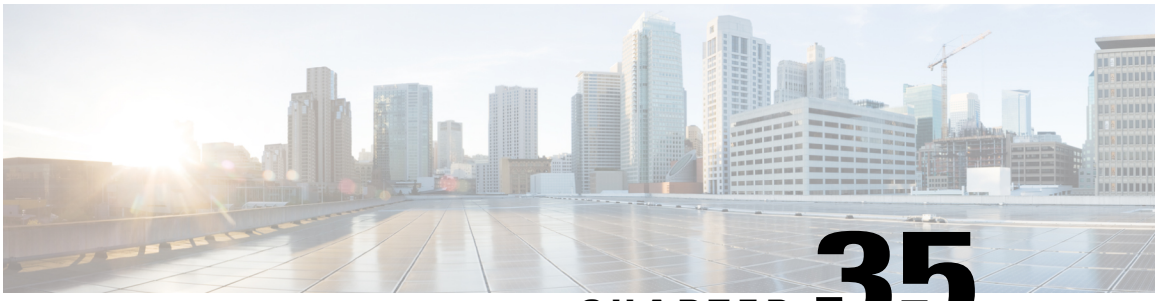
show sls-service statistics [name *svc_name* **] [sls | sctp] [esmlc-id** *esmlc-id* **]**
The following commands show the last known location of the UE that was derived using the E-SMLC.

show mme-service db record imsi
show mme-service db record guti

Event Logging

Event logging for the SLs interface can be enabled using the following command:

logging filter active facility sls level *severity_level*
Refer to the *System Logs* chapter of the *System Administration Guide* for more information about event logging.



CHAPTER 35

MBMS for MME (eMBMS)

Released as Deploy Quality in Release 20.0.

This chapter deals with the implementation of the LTE version of Multimedia Broadcast/Multicast Service (eMBMS) on the Cisco Mobility Management Entity (MME).

Feature Description

Multimedia Broadcast/Multicast Service (MBMS) is available on a number of network elements and is variously and well described on the Internet. Before looking at the implementation of eMBMS on the Cisco MME, we start with a quick overview of the 3GPP standard concepts to confirm the MME's position.

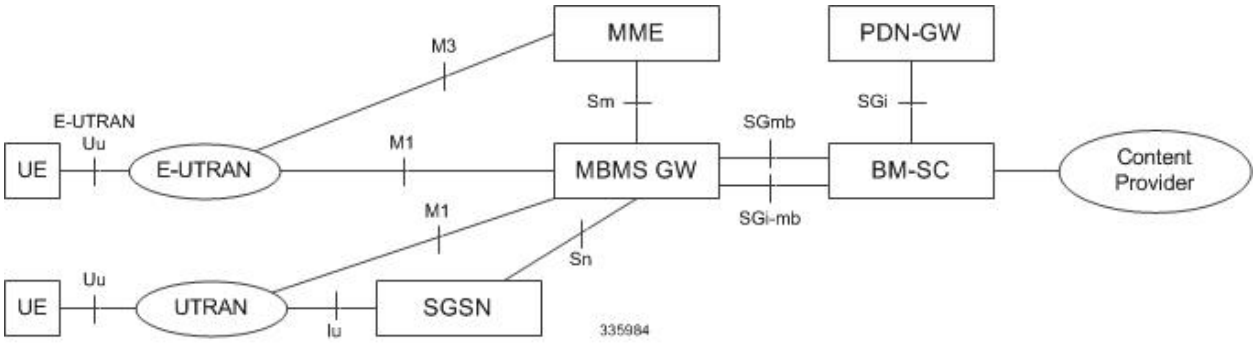
Overview per 3GPP TS 23.246

As defined by 3GPP TS 23.246:

MBMS is a point-to-multipoint service in which data is transmitted from a single source entity to multiple recipients. Transmitting the same data to multiple recipients allows network resources to be shared.

The MBMS bearer service offers two modes: Broadcast & Multicast mode. Broadcast Mode is supported for EPS and GPRS and Multicast Mode is supported for GPRS.

Figure 23: eMBMS Network Diagram



Use Cases for eMBMS on the MME

Transmitting one set of data to many, many eMBMS-capable end-users has a range of possible operator use cases:

- Mobile TV
- Digital Radio
- Video Kiosk or Video on Demand
- Connected Car
- Fixed LTE Quadruple Play
- Local Information such as Coupons
- Wireless Emergency Alerts
- Stadium App
- Data Feeds & Notifications
- e-Newspapers and e-Magazines
- Firmware/OS Updates
- Pushed Video Ads
- Last Mile CDN
- Internet of Things (Smart Meters)

MME Support for MBMS

In an LTE network, the operator using a Cisco MME can provide an MBMS data service using the e-MBMS solution proposed in 3GPP TS 23.246. eMBMS in the LTE network involves the following nodes and reference points:

- Broadcast Multicast Service Centre (BM-SC) - Supports various MBMS user-service specific services such as provisioning and delivery. The BM-SC sets up the e-MBMS session, initiates delivery of the

content by pulling it from the content server, uses appropriate CODEC on the content, and collects the reception receipt from the UEs for certain kinds of content.

- MBMS-GW - Creates the MBMS bearer and receives the user-plane MBMS traffic from the BM-SC. Once received, the MBMS-GW allocates a multicast transport address and performs the GTP-U encapsulation of the MBMS data.
- **MME** - Running the Cisco MME-eMBMS service on the MME, the MME communicates with the MBMS GW and the MCE using Sm and M3 interfaces, respectively, for all eMBMS communications and functions. MME-eMBMS facilitates sessions scheduled by the BM-SC. The MME-eMBMS service identifies service areas to be served by a particular MBMS session, so that the MME handles session start, update, and stop. The MME also handles setup and configuration requests from the MCEs.
- E-UTRAN (eNodeB/MCE) - Handles session setup and broadcasting of MBMS data on the broadcast channel on the air. The Multicell/Multicast Coordination Entity (MCE) manages the MBMS content and resources.
- M1 - Is the reference point between MBMS GW and E-UTRAN/UTRAN for MBMS data delivery. IP Multicast is used on this interface to forward data.
- M3 - Is the reference point for the control plane between MME and E-UTRAN.
- Sm - Is the reference point for the control plane between MME and MBMS-GW.
- Sn - Is the reference point between MBMS GW and SGSN (S4 based) for the control plane and for MBMS data delivery. Point-to-point mode is used on this interface to forward data.
- SGi-mb - Is the reference point between BM-SC and MBMS-GW function for MBMS data delivery.
- SGmb - Is the reference point for the control plane between BM-SC and MBMS-GW.

With MBMS functionality, the MME now supports additional interfaces :

- the Sm interface, between the MME and the MBMS-GW, receives MBMS service control messages and the IP Multicast address for MBMS data reception from the MBMS-GW. It also carries the EPS GTPv2-C messages:
  - MBMS Session Start messages
  - MBMS Session Update messages
  - MBMS Session Stop messages
- the M3 interface provides the reference point for the control plane between the MME and the MCE (E-UTRAN). The M3 Application Protocol (M3AP) supports the functions of the M3 interface by providing:
  - Support for both IPV4 and IPV6 addresses at MME endpoint.
  - Session Management - This overall functionality is responsible for starting, updating, and stopping MBMS sessions via the session control signaling on the SAE bearer level.
  - M3 Setup functionality for initial M3 interface setup for providing configuration information.
  - Reset functionality to ensure a well-defined re-initialization on the M3 interface.
  - Error Indication functionality to allow a proper error reporting.
  - MCE Configuration Update function to update the application level configuration data needed for the MCE.

Relationships

The MME-eMBMS service is not associated with the MME service or any of the other major services available on the MME, such as the SBC, SLS, or SGS services.

License Information

A valid license key for the M3 and Sm interfaces is required to enable the controlling CLI and functionality of eMBMS on the MME. Contact your Cisco Account or Support representative for information on how to obtain a license.

How It Works

MBMS Broadcast Service - the Basic Phases

Pre-requisites - the UE, MME, and eNodeB must all be eMBMS capable.

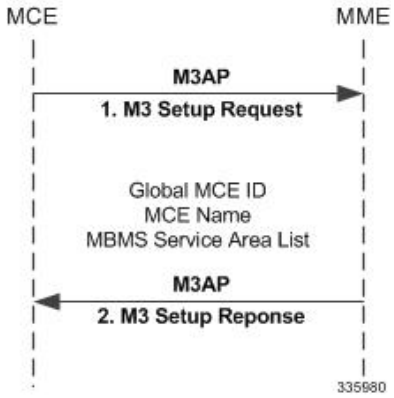
The basic phases of the MBMS broadcast service are:

1. Service Announcement - Informs UEs with media descriptions specifying the media to be delivered as part of an MBMS user service. An MBMS user service announcement can use any one of many mechanisms, for example: SMS Cell broadcast, PUSH mechanism like WAP, MMS, HTTP.
2. Session Start - The BM-SC is ready to send data. Session Start is the trigger for bearer resource establishment for MBMS data transfer.
3. MBMS Notification - Informs the UEs about forthcoming/ongoing MBMS data transfer.
4. Data Transfer - Data transferred to the UE.
5. Session Stop - BM-SC determines that there will be no more data. All the bearer resources are released at session stop.

M3 Setup Procedure

M3 Setup procedure exchanges application level data needed for the MCE and MME to correctly interoperate on the M3 interface.

Figure 24: M3 Setup Procedure

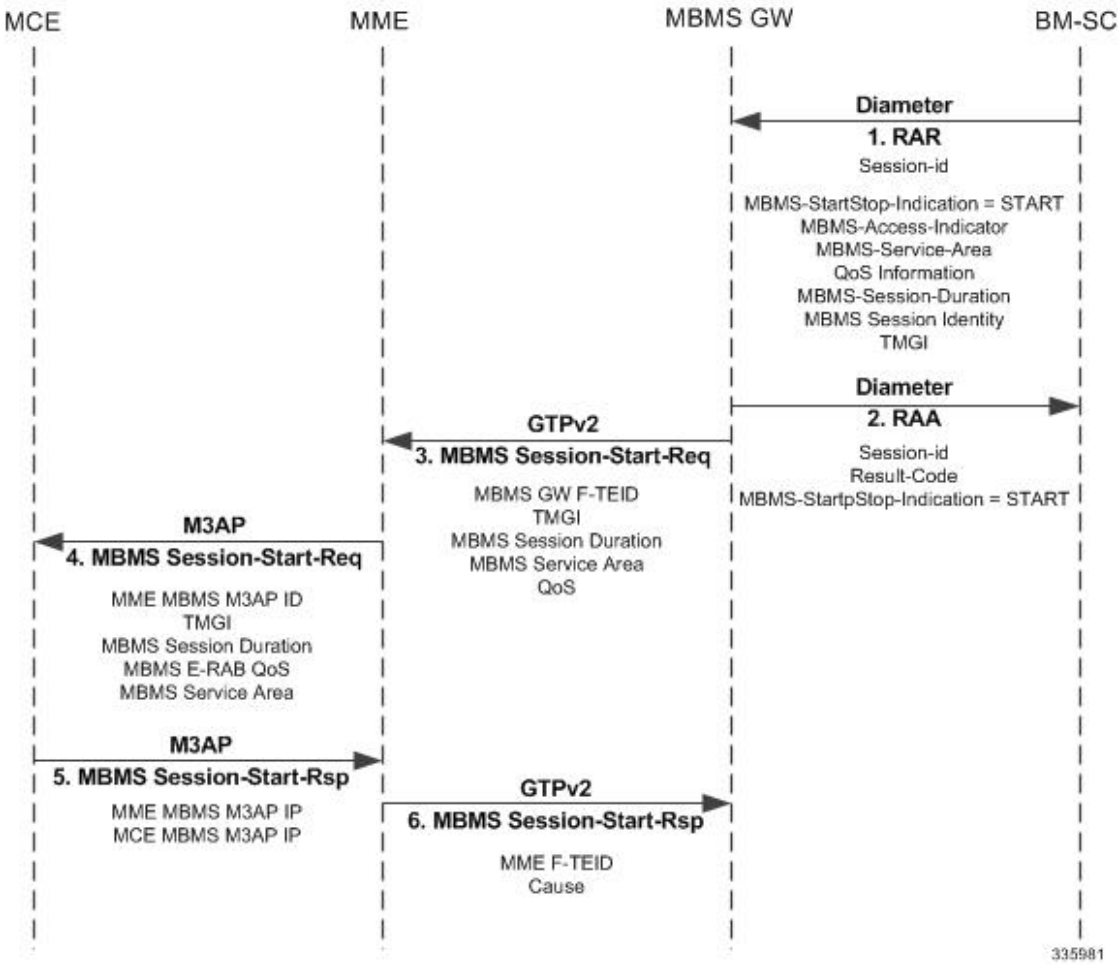


1 The MCE sends an M3 Setup Request containing the Global MCE ID, MCE Name & Service Area List.

2 The MME Responds with an M3 Setup Response.

Session Start Procedure

Figure 25: Session Start Procedure



1 The BM-SC sends an RAR (Diameter Re-Authorization Request) message to indicate start of the transmission and to provide the session attributes to the MBMS GWs. The session attributes sent includes but is not limited to: Temporary Mobile Group Identity (TMGI), Flow Identifier, quality of service (QoS), MBMS Service Area, Session Identifier, Estimated Session Duration, List of MBMS control plane nodes (MMEs, SGSNs) for MBMS-GW, access indicator.

2 The MBMS-GW creates an MBMS bearer context, stores the session attributes in the MBMS bearer context, and sends an RAA (Diameter Re-Authorization Response) message to the BM-SC.

3 The MBMS-GW sends a Session Start Request message including the session attributes to MMEs (identified from the "List of MBMS control plane nodes" attribute).

4 The MME creates an MBMS bearer context and initiates an MBMS SESSION START REQUEST message to the MCE. This also sets up the MBMS service-associated logical M3 connection with the MCE.

5 The MCE creates an MBMS bearer context, stores the session attributes and sets the state attribute of its MBMS bearer context to 'Active'. The MCE reports the result of the requested MBMS E-RAB in the MBMS SESSION START RESPONSE message.

6 The MME responds with MBMS Session Start Response to the MBMS-GW as soon as the session request is accepted by one E-UTRAN node.

In some cases, the session start procedure can involve multiple MCEs. The following briefly outlines the procedures for three possible scenarios:

Scenario 1: Some MCEs (remember, that a single Start Request can go to multiple MCEs in parallel) return failure for the Start Request:

1 The MBMS-GW sends an MBMS Session Start Request to the MME (perhaps in an MBMS Service Area served by multiple MCEs).

2 The MME sends MBMS Session Start Request to multiple MCEs simultaneously.

Some MCEs respond with MBMS Session Start Failure.

3 An MCE sends the MME an MBMS Session Start Response indicating a successful outcome.

4 The MME responds with cause "Request Accepted".

Scenario 2: All MCEs return failure for the Start Request:

1 The MBMS-GW sends an MBMS Session Start Request to the MME (perhaps in an MBMS Service Area served by multiple MCEs).

2 The MME sends MBMS Session Start Request to the MCEs

3 All MCEs respond with MBMS Session Start Failure.

4 The MME responds with failure cause "Invalid Peer".

Scenario 3: Delayed success response from some MCEs:

1 The MBMS-GW sends an MBMS Session Start Request to the MME (perhaps in an MBMS Service Area served by multiple MCEs).

2 The MME sends MBMS Session Start Request to the MCEs

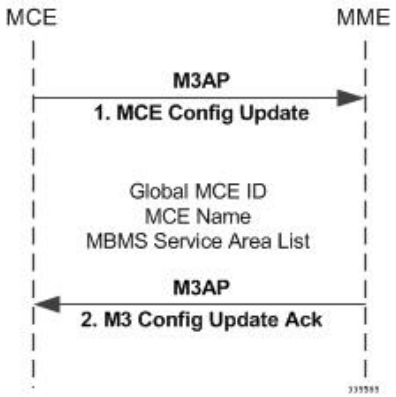
3 An MCE sends the MME an MBMS Session Start Response indicating a successful outcome.

4 The MME responds with cause "Request Accepted".

5 Further Start Session Responses will be ignored and they will not have any effect on the MBMS bearer context state.

MCE Configuration Update Procedure

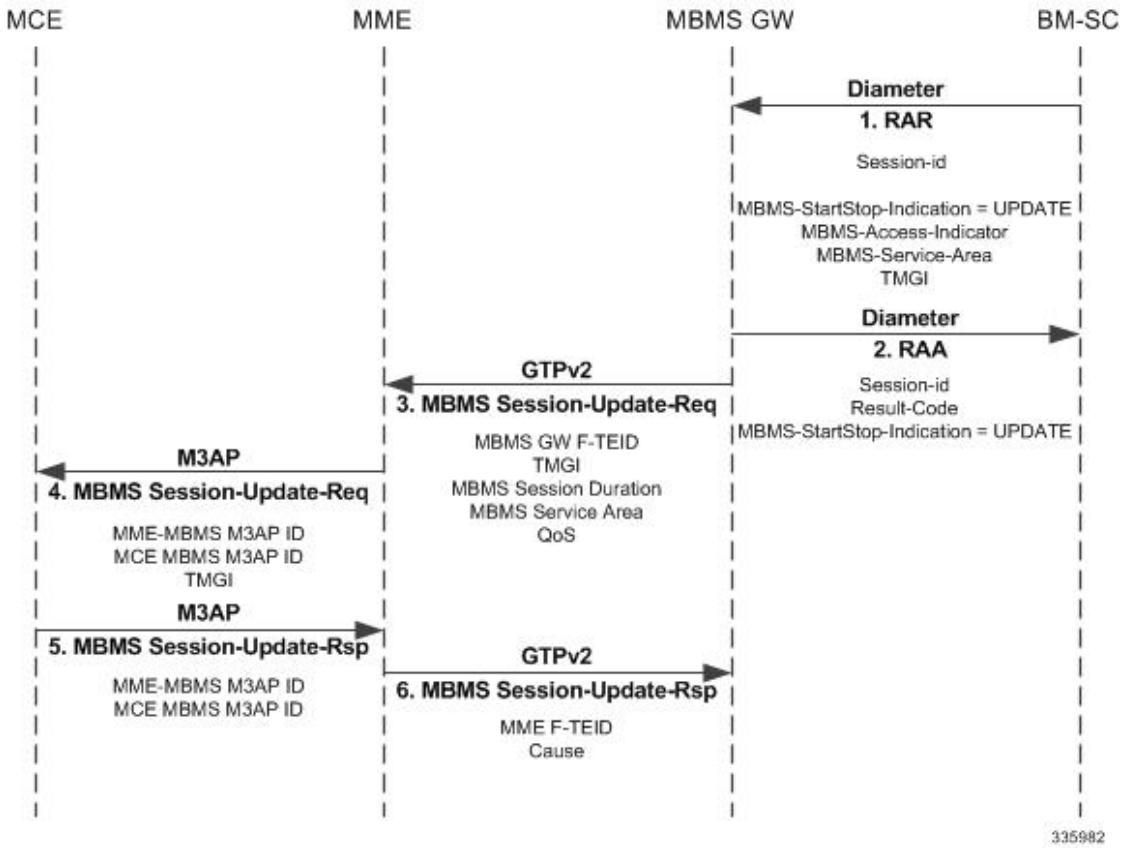
Figure 26: MCE Configuration Update



1. MCE Sends a MCE Configuration Update containing the Global MCE ID, MCE Name & Service Area List.
2. MME Responds with MCE Configuration Acknowledge.

Session Update Procedure

Figure 27: Session update Procedure

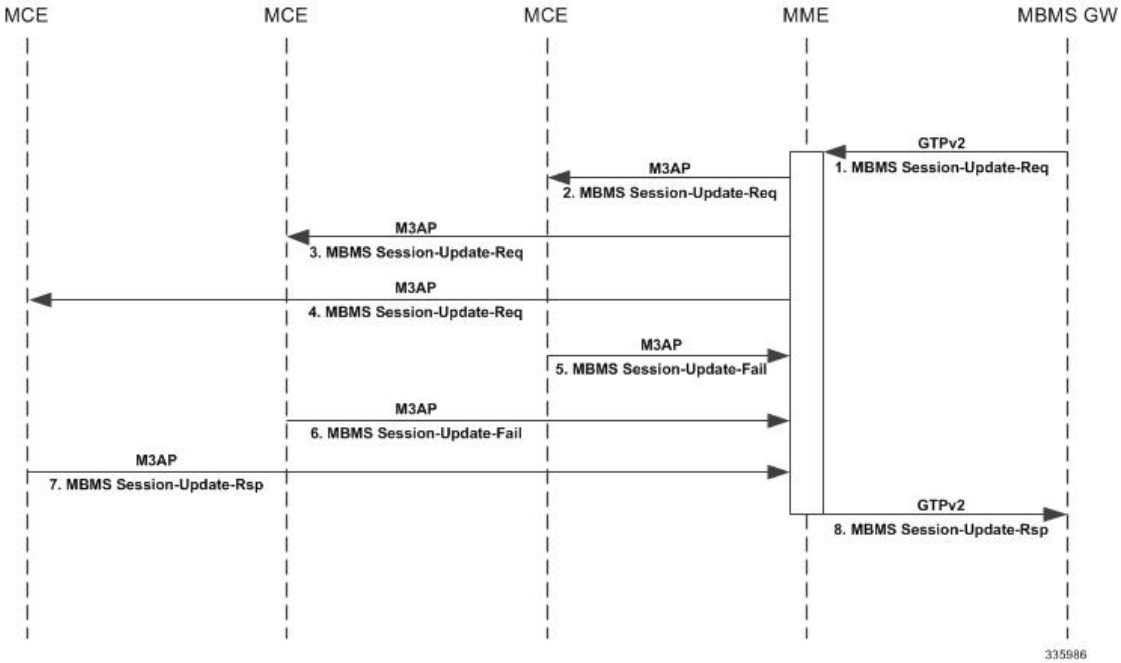


1. The BM-SC sends a RAR message to indicate that the MBMS session is updated. The attributes that can be modified by the RAR message are the MBMS Service Area, the Access indicator and the list of MBMS control plane nodes.
2. The MBMS-GW responds with a RAA message to the BM-SC.
3. The MBMS-GW initiates session start or session update procedure towards the MMEs in its list of MBMS control plane nodes.
4. The MME informs the MCEs, about changed characteristics of an ongoing MBMS service session, based on the MBMS Session Update Request. The MME sends MBMS Session Update Request to all MCEs which have earlier received an MBMS Session Start Request with the same TMGI and GLOW ID.
5. The MCE responds to the MME to confirm the reception of the Session Update Request message.
6. The MME returns a response to the MBMS-GW as soon as the Session Update Request is accepted by any E-UTRAN node.

In some cases, the session update procedure can involve multiple MCEs. The following briefly outlines the procedures for three possible scenarios:

Scenario 1: Some MCEs return failure for the Update Request:

Figure 28: Update Failure from an MCE



1 The MBMS-GW sends an MBMS Session Update Request to the MME.

2 The MME sends an MBMS Session Update Request to MCEs.

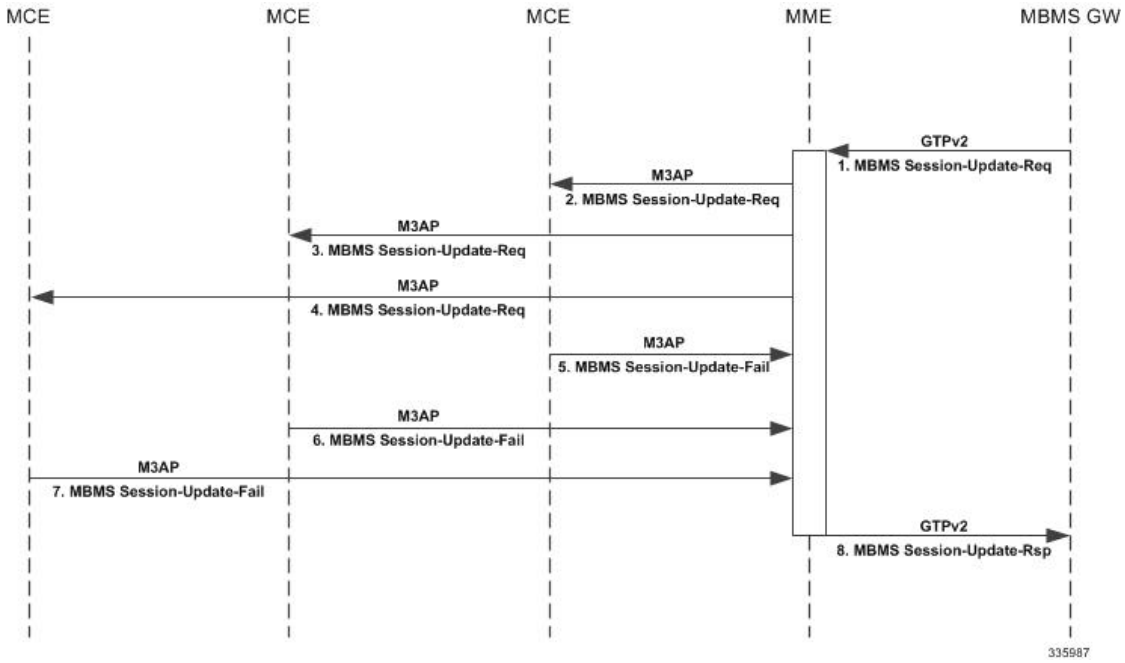
3 Some MCEs respond with MBMS Session Update Failure.

4 The MCE sends an MBMS Session Update Response indicating a successful outcome.

5 The MME responds with cause "Request Accepted"

Scenario 2: All MCEs return failure for the Update Request:

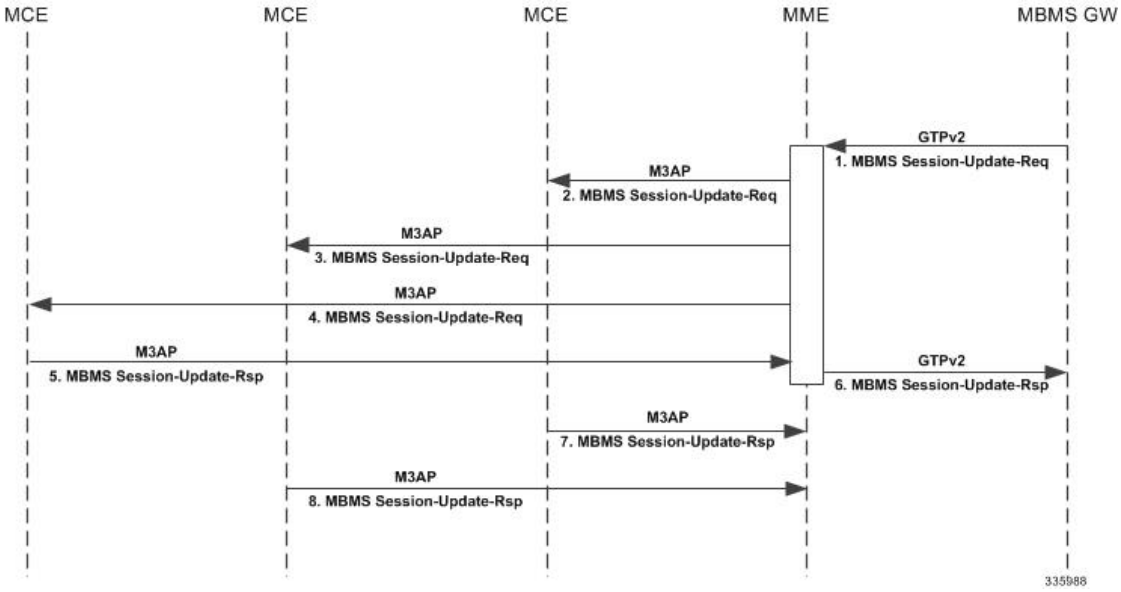
Figure 29: Update Failure from All MCEs



1. The MBMS-GW sends an MBMS Session Update Request to the MME.
2. The MME sends an MBMS Session Update Request to MCEs.
3. All MCEs respond with MBMS Session Update Failure.
4. The MME responds by sending Session Update Response with cause EGTP_CAUSE_INVALID_REPLY_FROM_REMOTE_PEER to the MBMS GW.

Scenario 3: Delayed success responses from all MCEs:

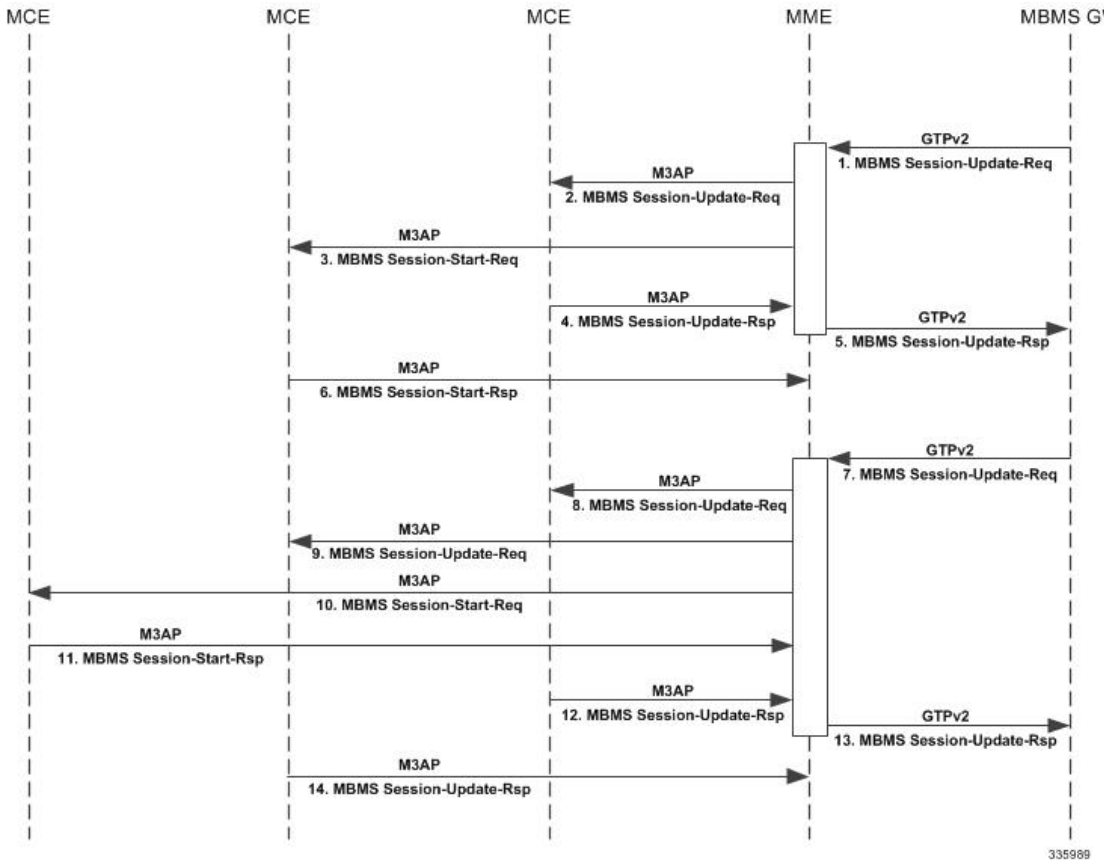
Figure 30: Delayed Update Responses



1. The MBMS-GW sends an MBMS Session Update Request to the MME.
2. The MME sends an MBMS Session Update Request to MCEs.
3. An MCE sends an MBMS Update Response indicating a successful outcome.
4. The MME responds with cause "Request Accepted"
5. Further responses are ignored and will have no effect on the MBMS bearer context state.

Scenario 4: Session update involved the additional / deletion of MBMS service areas:

Figure 31: Session Update Changing MBMS Service Areas



1. The MBMS-GW sends an MBMS Session Start Request to an MME. (For this scenario, consider that the Start Request has been sent to multiple MCEs, in this case MCE1 and MCE2.)
2. The MBMS Session Start Request is sent to MCE1.
3. The MBMS Session Start Request is sent to MCE2.
4. MCE1 responds with successful outcome.
5. The MME responds with cause "Request Accepted" without waiting for response from all MCEs.
6. MCE2 responds with successful outcome.
7. For an existing MBMS bearer context, Update Request is sent from MBMS-GW. (Let us consider there is an MBMS service area deleted and a new service area added.)
8. MME sends MBMS Session Update Request to MCE1. MCE1 has already processed MBMS Session Start Request.
9. MBMS Service Area in MCE2 is deleted in the Session Update Request. Despite this, the MME sends a Session Update Request to MCE2 with service areas received in MBMS Session Update Request from the MBMS GW over GTPv2.

10 For a new Service Area present in the Update Request, the MME sends a Session Start Request to MCE3.

11 The MCE is expected to create an MBMS bearer context and set its state attribute to "Active" and to confirm the Session Start Request.

12 As soon as the MME receives a response with successful outcome, the MME responds with cause "Request Accepted" without waiting for responses from all MCEs.

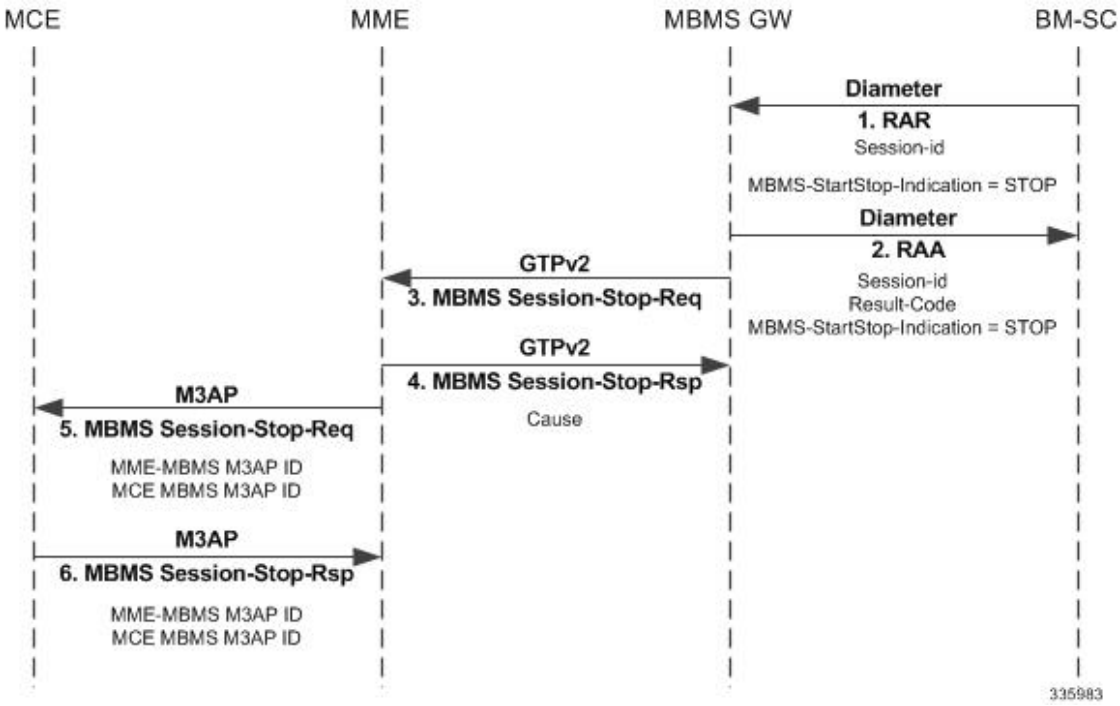
13 The MME receives a Session Update Response, indicating successful outcome, from the MCE for the Session Update Request which was sent earlier.

14 The MME sends MBMS Session Update Response with cause "Request Accepted" to the MBMS GW.

15 Responses for Update and Start Requests are sent to the MME from other MCEs.

Session Stop Procedure

Figure 32: Session Stop Procedure



1 The BM-SC sends an RAR message to indicate that the MBMS session is terminated and the bearer plane resources can be released.

2 The MBMS-GW responds with Session Stop Response and releases its information regarding the session.

3 The MBMS-GW forwards Session Stop Request message to the MME.

4 The MME releases the MBMS bearer context and responds with MBMS Session Stop Response.

5 The MME initiates MBMS Session Stop Request message to the MCE.

6 The MCE releases the MBMS bearer context associated with the logical M3 connection and responds with MBMS Session Stop Response.

Architecture - MME-eMBMS Service

A new service (mme-embms-service) supports MME's eMBMS functionality. This service is not coupled with the existing mme-service. The maximum number of MME-eMBMS services that can be created is 8. For details about the command in the configuration mode, refer to the *Configuring eMBMS* section in this document.

MCEs can be deployed with eNodeB(s) or they can be standalone. Depending on the deployment model, the number of MCEs supported can vary. Currently, the MME (system) support is limited to 300 MCEs and 100 MBMS sessions. There is no separate limit enforced on the number of MCEs per mme-embms service.

Important The MME supports a maximum total combination of eight (8) MME-specific services, of the types MME + eMBMS + SGs+ SBc + SLs -service, be configured per chassis.

Supported Features and Functions

- Sessions are identified by the combination of the TMGI and the MBMS Flow ID. In the case of no Flow ID, TMGI alone can be used to identify sessions and MBMS Flow ID would be assumed to be 0.
- Session Controller Recovery is provided to fetch MME eMBMS service configuration from the Session Manager in case of session controller failure.
- Manager Recovery support for: MMEdemux, MMEmgr, SessMgr, AAAmgr, EgtpegMgr.
- SMC switchover, PSC card migration, and slot hiding.

Standards Compliance

The Cisco implementation of eMBMS on the Cisco MME is compliant with the following standards:

- 3GPP TS 23.246, Version 12.6.0 - Multimedia Broadcast/Multicast Service (MBMS); Architecture and functional description
- TS 36.444, Version 12.2.0 - M3 Application Protocol
- TS 29.274, Version 12.8.0 - Tunnelling Protocol for Control plane (GTPv2-C)

Limitations

- MBMS flags are supported only for MBMS Session Start Request messages and not for MBMS Session Stop Request messages.
  - Re-establishment IE, which comes from MBMS-GW in Session Start Request, is forwarded to the MCEs.
  - MBMS flags are not supported in MBMS Session Stop Request messages.
- Currently, CLI limitations for the MME eMBMS feature include:
  - the **monitor protocol** command is supported, but without any of the command keywords.
  - the **monitor subscriber** command is not supported at this time for use with eMBMS.

- In the event that all MMEmgrs are restarted at the same time, then MCE Restart Handling will not perform properly.
- If the Session-Start-Response message includes an Absolute Time timestamp value (for the MBMS Data Transfer) that corresponds to a time in the past, then Session Start is rejected with cause "Mandatory IE Incorrect".

Configuring MME-eMBMS Service

Reminder: A valid M3/Sm interface license key is required to use the following commands to create an MME-eMBMS service.

The following configuration commands will setup a single MME-eMBMS Service. The commands in the MME-eMBMS service configuration mode are listed in the order in which they appear. The commands can be entered in a different order, to suit your needs.

```
configure
  context ctxt_name
    mme-embms-service mme_embms_service_name
      associate egtp-service egtp_service_name [ context ctxt_name ]
      associate sctp-param-template sctp_param_template_name
      bind { ipv4-address ipv4_address | ipv6-address ipv6_address }
      mmemgr-recovery { no-reset | reset-peers }
      plmn-id mcc mcc mnc mnc
      sctp port port_number
      setup-timeout number_seconds
```

Notes:

- The *ctxt_name* identifies the context in which the MME-eMBMS service configuration is to reside. The name must be a string of 1 through 79 alphanumeric characters.
- The *mme_embms_service_name* must be a string of 1 through 63 alphanumeric characters. We recommend that this service name be unique on the chassis. For additional information, refer to the **mme-embms-service** command description in the *Global Configuration Mode Commands* section of the *Command Line Interface Reference*.
- The **associate** command associates either a previously configured eGTP service with the MME-eMBMS service or a previously configured SCTP parameter template. The command should be repeated to associate both with the MME-eMBMS service.
  - **egtp-service** *egtp_service_name* must be a string of 1 through 63 alphanumeric characters.
  - **context** *ctxt_name* in which the eGTP service has been configured; the context name must be a string of 1 through 79 alphanumeric characters.
  - **sctp-param-template** *sctp_param_template_name* must be a string of 1 through 63 alphanumeric characters.
  - For additional information about the eGTP service or SCTP parameter template configurations, refer to the *Command Line Interface Reference*.
- The **bind** command binds the MME-eMBMS service to a logical IP interface serving as the M3 interface. Enter either a standard IPv4 or IPv6 address.

- The **mmemgr-recovery** command sets the action the MME is to take regarding the peers (MCEs) upon recovery after an MME Manager crash/failure:
  - **no-reset** - so peer associations are not reset.

    reset-peers - so peer associations are reset. *NOTE: Currently, this option is not supported.*
- The **plmn-id** command configures the PLMN identifier associated with the eMBMS service area.
- The **sctp** command configures the SCTP port number to be associated with the M3AP interface of the eMBMS service. The *port_number* is an integer from 1 to 65535 and the default is 36412.
- The **setup-timeout** command configures the number of seconds for the guard timer expiry for call setup. The *timeout_value* is an integer from 1 to 10000 and the default is 60.

Important The maximum number of MME-eMBMS services that can be created on a single chassis is 8. However, you need to note that Of the 256 possible services, the MME supports a maximum total combination of eight (8) MME-specific services, of the types MME + MME-eMBMS + SBc + SGs + SLs -service, be configured per chassis.

Verifying the MME-eMBMS Feature Configuration

Use the following command to verify your configuration:

show mme-embms-service [all | name *mme_embms_service_name* **]**

The output will provide a display similar to the following:

```
[local]asr5000# show mme-embms-service name embms1

 Service name                    : embms1
 Context                         : ingress
 Status                          : STARTED
 SCTP Bind Port                  : 36444
 MME-EMBMS IP Address            : 192.80.80.201
                                   192.80.80.202
 SCTP Param Template Associated  : sctptemp1
 Setup Timeout                   : 60
 PLMN                            : mcc 123 mnc 456
 EGTPC Service                   : egtp_mbms
```

Managing/Troubleshooting the eMBMS on the MME

Managing the eMBMS Service

The following commands can be used to manage an active eMBMS service. They are issued from the Exec mode.

- To reset MCE associations on the M3AP link by sending a RESET message to a designated MCE/eNodeB to reset all UE-associated M3 connections.

  mme-embms reset m3-peer *peer_id*

- To disconnect MCE associations on the M3AP link and perform a graceful/ungraceful disconnection of an SCTP peer (MCE) , use the following command in the Exec mode:

  mme-embms disconnect m3-peer *peer_id*

Output from "show" Commands

Numerous counters and information fields provide information helpful for monitoring and/or troubleshooting eMBMS on the MME. The following is a listing of the commands with brief information on their usefulness:

show mme-embms-service { all | { all-session-info [summary] } | { m3ap statistics { all [verbose] | name *mme_embms_service_name* **} } | { mce-association { all [summary] | full { all | name** *mme_embms_service_name* **} | name** *mme_embms_service_name* **[summary] | path-info { all | name** *mme_embms_service_name* **} } } | { mce-session-association { plmn-id mcc** *mcc* **mnc** *mnc* **mce-id** *mce_id* **| tmgi-service-id** *tmgi_service_id* **mbms-flow-id** *mbms_flow_id* **} } | name** *mme_embms_service_name* **| sctp statistics { all | name** *mme_embms_service_name* **} } }**

Notes:

- **all** -- a listing of the names of all created MME-eMBMS services and a display of the overall MBMS service status.
- **all-session-info [summary]** -- a listing of the eMBMS sessions being handled by the MMEmgr or optionally a summary of eMBMS session information.
- **m3ap statistics { all [verbose] | name** *mme_embms_service_name* **} }** -- a display of all M3AP statistics available for the MME or a display of the M3AP statistics for the named “active” MME-eMBMS service.
- **mce-association { all [summary] | full { all | name** *mme_embms_service_name* **} | name** *mme_embms_service_name* **[summary] | path-info { all | name** *mme_embms_service_name* **} } –** displays
  - all MCE peer associations for all or named MME-eMBMS service(s)
  - identifies the number of MCE associations with all or the named MME-eMBMS service(s)
  - displays path information for MCEs associated with all or the named MME-eMBMS service(s); particularly useful for checking multi-homed sessions.
- **mce-session-association { plmn-id mcc** *mcc* **mnc** *mnc* **mce-id** *mce_id* **| tmgi-service-id** *tmgi_service_id* **mbms-flow-id** *mbms_flow_id* **} –** displays
  - MCE session associations for a specific MCE
  - MCE session associations for the TMGI or TMGI and FLOW ID combination.
- **name** *mme_embms_service_name* **[summary] –** displays the configuration for the named eMBMS service.
- **sctp statistics { all | name** *mme_embms_service_name* **} –** displays SCTP statistics for all or named “active” eMBMS service(s).

show mme-embms-service m3ap statistics all [verbose]

Notes:

The command above is used to clarify status of MBMS sessions with the following counters added to the output:

- MBMS Session Start Request
- MBMS Session Start Response
- MBMS Session Start Response Failure

show mme-embms-service all-session-info [summary]

Notes:

The command above displays counters to illustrate session information maintained at all MMEMgrs.

show mme-embms-service mce-session-association tmgi-service-id *tmgi_service_id* **[mbms-flow-id** *mbms_flow_id* **]**

Notes:

The command above displays fields and counters to illustrate configured MCE associations.

show subscribers mme-embms-only [all | full]

Notes:

The command above displays MBMS subscriber information.

Disconnect Reasons

Information for system disconnects specific to eMBMS, can be found in the statistics for the following:

- disc-reason-607 = mme-embms-call-setup-timeout(607) - The number of times an eMBMS call setup has timed out.
- disc-reason-608 = mme-embms-normal-disconnect(608) - The number of times an eMBMS call has disconnected normally.
- disc-reason-609 = mme-embms-sctp-down(609) - The number of times an eMBMS call experienced an SCTP failure.

To generate the disconnect reason statistics, use the command **show session disconnect-reasons verbose** or refer to the system schema bulk statistics.

Logging Support

The following commands identify the logging support provided for the MME eMBMS Service functionality:

logging filter active facility mme-embms level {critical | error | warning | unusual | info | trace | debug }

logging filter active facility m3ap level {critical | error | warning | unusual | info | trace | debug }

Logging Events

The range of event IDs supported for eMBMS is 212001 to 212024.

The following configuration disables logging for specified event or event ranges:

configure
logging disable eventid *event_id* **[to** *event_id* **]**

The following configuration enables logging for specified event or event ranges:

configure
no logging disable eventid *event_id* **[to** *event_id* **]**

Monitor Protocol Logging

- Monitor protocol option (97-M3AP) is added to display M3AP messages.
- Monitor protocol option (74 - EGTPC) is re-used to display GTPv2 messages on Sm Interface.

Bulk Statistic Support

mme-embms is the schema that has been added to enable the MME to provide statistics specific to eMBMS on the MME. Variables included are:

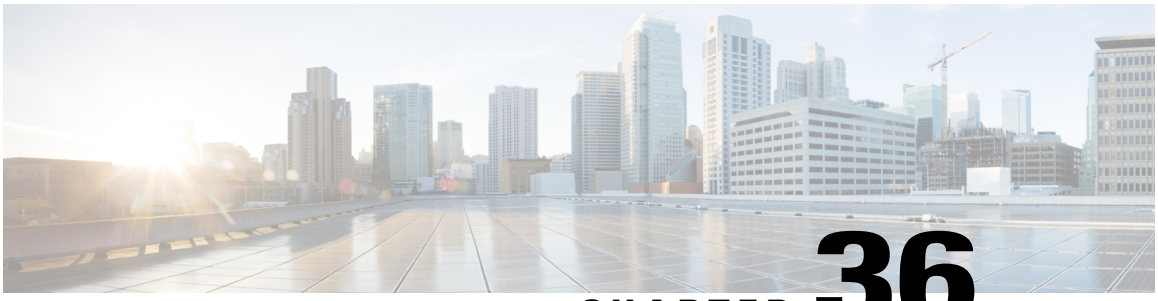
- mme-embms-m3ap-recdata-m3setup-req
- mme-embms-m3ap-recdata-mce-config-upd
- mme-embms-m3ap-recdata-mbms-sess-start-rsp
- mme-embms-m3ap-recdata-mbms-sess-start-rsp-fail
- mme-embms-m3ap-recdata-mbms-sess-upd-rsp
- mme-embms-m3ap-recdata-mbms-sess-upd-rsp-fail
- mme-embms-m3ap-recdata-mbms-sess-stop-rsp
- mme-embms-m3ap-recdata-reset
- mme-embms-m3ap-recdata-reset-ack
- mme-embms-m3ap-recdata-err-ind
- mme-embms-m3ap-transdata-m3setup-rsp
- mme-embms-m3ap-transdata-m3setup-rsp-fail
- mme-embms-m3ap-transdata-mce-config-upd-ack
- mme-embms-m3ap-transdata-mce-config-upd-ack-fail
- mme-embms-m3ap-transdata-mbms-sess-start-req
- mme-embms-m3ap-transdata-mbms-sess-upd-req
- mme-embms-m3ap-transdata-mbms-sess-stop-req
- mme-embms-m3ap-transdata-reset
- mme-embms-m3ap-transdata-reset-ack
- mme-embms-m3ap-transdata-err-ind
- mme-embms-m3ap-unknown-mme-mbms-m3ap-id
- mme-embms-m3ap-unknown-mce-mbms-m3ap-id
- mme-embms-m3ap-unknown-mbms-m3ap-id-pair
- mme-embms-m3ap-tx-syntax-err

- mme-embms-m3ap-semantic-err
- mme-embms-m3ap-msg-not-compatible
- mme-embms-m3ap-abstract-syntax-err
- mme-embms-m3ap-abstract-syntax-err-reject
- mme-embms-m3ap-abstract-syntax-err-ignore-notify
- mme-embms-m3ap-abstract-syntax-err-false-constr-msg
- mme-embms-m3ap-mce-total-active
- mme-embms-m3ap-mce-total-created
- mme-embms-m3ap-mce-total-closed
- mme-embms-m3ap-mce-total-rejected

SNMP Traps

The following identifies the traps new for the MME eMBMS feature and illustrates a sample display:

```
[local]ASR5K# show snmp trap statistics

 Trap Name                #Gen   #Disc  Disable  Last Generated
 -----------------------  -----  -----  -------  --------------------
 MMEEMBMSServiceStart       1      0      0      2015:09:08:09:14:08
 MMEEMBMSServiceStop        1      0      0      2015:09:08:09:14:03
 MCEAssocDown               1      0      0      2015:09:08:09:14:19
 MCEAssocUp                 1      0      0      2015:09:08:09:14:16
```



CHAPTER 36

Operator Policy

The proprietary concept of an operator policy, originally architected for the exclusive use of an SGSN, is non-standard and currently unique to the ASR 5x00. This optional feature empowers the carrier with flexible control to manage functions that are not typically used in all applications and to determine the granularity of the implementation of any operator policy: to groups of incoming calls or to simply one single incoming call.

The following products support the use of the operator policy feature:

- MME (Mobility Management Entity - LTE)
- SGSN (Serving GPRS Support Node - 2G/3G/LTE)
- S-GW (Serving Gateway - LTE)

This document includes the following information:

What Operator Policy Can Do

Operator policy enables the operator to specify a policy with rules governing the services, facilities and privileges available to subscribers.

A Look at Operator Policy on an S-GW

The S-GW operator policy provides mechanisms to fine tune the behavior for subsets of subscribers. It also can be used to control the behavior of visiting subscribers in roaming scenarios by enforcing roaming agreements and providing a measure of local protection against foreign subscribers.

The S-GW uses operator policy in the SGW service configuration to control the accounting mode. The default accounting mode is GTPP, but RADIUS/Diameter and none are options. The accounting mode value from the call control profile overrides the value configured in SGW service. If the accounting context is not configured in the call control profile, it is taken from SGW service. If the SGW service does not have the relevant configuration, the current context or default GTPP group is assumed.

The Operator Policy Feature in Detail

This flexible feature provides the operator with a range of control to manage the services, facilities and privileges available to subscribers.

Operator policy definitions can depend on factors such as (but not limited to):

- roaming agreements between operators,
- subscription restrictions for visiting or roaming subscribers,
- provisioning of defaults to override standard behavior.

These policies can override standard behaviors and provide mechanisms for an operator to circumvent the limitations of other infrastructure elements such as DNS servers and HLRs in 2G/3G networks.

By configuring the various components of an operator policy, the operator fine-tunes any desired restrictions or limitations needed to control call handling and this can be done for a group of callers within a defined IMSI range or per subscriber.

Re-Usable Components - Besides enhancing operator control via configuration, the operator policy feature minimizes configuration by drastically reducing the number of configuration lines needed. Operator policy maximizes configurations by breaking them into the following reusable components that can be shared across IMSI ranges or subscribers:

- call control profiles
- IMEI profiles (SGSN only)
- APN profiles
- APN remap tables
- operator policies
- IMSI ranges

Each of these components is configured via a separate configuration mode accessed through the Global Configuration mode.

Call Control Profile

A call control profile can be used by the operator to fine-tune desired functions, restrictions, requirements, and/or limitations needed for call management on a per-subscriber basis or for groups of callers across IMSI ranges. For example:

- setting access restriction cause codes for rejection messages
- enabling/disabling authentication for various functions such as attach and service requests

- enabling/disabling ciphering, encryption, and/or integrity algorithms
- enabling/disabling of packet temporary mobile subscriber identity (P-TMSI) signature allocation (SGSN only)
- enabling/disabling of zone code checking
- allocation/retention priority override behavior (SGSN only)
- enabling/disabling inter-RAT, 3G location area, and 4G tracking area handover restriction lists (MME and S-GW only)
- setting maximum bearers and PDNs per subscriber (MME and S-GW only)

Call control profiles are configured with commands in the Call Control Profile configuration mode. A single call control profile can be associated with multiple operator policies

For planning purposes, based on the system configuration, type of packet services cards, type of network (2G, 3G, 4G, LTE), and/or application configuration (single, combo, dual access), the following call control profile configuration rules should be considered:

- 1 (only one) - call control profile can be associated with an operator policy
- 1000 - maximum number of call control profiles per system (e.g., an SGSN).
- 15 - maximum number of equivalent PLMNs for 2G and 3G per call control profile
  - 15 - maximum number of equivalent PLMNs for 2G per ccprofile.
  - 15 - maximum number of supported equivalent PLMNs for 3G per ccprofile.
- 256 - maximum number of static SGSN addresses supported per PLMN
- 5 - maximum number of location area code lists supported per call control profile.
- 100 - maximum number of LACs per location area code list supported per call control profile.
- unlimited number of zone code lists can be configured per call control profile.
- 100 - maximum number of LACs allowed per zone code list per call control profile.
- 2 - maximum number of integrity algorithms for 3G per call control profile.
- 3 - maximum number of encryption algorithms for 3G per call control profile.

APN Profile

An APN profile groups a set of access point name (APN)-specific parameters that may be applicable to one or more APNs. When a subscriber requests an APN that has been identified in a selected operator policy, the parameter values configured in the associated APN profile will be applied.

For example:

- enable/disable a direct tunnel (DT) per APN. (SGSN)
- define charging characters for calls associated with a specific APN.
- identify a specific GGSN to be used for calls associated with a specific APN (SGSN).
- define various quality of service (QoS) parameters to be applied to calls associated with a specific APN.

- restrict or allow PDP context activation on the basis of access type for calls associated with a specific APN.

APN profiles are configured with commands in the APN Profile configuration mode. A single APN profile can be associated with multiple operator policies.

For planning purposes, based on the system configuration, type of packet processing cards and 2G, 3G, 4G, and/or dual access, the following APN profile configuration rules should be considered:

- 50 - maximum number of APN profiles that can be associated with an operator policy.
- 1000 - maximum number of APN profiles per system (e.g., an SGSN).
- 116 - maximum gateway addresses (GGSN addresses) that can be defined in a single APN profile.

IMEI-Profile (SGSN only)

The IMEI is a unique international mobile equipment identity number assigned by the manufacturer that is used by the network to identify valid devices. The IMEI has no relationship to the subscriber.

An IMEI profile group is a set of device-specific parameters that control SGSN behavior when one of various types of Requests is received from a UE within a specified IMEI range. These parameters control:

- Blacklisting devices
- Identifying a particular GGSN to be used for connections for specified devices
- Enabling/disabling direct tunnels to be used by devices

IMEI profiles are configured with commands in the IMEI Profile configuration mode. A single IMEI profile can be associated with multiple operator policies.

For planning purposes, based on the system configuration, type of packet processing cards, type of network (2G, 3G, 4G, LTE), and/or application configuration (single, combo, dual access), the following IMEI profile configuration rules should be considered:

- 10 - maximum number of IMEI ranges that can be associated with an operator policy.
- 1000 - maximum number of IMEI profiles per system (such as an SGSN).

APN Remap Table

APN remap tables allow an operator to override an APN specified by a user, or the APN selected during the normal APN selection procedure, as specified by 3GPP TS 23.060. This atypical level of control enables operators to deal with situations such as:

- An APN is provided in the Activation Request that does not match with any of the subscribed APNs either a different APN was entered or the APN could have been misspelled. In such situations, the SGSN would reject the Activation Request. It is possible to correct the APN, creating a valid name so that the Activation Request is not rejected.
- In some cases, an operator might want to force certain devices/users to use a specific APN. For example, all iPhone4 users may need to be directed to a specific APN. In such situations, the operator needs to be able to override the selected APN.

An APN remap table group is a set of APN-handling configurations that may be applicable to one or more subscribers. When a subscriber requests an APN that has been identified in a selected operator policy, the parameter values configured in the associated APN remap table will be applied. For example, an APN remap table allows configuration of the following:

- APN aliasing - maps incoming APN to a different APN based on partial string match (MME and SGSN) or matching charging characteristic (MME and SGSN).
- Wildcard APN - allows APN to be provided by the SGSN when wildcard subscription is present and the user has not requested an APN.
- Default APN - allows a configured default APN to be used when the requested APN cannot be used for example, the APN is not part of the HLR subscription.

APN remap tables are configured with commands in the APN Remap Table configuration mode. A single APN remap table can be associated with multiple operator policies, but an operator policy can only be associated with a single APN remap table.

For planning purposes, based on the system configuration, type of packet processing cards, type of network (2G, 3G, 4G, LTE), and/or application configuration (single, combo, dual access), the following APN remap table configuration rules should be considered:

- 1 - maximum number of APN remap tables that can be associated with an operator policy.
- 1000 - maximum number of APN remap tables per system (such as an SGSN).
- 100 - maximum remap entries per APN remap table.

Operator Policies

The 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. An operator policy binds the various configuration components together. It associates APNs, with APN profiles, with an APN remap table, with a call control profile, and/or an IMEI profile (SGSN only) and associates all the components with filtering ranges of IMSIs.

In this manner, an operator policy manages the application of rules governing the services, facilities, and privileges available to subscribers.

Operator policies are configured and the associations are defined via the commands in the Operator Policy configuration mode.

The IMSI ranges are configured with the command in the SGSN-Global configuration mode.

For planning purposes, based on the system configuration, type of packet processing cards, type of network (2G, 3G, 4G, LTE), and/or application configuration (single, combo, dual access), the following operator policy configuration rules should be considered:

- 1 maximum number of call control profiles associated with a single operator policy.
- 1 maximum number of APN remap tables associated with a single operator policy.
- 10 maximum number of IMEI profiles associated with a single operator policy (SGSN only)
- 50 maximum number of APN profiles associated with a single operator policy.
- 1000 maximum number of operator policies per system (e.g., an SGSN) this number includes the single default operator policy.

- 1000 maximum number of IMSI ranges defined per system (e.g., an SGSN).

Important SGSN operator policy configurations created with software releases prior to Release 11.0 are not forward compatible. Such configurations can be converted to enable them to work with an SGSN running Release 11.0 or higher. Your Cisco Account Representative can accomplish this conversion for you.

IMSI Ranges

Ranges of international mobile subscriber identity (IMSI) numbers, the unique number identifying a subscriber, are associated with the operator policies and used as the initial filter to determine whether or not any operator policy would be applied to a call. The range configurations are defined by the MNC, MCC, a range of MSINs, and optionally the PLMN ID. The IMSI ranges must be associated with a specific operator policy.

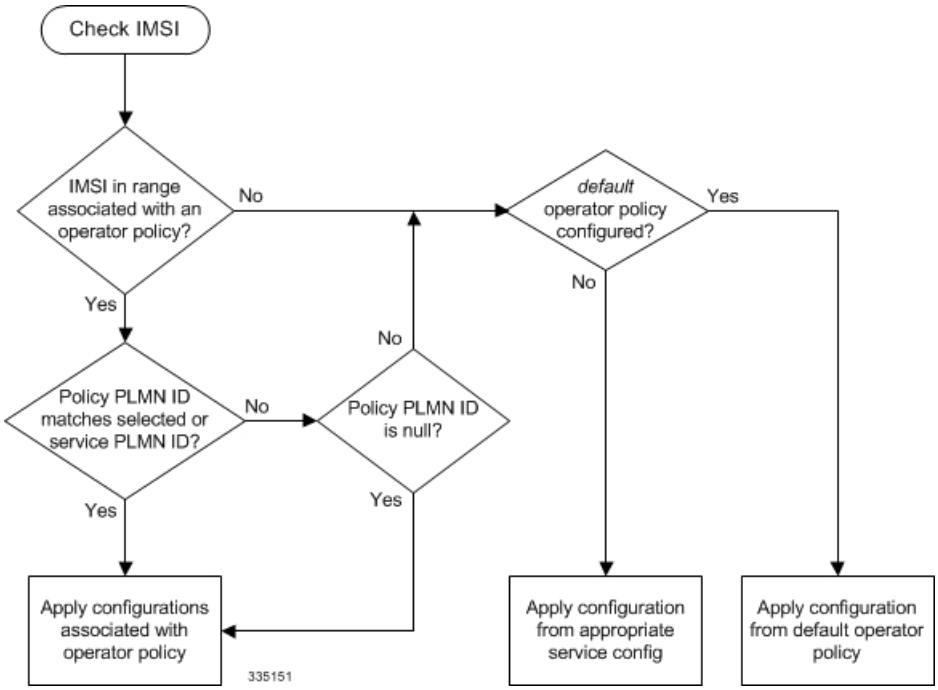
IMSI ranges are defined differently for each product supporting the operator policy feature.

How It Works

The specific operator policy is selected on the basis of the subscriber's IMSI at attach time, and optionally the PLMN ID selected by the subscriber or the RAN node's PLMN ID. Unique, non-overlapping, IMSI + PLMN-ID ranges create call filters that distinguish among the configured operator policies.

The following flowchart maps out the logic applied for the selection of an operator policy:

Figure 33: Operator Policy Selection Logic



Operator Policy Configuration

This section provides a high-level series of steps and the associated configuration examples to configure an operator policy. By configuring an operator policy, the operator fine-tunes any desired restrictions or limitations needed to control call handling per subscriber or for a group of callers within a defined IMSI range.

Most of the operator policy configuration components are common across the range of products supporting operator policy. Differences will be noted as they are encountered below.

Important After creating or modifying the S4-SGSN's configuration, you must save the configuration and reboot the node for the change(s) to take effect.

Important This section provides a minimum instruction set to implement operator policy. For this feature to be operational, you must first have completed the system-level configuration as described in the *System Administration Guide* and the service configuration described in your product's administration guide.

The components can be configured in any order. This example begins with the call control profile:

Step 1 Create and configure a call control profile, by applying the example configuration presented in the Call Control Profile Configuration section.

Step 2 Create and configure an APN profile, by applying the example configuration presented in the APN Profile Configuration section.

Note It is not necessary to configure both an APN profile and an IMEI profile. You can associate either type of profile with a policy. It is also possible to associate one or more APN profiles with an IMEI profile for an operator policy (SGSN only).

Step 3 Create and configure an IMEI profile by applying the example configuration presented in the *IMEI Profile Configuration* section (SGSN only).

Step 4 Create and configure an APN remap table by applying the example configuration presented in the *APN Remap Table Configuration* section.

Step 5 Create and configure an operator policy by applying the example configuration presented in the *Operator Policy Configuration* section.

Step 6 Configure an IMSI range by selecting and applying the appropriate product-specific example configuration presented in the *IMSI Range Configuration* sections below.

Step 7 Associate the configured operator policy components with each other and a network service by applying the example configuration in the *Operator Policy Component Associations* section.

Step 8 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* .

Step 9 Verify the configuration for each component separately by following the instructions provided in the *Verifying the Feature Configuration* section of this chapter.

Call Control Profile Configuration

This section provides the configuration example to create a call control profile and enter the configuration mode.

Use the call control profile commands to define call handling rules that will be applied via an operator policy. Only one call control profile can be associated with an operator policy, so it is necessary to use (and repeat as necessary) the range of commands in this mode to ensure call-handling is sufficiently managed.

Configuring the Call Control Profile for an SGSN

The example below includes some of the more commonly configured call control profile parameters with sample variables that you will replace with your own values.

```
configure
    call-control-profile profile_name>
        attach allow access-type umts location-area-list instance list_id
        authenticate attach
        location-area-list instance instance area-code area_code
        sgsn-number E164_number
        end
```

Notes:

- Refer to the *Call Control Profile Configuration Mode* chapter in the *Command Line Interface Reference* for command details and variable options.
- This profile will only become valid when it is associated with an operator policy.

Configuring the Call Control Profile for an MME or S-GW

The example below includes some of the more commonly configured call control profile parameters with sample variables that you will replace with your own values.

```
configure
     call-control-profile profile_name
        associate hss-peer-service service_name s6a-interface
        attach imei-query-type imei verify-equipment-identity
        authenticate attach
        dns-pgw context mme_context_name
        dns-sgw context mme_context_name
        end
```

Notes:

- Refer to the *Call Control Profile Configuration Mode* chapter in the *Command Line Interface Reference* for command details and variable options.
- This profile will only become valid when it is associated with an operator policy.

APN Profile Configuration

This section provides the configuration example to create an APN profile and enter the apn-profile configuration mode.

Use the **apn-profile** commands to define how calls are to be handled when the requests include an APN. More than one APN profile can be associated with an operator policy.

The example below includes some of the more commonly configured profile parameters with sample variables that you will replace with your own values.

```
configure
   apn-profile profile_name
      gateway-address 123.123.123.1 priority 1 (SGSN only)
      direct-tunnel not-permitted-by-ggsn (SGSN only)
      idle-mode-acl ipv4 access-group station7 (S-GW only)
      end
```

Notes:

- All of the parameter defining commands in this mode are product-specific. Refer to the *APN Profile Configuration Mode* chapter in the *Command Line Interface Reference* for command details and variable options.
- This profile will only become valid when it is associated with an operator policy.

IMEI Profile Configuration - SGSN only

This section provides the configuration example to create an IMEI profile and enter the imei-profile configuration mode.

Use the **imei-profile** commands to define how calls are to be handled when the requests include an IMEI in the defined IMEI range. More than one IMEI profile can be associated with an operator policy.

The example below includes some of the more commonly configured profile parameters with sample variables that you will replace with your own values.

```
configure
   imei-profile profile_name
      ggsn-address 211.211.123.3
      direct-tunnel not-permitted-by-ggsn (SGSN only)
      associate apn-remap-table remap1
      end
```

Notes:

- It is optional to configure an IMEI profile. An operator policy can include IMEI profiles and/or APN profiles.
- This profile will only become valid when it is associated with an operator policy.

APN Remap Table Configuration

This section provides the configuration example to create an APN remap table and enter the apn-remap-table configuration mode.

Use the **apn-remap-table** commands to define how APNs are to be handled when the requests either do or do not include an APN.

The example below includes some of the more commonly configured profile parameters with sample variables that you will replace with your own values.

configure
apn-remap-table *table_name*
apn-selection-default first-in-subscription
wildcard-apn pdp-type ipv4 network-identifier *apn_net_id*
blank-apn network-identifier *apn_net_id* `(SGSN only)`
end

Notes:

- The **apn-selection-default first-in-subscription** command is used for APN redirection to provide "guaranteed connection" in instances where the UE-requested APN does not match the default APN or is missing completely. In this example, the first APN matching the PDP type in the subscription is used. The first-in-selection keyword is an MME feature only.
- Some of the commands represented in the example above are common and some are product-specific. Refer to the *APN-Remap-Table Configuration Mode* chapter in the *Command Line Interface Reference* for command details and variable options.
- This profile will only become valid when it is associated with an operator policy.

Operator Policy Configuration

This section provides the configuration example to create an operator policy and enter the operator policy configuration mode.

Use the commands in this mode to associate profiles with the policy, to define and associate APNs with the policy, and to define and associate IMEI ranges. Note: IMEI ranges are supported for SGSN only.

The example below includes sample variable that you will replace with your own values.

configure
operator-policy *policy_name*
associate call-control-profile *profile_name*
apn network-identifier *apn-net-id_1* **apn-profile** *apn_profile_name_1*
apn network-identifier *apn-net-id_2* **apn-profile** *apn_profile_name_1*
imei range <*imei_number* **to** *imei_number* **imei-profile name** *profile_name*
associate apn-remap-table *table_name*
end

Notes:

- Refer to the *Operator-Policy Configuration Mode* chapter in the *Command Line Interface Reference* for command details and variable options.
- This policy will only become valid when it is associated with one or more IMSI ranges (SGSN) or subscriber maps (MME and S-GW).

IMSI Range Configuration

This section provides IMSI range configuration examples for each of the products that support operator policy functionality.

Configuring IMSI Ranges on the MME or S-GW

IMSI ranges on an MME or S-GW are configured in the Subscriber Map Configuration Mode. Use the following example to configure IMSI ranges on an MME or S-GW:

configure
subscriber-map *name*
lte-policy
precedence *number* **match-criteria imsi mcc** *mcc_number* **mnc** *mnc_number* **msin first** *start_range* **last** *end_range* **operator-policy-name** *policy_name*
end

Notes:

- The precedence number specifies the order in which the subscriber map is used. 1 has the highest precedence.
- The operator policy name identifies the operator policy that will be used for subscribers that match the IMSI criteria and fall into the MSIN range.

Associating Operator Policy Components on the MME

After configuring the various components of an operator policy, each component must be associated with the other components and, ultimately, with a network service.

The MME service associates itself with a subscriber map. From the subscriber map, which also contains the IMSI ranges, operator policies are accessed. From the operator policy, APN remap tables and call control profiles are accessed.

Use the following example to configure operator policy component associations:

configure
operator-policy *name*
associate apn-remap-table *table_name*
associate call-control-profile *profile_name*
exit
lte-policy
subscriber-map *name*
precedence match-criteria all operator-policy-name *policy_name*
exit
exit
context *mme_context_name*
mme-service *mme_svc_name*
associate subscriber-map *name*
end

Notes:

- The **precedence** command in the subscriber map mode has other **match-criteria** types. The **all** type is used in this example.

Configuring Accounting Mode for S-GW

The **accounting mode** command configures the mode to be used for the S-GW service for accounting, either **GTPP** (default), **RADIUS/Diameter**, or **None**.

Use the following example to change the S-GW accounting mode from GTPP (the default) to RADIUS/Diameter:

configure
context *sgw_context_name*
sgw-service *sgw_srv_name*
accounting mode radius-diameter
end

Notes:

- An accounting mode configured for the call control profile will override this setting.

Verifying the Feature Configuration

This section explains how to display the configurations after saving them in a .cfg file as described in the *System Administration Guide* .

Important All commands listed here are under Exec mode. Not all commands are available on all platforms.

Verify that the operator policy has been created and that required profiles have been associated and configured properly by entering the following command in Exec Mode:
show operator-policy full name *oppolicy1*
The output of this command displays the entire configuration for the operator policy configuration.

```
[local]asr5x00 show operator-policy full name oppolicy1
Operator Policy Name = oppolicy1
Call Control Profile Name                    : ccprofile1
   Validity                                  : Valid
APN Remap Table Name                         : remap1
   Validity                                  : Valid
IMEI Range 711919739      to       711919777
   IMEI Profile Name                         : imeiprof1
      Include/Exclude                        : Include
        Validity                             : Valid
APN NI homers1
   APN Profile Name                          : apn-profile1
      Validity                               : Valid
```

Notes:

- If the profile name is shown as "Valid", the profile has actually been created and associated with the policy. If the Profile name is shown as "Invalid", the profile has not been created/configured.
- If there is a valid call control profile, a valid APN profile and/or valid IMEI profile, and a valid APN remap table, the operator policy is valid and complete if the IMSI range has been defined and associated.

CHAPTER 37

Operator Specific QCI

This chapter describes the addition of new standardized QCI values and Operator Specific QCI values.

Feature Description

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

The Operator Specific QCI feature provides the following functionalities:

- MME provides a CLI to enable/disable 'operator-defined-qci' under QOS-Profile.
- Operator Specific QCI value ranges from 128 to 254.
- The new standardized QCI values 65, 66, 69 and 70 is accepted for configuration under all existing CLIs that involves QCI.
- QCI validation is performed during configuration to avoid invalid values.
- Existing QOS control on all bearers is extended to the new QCIs values. A specific QCI or a range of QCIs can be associated to a Bearer Control Profile under QoS-Profile. An operator specific QCI can be re-mapped to another QCI using this Bearer Control Profile. Bearer level parameters such as ARP, MBR, GBR values can be configured independently for default/dedicated bearer along with action such as **prefer-as-cap** or **pgw-upgrade** in the Bearer Control Profile.

- MME rejects the default/dedicated bearers with QCIs that are configured to be rejected under QoS-Profile.
- MME provides CLI configuration under the Bearer Control Profile to map Operator Specific QCI to Pre-Release8 QoS parameters or a standard QCI.
- The standardized QCI mapping is defined according to the TS 23.401 3GPP specification.
- Every Standard QCI GBR/Non-GBR is associated with a priority level as shown below:

QCI	Resource Type	Priority
1	GBR	2
2	GBR	4
3	GBR	3
4	GBR	5
5	Non-GBR	1
6	Non-GBR	6
7	Non-GBR	7
8	Non-GBR	8
9	Non-GBR	9
65	GBR	0.7
66	GBR	2
69	Non-GBR	0.5
70	Non-GBR	5.5

  - Priority Level 1 has the highest priority and in case of congestion lowest priority level traffic would be the first to be discarded.
  - The operator specific QCIs from 128 to 254 shall have the lowest priority. These priority values are considered while deriving resultant QoS values for the Minimum and Reject-if-exceed actions configured in prefer-as-cap or pgw-upgrade

- The **paging-map** CLI is enhanced to accommodate QCI values - 65, 66, 69 and 70.
- The **qci-reject** CLI under QoS-Profile is modified to accept Operator Specific QCI values.

Note MME supports standardized QCIs from 1 to 9. It accepts the new standardized QCI values 69 and 70 for default bearer creation and 65, 66, 69 and 70 for dedicated bearer creation. Any other QCI value is considered invalid.

Controlling Process Related QCI on S6A

Standardized Non-GBR QCI values 69 and 70, and operator specific QCI values in the range 128 to 254 enabled using the **operator-defined-qci** CLI under QoS-Profile is accepted from the subscription (HSS). If the CLI is not enabled, MME will reject all Operator Specific values.

Controlling Process Related QCI on S11

Standardized QCI values 65, 66, 69 and 70, and operator specific QCI values in the range 128 to 254 enabled using the **operator-defined-qci** CLI under QoS-Profile is accepted from the S-GW. If the CLI is not enabled, MME will reject all Operator Specific values.

Note

- The **qci-reject** CLI under QoS profile can be used to reject any specific QCI value or a range of QCI values.
- Standardized QCI values are accepted even if the operator-defined-qci CLI is not enabled.

Mapping of Operator Specific QCI to 3GPP Pre-Release QoS Parameters

Mapping of Operator Specific QCIs to Pre-Release8 QoS parameters is supported for successful handover of bearers to UTRAN/GERAN during handoff

A new CLI is implemented in MME to map standard or non-standardized QCI's to PreRelease8QoS parameters so that the bearers are transferred during a handover to Gn-Gp SGSN. The mapped QoS values would be sent in GTPv1 SGSN-Context-Response or Forward-Relocation-Request messages to peer SGSN.

One of the following values can be used to map EPC QoS from non-standard QCIs to 3GPP pre-release8 QoS:

- All pre-release8 QoS parameters.
- A standard QCI value (according to the mapping defined in 3GPP TS 23.401 standards).

To support mapping, a new CLI is added in the Bearer Control Profile Configuration Mode. If this configuration is not available, MME uses background class values as default, and maps the QCIs to the background class and its associated QoS parameters.

Standards Compliance

The Non-Standard and Operator Specific QCI feature complies with the following standards:

- LTE; General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access (3GPP TS 23.401 version 12.8.0 Release 12).
- LTE; Quality of Service (QoS) concept and architecture (3GPP TS 23.107 version 12.0.0 Release 12).
- LTE; Policy and charging control architecture (3GPP TS 23.203 version 13.1.0).

Configuring Operator Specific QCI

This section documents the configuration procedures for the Operator Specific QCI feature.

The following CLI enables Operator Specific QCI in MME. If this CLI is enabled, MME accepts the QCI range 128 - 254 from HSS and P-GW.

configure
quality-of-service-profile *profile_name*
[remove] operator-defined-qci
end

Note

- By default, this command is disabled.
- **operator-defined-qci** enables Operator Specific QCI values.
- **remove** disables the Operator Specific QCI configuration.

The following CLI maps non-standardized QCIs to PreRelease8QoS parameters for transferring bearers during a handover to Gn-Gp SGSN:

configure
bearer-control-profile *profile_name*
[remove] { pre-rel8-qos-mapping { { class { background | conversational | interactive | streaming } } { thp *thp_value* **} { sig-ind** *indicator_value* **} { src-stat-desc** *value* **} { min-transfer-delay** *value* **} { sdu error-ratio** *value* **} } | qci** *value* **}**
end

Note

- **pre-rel8-qos-mapping** defines (MME) mapping of EPC QOS (non-standard QCIs) to 3GPP PreRelease8 QoS parameters.
- **qci** indicates the QoS class. Its value ranges from 1 to 9. When QCI is configured, the corresponding mapping takes place based on 3GPP TS 23.401.
- **class** indicates the UMTS traffic classified into the following categories:
  - **background**
  - **conversational**
  - **interactive**
  - **streaming**
- **thp** Traffic handling priority specifies the relative importance of handling all SDUs that belong to the UMTS bearer compared to the SDUs of other bearers. The priority value ranges from 1 to 3, where the value 1 holds the highest priority. The predefined thp value is 3
- **sig-ind** toggles the state of the signal. The values are either 0 or 1.
- **src-stat-desc** toggles the state of the signal. The values are either 0 or 1.
- **sdu error-ratio** Service Data Unit (SDU) Error ratio indicates the fraction of SDUs lost or detected as error packets. SDU error ratio is defined only for conforming traffic. The range is an integer ranging from 1 to 7. The ratio ranges from 10^-1 to 10^-6. Allowed values are 1(10^-2), 2(7*10^-3), 3(10^-3), 4(10^-4), 5(10^-5), 6(10^-6) and 7(10^-1). The predefined minimum value is 1.
- **min-transfer-delay** defines the maximum delay for 95th percentile of the delay distributed for all delivered SDUs during the lifetime of a bearer service. The delay value ranges from 10 to 40,000 milliseconds. The predefined minimum value is 100.

  The delay for an SDU is defined as the time from request to transfer and SDU at one SAP to its delivery at the other SAP.

Monitoring and Troubleshooting Operator Specific QCI

This section provides information on how to monitor and troubleshoot the Non-Standard and Operator Specific QCI Support feature.

For information on troubleshooting, please refer to the Monitoring and Troubleshooting section in the *QoS Profile Support* chapter in the *MME Administration Guide*

Non-Standard and Operator Specific QCI Support Show Command(s) and/or Outputs

Monitor the configuration of Non-Standard and Operator Specific QCI feature, by using the following command:

show quality-of-service-profile full all

On executing the above show command, the following new field is displayed:

- Operator Defined QCI

show bearer-control-profile full all

This command is used to display QoS parameters configured for mapping Operator Specific QCI to 3GPP Pre-Release8 parameters

On executing the above command, the following new fields are displayed:

- pre-rel8-qos-mapping
  - Class
  - traffic handling priority
  - sdu error ratio
  - minimum transfer delay
  - source stats descriptor
  - signaling indication
  - QCI value

show mme-service statistics esm-only verbose

A new counter is added to monitor Operator Specific QCIs. This command is used to display the total number of bearers using Operator Specific QCIs.

On executing the above command, the following fields are displayed:

Bearer Statistics:

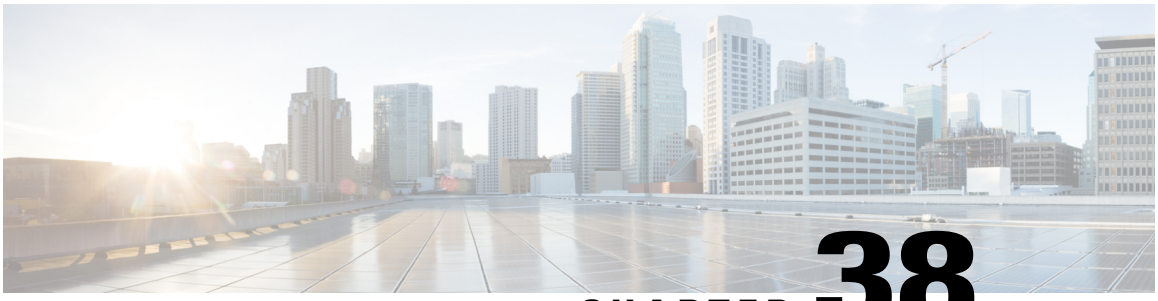
All Bearers: 0 Connected Bearers: 0

Idle Bearers: 0

Bearers Using Operator-Specific QCI:

All Bearers: 0 Connected Bearers: 0

Idle Bearers: 0



CHAPTER 38

Operator Policy Selection Based on IMEI-TAC

Feature Description

Operator policies (proprietary Cisco functionality) empower the carrier/network operators to configure preferred call handling practices. Also, operator policies can be configured to determine the granularity of the implementation: to groups of incoming calls or simply to one single incoming call. The purpose, use, and configuration of operator policies is outlined in the *Operator Policy* chapter elsewhere in this guide.

Based on the configuration (see *Configuring Operator Policy Based on IMEI-TAC*), the MME will select / re-select the operator policy whenever the MME retrieves the IMEI or IMEI-SV in one of the following scenario:

- normal 4G Attach when the IMEI/IMEI-SV is retrieved via Identity-Request with IMEI.
- normal 4G Attach when the IMEI/IMEI-SV is retrieved via Security-Mode-Complete (**policy attach imei-query-type** under MME service must be enabled).
- normal 4G TAU when the IMEI/IMEI-SV is retrieved via Security-Mode-Complete (**policy tau imei-query-type** under MME service must be enabled).
- inbound handover when IMEI/IMEI-SV is received with IMSI via the Forward-Relocation-Request.
- S10 and S3 Attaches when IMEI/IMEI-SV is retrieved with IMSI via EGTP-Identification-Request.
- Inter-RAT TAU and Intra-RAT TAU with MME change when IMEI/IMEI-SV is received with IMSI in Context-Response.

Selection Based on IMEI-TAC

With Releases 18.5 and higher,"Operator Policy Selection Based on IMEI-TAC" enables the MME to selects / re-select 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 IMEI number is assigned to a mobile device or user equipment (UE) by the manufacturer. The network uses the IMEI to identify if devices are valid.

Including the type allocation code (TAC) in the operator policy selection process supports network access restrictions being applied to UEs based on the type of wireless device identified by the IMEI-TAC. The TAC, the first eight digits of the 15-digit IMEI or 16-digit IMEI-SV, identifies the equipment manufacturer, the wireless device type and the model number (if there is one); for example, TAC of 35201906 identifies an Apple iPhone 5S.

IMEI-TAC Groups

With Release 18.6 and higher, the MME supports configuration of up to 25,000 IMEI-TAC, up from the original number of 1024 IMEI-TAC per MME. As well, these IMEI-TAC can be configured in groups listing individual IMEI-TAC and/or organized in ranges of IMEI-TAC. Up to 50 IMEI-TAC groups can be configured per MME and once an IMEI-TAC group is created, each group can be configured with up to 500 unique IMEI-TAC values and/or up to 20 IMEI-TAC ranges - which can overlap. For command details, refer to the *Configuration* section below.

Granular Selection Options for IMEI-TAC: MCC/MNC, MSIN, PLMNID

With Release 19.4 and higher, the operator is allowed more granular control of configuration for operator policy selection. Besides operator policy selection based on IMEI-TAC of the UE, the operator can optionally configure selection based on:

1. IMEI-TAC only,
2. IMEI-TAC + Service PLMNID,
3. IMEI-TAC + MCC-MNC of UE,
4. IMEI-TAC + MCC-MNC of UE + Serving PLMNID,
5. IMEI-TAC + IMSI,
6. IMEI-TAC + IMSI + Serving PLMNID,

The MME uses this configuration to select the operator policy whenever it retrieves the IMEI/IMEI-SV from either a UE or a peer for all non-emergency calls.

How It Works

Based on the configuration (see *Configuring Operator Policy Based on IMEI-TAC*), the MME will select / re-select the operator policy whenever the MME retrieves the IMEI or IMEI-SV in one of the following scenario:

- normal 4G Attach when the IMEI/IMEI-SV is retrieved via Identity-Request with IMEI.
- normal 4G Attach when the IMEI/IMEI-SV is retrieved via Security-Mode-Complete (**policy attach imei-query-type** under MME service must be enabled).
- normal 4G TAU when the IMEI/IMEI-SV is retrieved via Security-Mode-Complete (**policy tau imei-query-type** under MME service must be enabled).
- inbound handover when IMEI/IMEI-SV is received with IMSI via the Forward-Relocation-Request.

- S10 and S3 Attaches when IMEI/IMEI-SV is retrieved with IMSI via EGTP-Identification-Request.
- Inter-RAT TAU and Intra-RAT TAU with MME change when IMEI/IMEI-SV is received with IMSI in Context-Response.

Supported Options

With this feature, the MME supports location-based restriction based on the IMEI-TAC. The MME Service configuration must include settings to instruct the MME to retrieve/query the IMEI/IMEI-SV for Attach and TAU. Refer to *Configuring Policy Selection for Normal 4G Attach/TAU*.

Restrictions

For all emergency calls, the MME selects the emergency profile and not an operator policy based on IMEI-TAC configuration.

Currently, the MME allows a maximum of 1024 associations of operator policy to the key where the key can be any of the following: IMSI, SERVICE PLMN-ID, SSI-ID, Domain, IMEI-TAC and ALL.

Configuring Operator Policy Selection Based on IMEI-TAC

There are multiple components involved in the configuration of this feature. We recommend that for first time feature configuration, you perform the configurations in the order in which they are presented below.

Configuration of this feature makes use of many previously existing commands and keywords. Only new or modified commands and keywords are explained in detail in this document.

Configuring the Operator Policy(s) and Call Control Profile(s)

We recommend that you first configure the operator policy and call control profile and make a note of the names you assign the policy and profile.

```
configure
    operator-policy name policy_name
        associate call-control-profile name profile_name
        exit
    call-control-profile name profile_name
        end
```

Notes:

- For information about these commands and keywords, refer to the *Command Line Interface Reference*.

Configuring Policy Selection for Normal 4G Attach/TAU

To enable the MME to retrieve the IMEI from the UE, the following MME service configuration is required. The following configures the Operator Policy selection based on IMEI-TAC for normal 4G Attach or normal 4G TAU when the IMEI/IMEI-SV is retrieved via Security-Mode-Complete. After the operator policy and

call control profile are configured, then perform the additional configuration of the **imei-query-type** for the MME service.

configure
context *context_name*
mme-service name *service_name*
policy { attach | tau } imei-query-type { imei | imei-sv } verify-equipment-identity [allow-on-eca-timeout | deny-greylisted | deny-unknown | verify-emergency]
end

Notes:

- The command listed above are not new for this feature. For information about these commands and keywords, refer to the *Command Line Interface Reference*.

Configuring IMEI-TAC based Selection of the Operator Policy

Important The operator policy(s), call-control profile(s), and IMEI-TAC group(s) need to be configured already and according to the instructions above.

To setup IMEI-TAC-based operator policy selection, use the **precedence** command in the LTE Subscriber Map configuration mode to:

- set the order of precedence for the subscriber map,
- set which type of matching criteria is to be used to determine which operator policy to select - for this procedure, use the **imei-tac** keyword,
- optionally, set more granular IMEI-TAC matching criteria, either singly or in pairs:
  - mcc + mnc
  - imsi
  - service-plmnid
- point to an operator policy for subscribers meeting the match criteria.

Important The following example details configuration for IMEI-TAC-based selection. Other match criteria options are not included here. For more information on configuration options, refer to the *Command Line Interface Reference*.

configure
lte-policy
subscriber-map *map_name*
precedence *precedence_number* **match-criteria imei-tac group** *group_name* **[imsi mcc** *mcc* **mnc** *mnc* **[msin { first** *start_msin_value* **last** *end_msin_value* **}]] [operator-policy-name** *policy_name*
end

no precedence *precedence_number*
end

Notes:

- **precedence** *precedence_number*- The precedence level defined by the operator is used to resolve the selection of the operator policy when multiple variable combinations match for a particular UE. The lower precedence number takes greater priority during selection. The precedence number must be an integer from 1 through 1024.
- **match-criteria** - Selects which set of variables will be 'matched-to' to select an operator policy. For this procedure, use the **imei-tac** keyword to select the IMEI-TAC group as the matching criteria. For more granular match criteria, include the following singly or in pairs: IMSI and/or MCC+MNC and/or serving PLMNID in accordance with the following usage options:
  - Operator policy selection based on IMEI-TAC only, syntax example:

    precedence 1 match-criteria imei-tac-group myGroup operator-policy-name BESTpol
  - Operator policy selection based on IMEI-TAC + Service PLMNID, syntax example:

    precedence 1 match-criteria imei-tac-group myGroup service-plmnid 12345 operator-policy-name BESTpol
  - Operator policy selection based on IMEI-TAC + MCC-MNC of UE, syntax example:

    precedence 1 match-criteria imei-tac-group myGroup imsi mcc 123 mnc 234 operator-policy-name BESTpol
  - Operator policy selection based on IMEI-TAC + MCC-MNC of UE + Serving PLMNID, syntax example:

    precedence 1 match-criteria imei-tac-group myGroup imsi mcc 123 mnc 234 service-plmnid 56789 operator-policy-name BESTpol
  - Operator policy selection based on IMEI-TAC + IMSI, syntax example:

    precedence 1 match-criteria imei-tac-group myGroup imsi mcc 123 mnc 234 msin first 1223 last 2333 operator-policy-name BESTpol
  - Operator policy selection based on IMEI-TAC + IMSI + Serving PLMNID, syntax example:

    precedence 1 match-criteria imei-tac-group myGroup imsi mcc 123 mnc 234 msin first 1223 last 2333 service-plmnid 56789 operator-policy-name BESTpol
- **group** *group_name* - Identifies the name of the previously-defined IMEI-TAC group with the configured IMEI-TAC values to use for matching. The group name is a string of 1 through 64 alphanumeric characters.
- **operator-policy-name** *policy_name* - Configures the name of the operator policy to which selection should be pointed after the criteria matching is completed. The policy name is a string of 1 through 63 alphanumeric characters.
- For more information about the **lte-policy**, **subscriber-map**, and the **precedence** commands, refer to the *LTE Subscriber MAP Configuration Mode* chapter in the *Command Line Interface Reference* .

Verifying the Configuration

From the Exec mode, use the following to verify the configuration for operator policy selection based on IMEI-TAC:

show configuration
The following is an example of the type of information that would be presented in the show output:

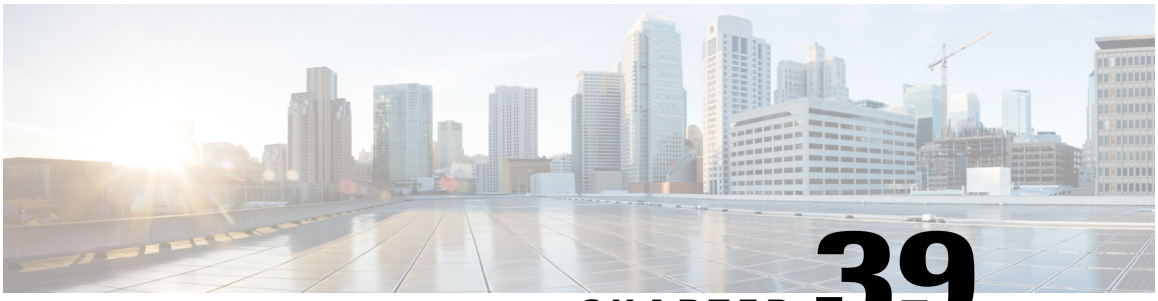
```
config
... ... ...
  lte-policy
    subscriber-map submap1
      precedence 1 match-criteria imei-tac group itacgrp1 operator-policy-name oppol1
      precedence 2 match-criteria imei-tac group imeitacgrp11 service-plmnid 12345
operator-policy-name op2
      precedence 3 match-criteria imei-tac group imeitacgrp2 operator-policy-name op1
    exit
    imei-tac-group itacgrp1
      tac 31441551 77777777 87650506 87654321
      tac-range from 23456789 to 98765432
    exit
    imei-tac-group imeitacgrp11
      tac 01192119 66666666 87650999 98765432
      tac-range from 11001100 to 11111111
….. … ….
    exit
... ... …
end
```

Monitoring and Troubleshooting the Operator Policy Selection Based on IMEI-TAC

Verify Configuration

Use the following show commands to verify the configuration to ensure that it is correct:

- **show operator policy full { all | name***policy_name* **}**
- **show call-control-profile full { all | name** *profile_name* **}**
- **show mme-service name** *service_name*
- **show lte-policy subscriber-map name** *map_name*
- **show lte-policy imei-tac-group summary**
- **show lte-policy imei-tac-group name** *group_name*



CHAPTER 39

Overcharging Protection

Overcharging Protection helps to avoid charging subscribers for dropped downlink packets while the UE is in idle-mode.

Feature Description

For Non-GBR (Guaranteed Bit Rate) 4G bearers, the P-GW is not aware when the UE loses radio coverage, and will continue to forward and charge downlink packets, which can result in overcharging of subscribers. 3GPP does not specify a standard solution to deal with such scenarios.

A typical example is when a subscriber drives into a tunnel while having an active download session. Downlink packets will be counted in P-GW before discarded later in S-GW due to the UE not responding to paging.

The subscriber may lose coverage while connected to a particular MME/S-GW and later regain coverage in the same or diiferent MME/S-GW.

The subscriber may lose coverage in 4G and regain coverage in 2G/3G, or vice versa.

Gn and S3/S4 based network architecture may be used in the case of Loss of Radio Coverage.

A valid license key is required to enable Overcharge Protection on the MME. Contact your Cisco Account or Support representative for information on how to obtain a license.

Relationships to Other Features

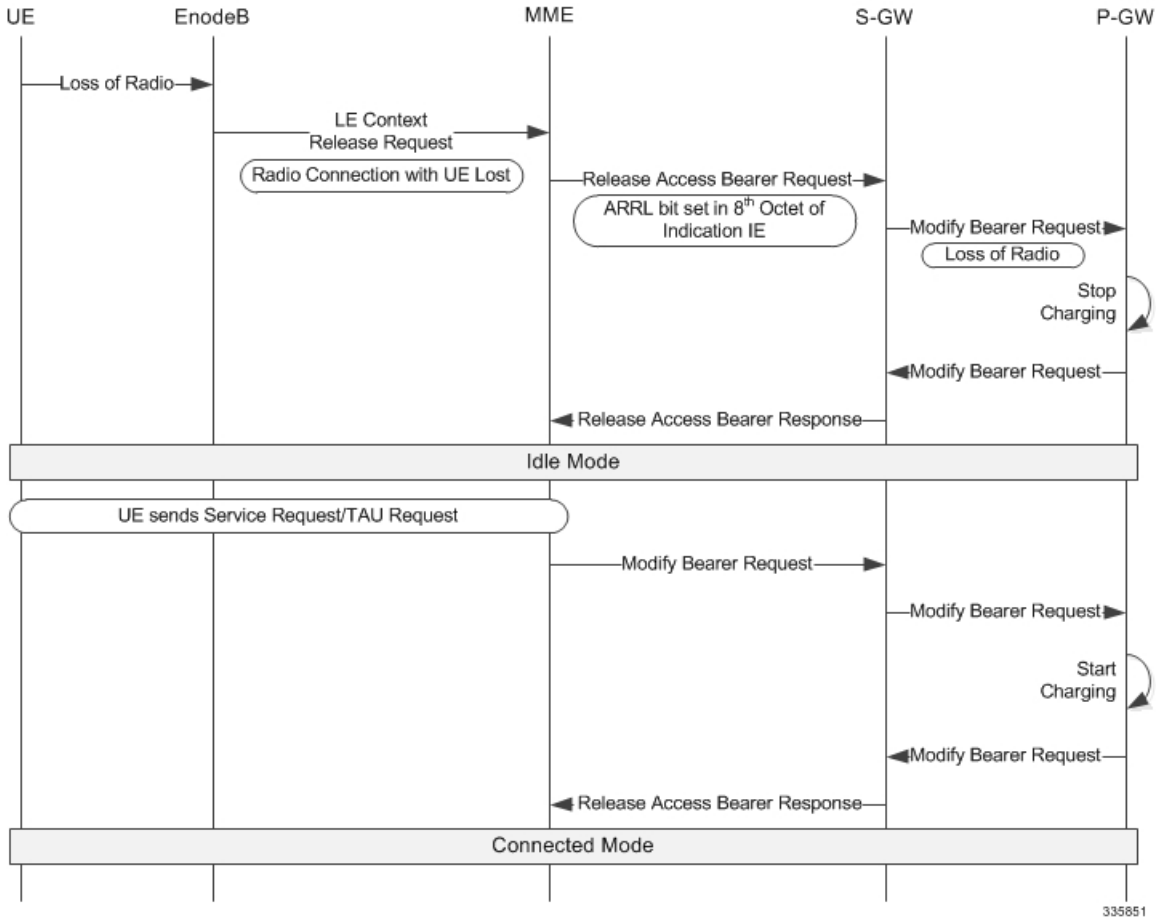
Overcharging protection on the MME requires separate overcharging protection licenses on the S-GW and P-GW.

How It Works

Call Flows

The following diagram depicts the call flow when a UE loses radio access, and then later regains access, as it relates to overcharging protection.

Figure 34: Overcharging Protection Call Flow



Overcharging protection in MME is triggered by a UE Context Release Request from the eNodeB. This request can come to MME when UE is in EMM connected/connecting mode.

On receiving the UE Context Release Request, the MME checks the radio cause in the received message against the configured overcharging protection cause code.

If the configured cause code matches the received cause code, the MME sends Loss of Radio Contact using ARRL (Abnormal Release of Radio Link) bit in the Release Access Bearer Request (GTPv2 message) to the S-GW. The ARRL (Abnormal Release of Radio Link) is bit 7 in the 8th Octet of Indication IE of Release Access Bearer Req message.

On Receiving ARRL indication in Release Access Bearer Request , the S-GW will inform the P-GW to stop charging.

When the radio contact is resumed in the 4G network, the Modify Bearer Req will enable the P-GW to start charging again.

The ARRL bit is supported only in Release Access Bearer Request message by MME.

Configuring Overcharge Protection

Enabling Overcharging Protection

To enable overcharging protection for a specific MME service, issue the following commands:

configure
context *context_name*
mme-service *svc_name*
policy overcharge-protection s1ap-cause-code-group *group_name*
end

To disable overcharging protection:

no policy overcharge-protection

Configuring S1AP Cause Code Group and Cause Code

To configure the S1AP Cause Code Group and S1AP cause code "Radio Connection With UE Lost (21)":

configure
lte-policy
cause-code-group *group_name* **protocol s1ap**
class radio cause *radio_cause_code*
end

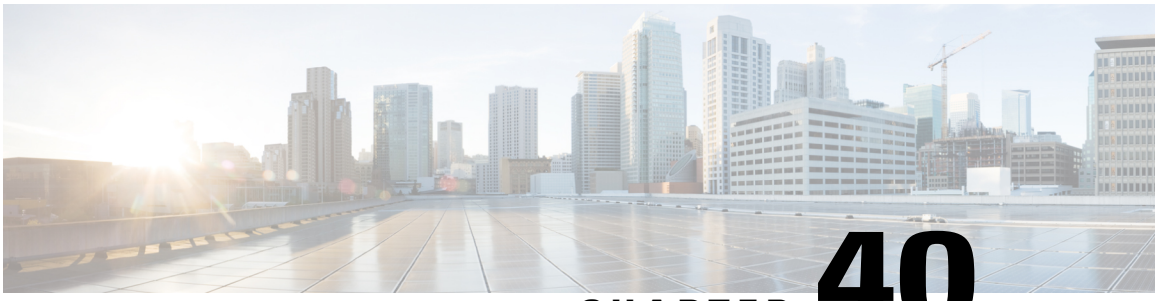
Notes:

- For example, to define a cause code group for the code "Radio Connection With UE Lost", enter: **class radio cause 21**

Verifying the Overcharge Protection Configuration

The **Overcharge Protection** field has been added to the output of **show mme-service name** *service_name* to display the configuration of this feature, either "Not configured" or showing the configured S1-AP cause code group name:

```
Policy Inter-RAT Indirect Fwd Tunnels    : Never
Policy Inter-RAT Ignore SGSN ContextID   : Disabled
Policy S1-Reset                          : Idle-Mode-Entry
Overcharge Protection                    : Cause Code Group grp1
```



CHAPTER 40

Paging Priority IE Support

Feature Description

This feature is developed to provide Paging Priority support on the MME. Paging priority support is provided for Mobile Originating and Mobile Terminating CSFB calls.

Mobile Terminating CSFB calls: Mobile terminating CSFB calls are prioritized by providing paging priority information to the eNodeB during CSFB calls; the eNodeB in turn pages the UEs accordingly. If the MME is configured to send paging priority to the eNodeB, when a paging request message is received on the SGs interface with an indication of the eMLPP priority level, the MME sends the paging priority value in the S1AP paging message request to the eNodeB.

Mobile Originating CSFB calls: In Mobile originating CSFB calls if the UE is subscribed for eMLPP services, the MME uses the mps-cs-priority received in the subscription to set the priority as "CSFB High Priority" in "CS Fallback Indicator IE". This priority value is sent in the S1AP UE Context Setup/Modification message to the eNodeB, the eNodeB then initiates the CSFB procedure with priority.

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

Important From release 20.0 onwards, Paging Priority is supported for Packet Switched traffic. The MME also supports eMPS (Enhanced Multimedia Priority Support) for both PS and CS domains. For more information see, feature chapter for Enhanced Multimedia Priority Service.

Architecture

Paging priority IE support is implemented in a network which supports CSFB priority call handling. When a call is received with an eMLPP Priority level indication, the VLR/MSC sends this value of priority level indication in the eMLPP priority information element as a part of SGs AP PAGING-REQUEST message to the MME. MME propagates this eMLPP priority as paging priority information element in S1AP paging-request message to eNodeB.

If MPS-Priority AVP is present and the UE is subscribed to the eMLPP or 1x RTT priority service in the CS domain as indicated by the MPS-CS-Priority bit of the AVP, the MME allows the UE to initiate the RRC connection with higher priority than other normal UEs during CS Fallback procedure.

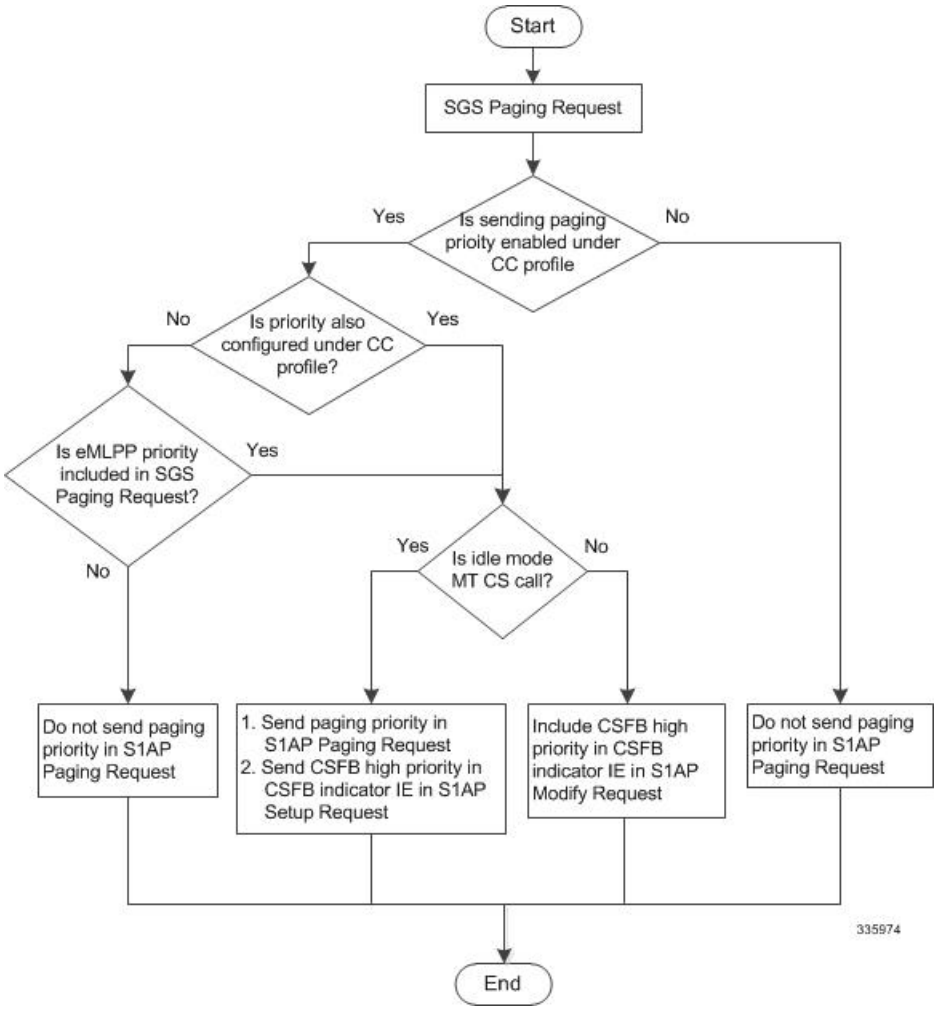
The MME uses the MPS-Priority received in subscription and sets CSFB fallback high priority in "CS Fallback Indicator IE" in the S1AP UE Context Setup/Modification in S1AP UE Context Setup/Modification messages.

How It Works

The MME relays the eMLPP priority value received from MSC/VLR as paging priority-ie in S1AP paging-request message to eNodeBs. With the implementation of this feature a new CLI command **paging-priority cs** is introduced under the Call Control Profile configuration mode through which the operator can configure the system to control sending of the paging priority value to the eNodeB. The operator can configure the system to ignore the eMLPP priority value received from MSC and configure the MME to send user-defined value as paging-priority to eNodeB. The operator can also choose to completely ignore eMLPP priority and disable sending priority value. Operator can configure the system to send paging priority IE always in S1AP Paging request irrespective of whether MSC/VLR include/supports eMLPP priority or not. This applicable to mobile terminating CS fall back call.

The following flowchart illustrates the paging priority support provided for Mobile Terminating CSFB calls:

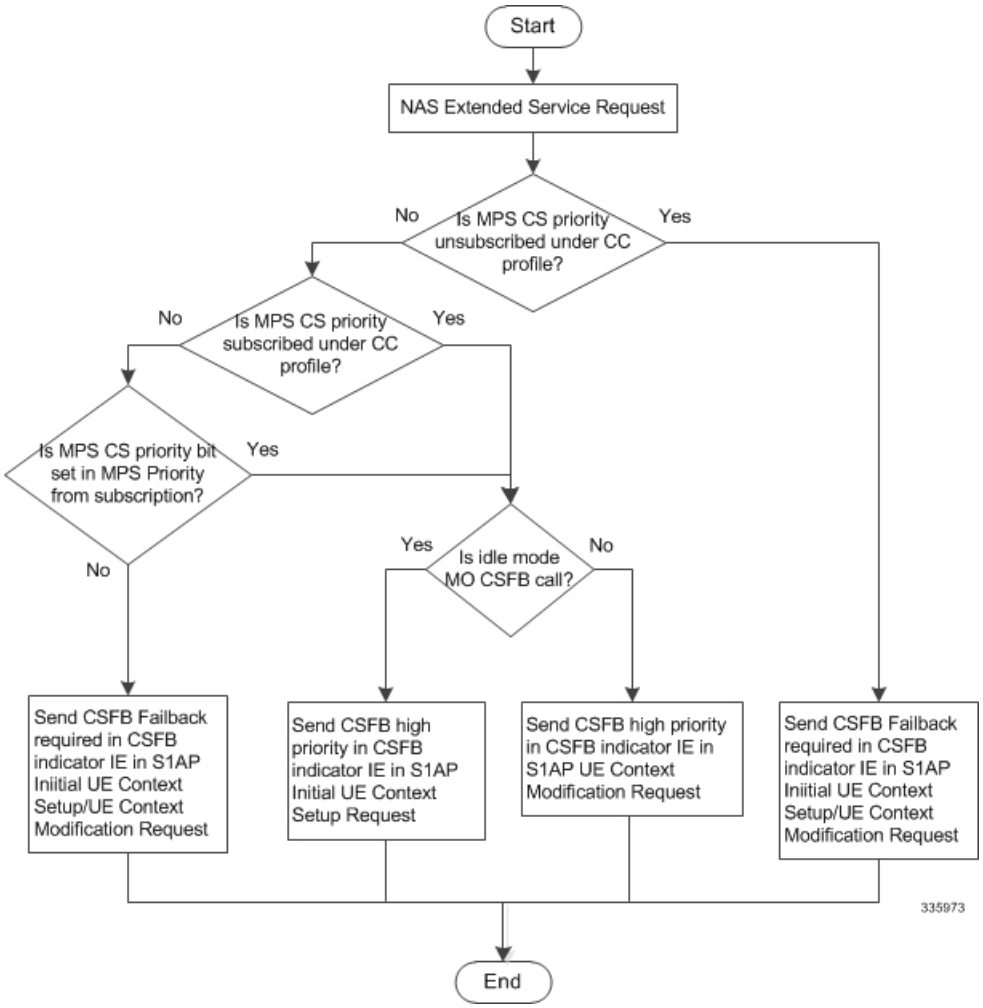
Figure 35: Paging Priority Support for Mobile Terminating CSFB Calls



A new CLI command **mps cs-priority** has been introduced under the Call Control Profile Configuration mode to control the handling of MPS-CS-Priority received in the subscription. If MME receives mps-cs-priority in the subscription, it sets the "CS Fallback Indicator IE" to "CSFB high priority" in the S1AP Context Setup/Modification. The Operator can choose to override the mps cs-priority using this CLI command. The MME shall set "CSFB high priority" in "CS Fallback Indicator IE" if either the subscription contains mps-cs priority OR the mps cs-priority subscribed CLI is configured. Similarly, MME shall not set "CSFB high priority" in "CS Fallback Indicator IE" if either the subscription does not have mps-cs priority OR the mps cs-priority none is configured. This is applicable to mobile originated CSFB call.

The following flowchart illustrates the paging priority support provided for Mobile Originating CSFB calls:

Figure 36: Paging Priority Support for Mobile Originating CSFB Calls



For more information see the configuration section for Paging Priority support in this feature chapter.

Limitations

- For release prior to 20.0, Paging Priority is not supported for PS paging.
- Inclusion of Additional CSFB indicator for CSFB MO Emergency calls is not supported

Standards Compliance

Paging priority support complies with the following 3GPP standards:

- 3GPP TS 36.413

- 3GPP TS 29.272
- 3GPP TS 29.118

Configuring Paging Priority Support for CSFB Calls

The following commands are configured to provide paging priority support for Mobile Originating CSFB calls and Mobile Terminating CSFB calls.

Configuring Paging Priority Support for Mobile Terminating CSFB calls

The following new CLI command under the Call Control profile configuration mode is configured to support sending of paging-priority value in S1AP paging-request message to the eNodeB. This command helps the operator to prioritize the Mobile terminated CSFB voice calls of a set of subscribers irrespective of them subscribed for eMLPP services or not.

configure
call-control-profile *cc_profile_name*
[remove] paging-priority cs *value*
exit

Notes:

- By default, sending of paging priority-ie in S1AP paging-request message to eNodeBs is enabled. The priority value received from the MSC/VLR is relayed to the eNodeB.
- The keyword **cs** is used to configure the value of paging-priority sent to eNodeB for CS paging. The paging priority value is an integer in the range "0" up to "7". Configuring a value of "0" disables sending of paging priority value to eNodeB.
- A lower value of paging priority indicates a higher priority.
- Older values of paging priority are overridden by configuring new values.
- The **remove** keyword deletes the existing configuration.

Usage example:

The following command is issued to disable sending of paging priority value to the eNodeB:

[local]asr5x00(config-call-control-profile-call1)# paging-priority cs 0

The following command enables sending of paging priority value to the eNodeB, a priority value of "5" is configured using this command:

[local]asr5000(config-call-control-profile-call1)# paging-priority cs 5

Configuring MPS CS priority subscription override for Mobile Originating CSFB calls

The following new CLI command under the Call Control profile configuration mode is configured to support multimedia priority service in the CS domain. This command helps the operator to prioritize the Mobile originating voice calls of a set of subscribers irrespective of them subscribed for eMLPP services or not.

configure
call-control-profile *cc_profile_name*
[remove] mps cs-priority { subscribed | none }
exit

Notes:

- By default MME sets the value of "CS fallback indicator IE" as "CSFB High Priority" in the S1AP UE Context Setup/Modification if the MPS-CS-Priority value is set in "MPS-Priority" in EPS Subscription from HSS
- The keyword **cs-priority** configures support for priority service in the CS domain.
- The keyword **subscribed** configures support for priority service in the CS domain. The "CS Fallback Indicator IE" is set to "CSFB High Priority" in the S1AP UE Context Setup/Modification message.
- The keyword **none** configures disables support for priority service in the CS domain. The "CS Fallback Indicator IE" is set to "CSFB Required" in the S1AP UE Context Setup/Modification message.
- The remove keyword deletes the existing configuration.

Usage example:

The following command is issued to set "CSFB High Priority" for "CS Fallback Indicator IE", in the S1AP UE Context Setup/Modification message:

[local]asr5x00(config-call-control-profile-call1)# mps cs-priority subscribed

The following command is issued to set "CSFB Required" for "CS Fallback Indicator IE", in the S1AP UE Context Setup/Modification message:

[local]asr5000(config-call-control-profile-call1)# mps cs-priority none

Monitoring and Troubleshooting the Paging Priority Support for CSFB Calls

This section provides information on the show commands available to monitor and troubleshoot paging priority support for CSFB calls.

Paging Priority Support Show Command(s) and/or Outputs

This section provides information regarding show commands and/or their outputs in support of the Paging priority support in CSFB calls.

show call-control profile full all

The following new fields are added to the show output to display the paging priority configuration for Mobile originating and terminating CSFB calls:

- Paging priority to be sent to eNodeB: If paging priority support is enabled this field displays the configured value of paging priority sent to eNodeB for CS paging. For example, if the paging priority value is set to "1", this field is displayed as "Enabled with value: 1". If paging priority support is disabled this field is displayed as "Disabled".
- MPS CS priority: Is displayed as either "Subscribed" or "None" based on the configuration.

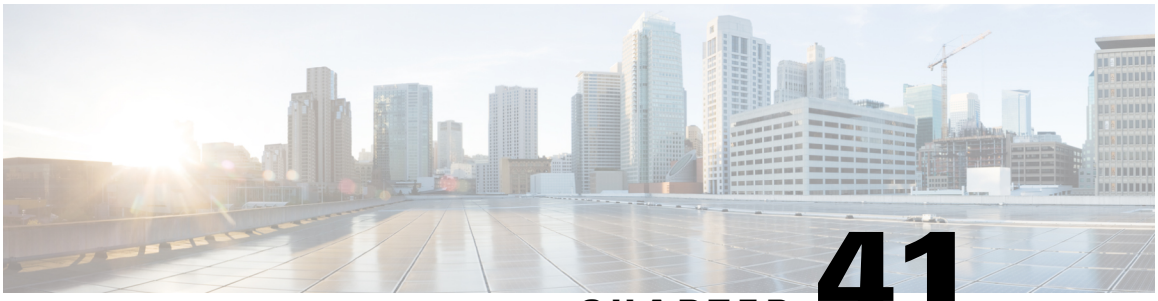
Support and Troubleshooting Information

This section describes trouble shooting information for the Paging Priority support in CSFB calls. If paging priority is not being sent to the eNodeB during mobile terminating CS call, verify the following:

- Verify if eMLPP priority is received from MSC/VLR in SGs-AP Paging-Request message.
- Ensure that sending of paging-priority to eNodeB is not disabled in the call control profile configuration. Execute the show command **show call-control-profile full all** to verify the configuration. The field **Paging priority to be sent to eNodeB** displays the configuration information as either **Disabled** or **Enabled with value <1…7>**.
- Ensure that subscriber under test hits any of the call control profile configured in the system. If the subscriber does not fall under any ccp, then also paging priority will not be sent to eNB.

If CSFB Fall back IE is not set to "CSFB high priority" in S1AP UE context setup/modification during mobile originating CS call, verify the following:

- Verify the configuration; ensure that setting of CSFB high priority is not disabled under Call Control profile. Execute the show command **show call-control-profile full all** to verify the configuration. The field **MPS CS priority** displays the configuration as either **Subscribed** or **None** or **Not Configured**.
- Ensure that the **mps cs priority** bit is set in MPS Priority AVP in subscription received.



CHAPTER 41

Power Saving Mode (PSM) in UEs

Feature Description

Internet of Things (IoT) is a computing concept where everyday objects have internet connectivity and they can collect and exchange data. IoT is a network which can comprise of a wide variety of physical devices, vehicles, buildings, and any other device/object used in our daily lives. They are embedded with sensors, software and network connectivity which help them communicate with other devices in the network and can be controlled remotely thus increasing efficiency, accuracy and economic benefit. Any device/object which has to be a part of the IoT network must have:

- Long battery life
- Low device cost
- Low deployment cost
- Full network coverage
- Support to connect to large number of devices

Power Saving Mode (PSM) was introduced in 3GPP Release 12, to improve device battery life of IOT devices. The most significant benefit of this feature is the UE has more control in terms of power management required for its application. There are a wide range of IoT applications where flexibility of the UE to manage its power is very important and also implementation of PSM can prevent network congestion. The timers of all the devices can be managed using PSM, and the wake-up periods can be adjusted to be offset as much as possible. This way all of the devices will not wake at the same time and attempt to access the network. The PSM mode is similar to power-off but the UE remains registered on the network.

The UE activates PSM by including two timer values in the Attach or Tracking Area Update (TAU). The first timer is the T3324, which defines the time the UE stays active after idle mode following the Attach or TAU procedure. The second timer is an extended T3412 which defines the extended time for an UE to send periodic TAU.

Power Saving Mode Timers

T3324 Active Timer

The UE requests for a T3324 Active Timer value during Attach and TAU procedures. The MME allocates the T3324 value to the UE. The T3324 active timer determines the duration during which the device remains reachable for mobile terminated transaction on transition from connected to idle mode. The device starts the active timer when it moves from connected to idle mode and when the active timer expires, the device moves to Power Saving Mode. The MME takes the UE requested value and MME local configuration into account for determining the Active Timer value. The MME includes the T3324 value IE in the ATTACH ACCEPT/TAU ACCEPT message only if the T3324 value IE was included in the ATTACH REQUEST/TAU REQUEST message. A UE using PSM is available for mobile terminating services only for the period of an Active Time after a mobile originated event like data transfer or signaling for example after a periodic TAU/RAU procedure.

The MME allows a value of '0' for the T3324 timer. In this case the UE enters the Power Saving Mode immediately.

T3412 Extended Timer

The T3412 timer is also referred to as the periodic Tracking Area Update (TAU) timer. Periodic tracking area updating is used to periodically notify the availability of the UE to the network. The procedure is controlled in the UE by the periodic tracking area update timer (timer T3412). The value of timer T3412 is sent by the network to the UE in the ATTACH ACCEPT message and can be sent in the TRACKING AREA UPDATE ACCEPT message. The UE shall apply this value in all tracking areas of the list of tracking areas assigned to the UE, until a new value is received. A longer periodic TAU timer is possible using T3412 extended timer. When the UE includes the T3324 value IE and the UE indicates support for extended periodic timer value in the MS network feature support IE, it may also include the T3412 extended value IE. Apart from the value requested by the UE, the MME verifies the local configuration into account while selecting a value for the T3412 extended timer. When the MME includes the T3412 extended value IE in the ATTACH ACCEPT message or TRACKING AREA UPDATE ACCEPT message , the MME uses timer T3412 extended value IE as the value of timer T3412.

Other Feature Enhancements

The MME allows a value of "0" for timer T3324 (Which implies the UE enters Power Saving Mode immediately).

MME may also include Downlink buffer duration and "Downlink suggested packet count" in DDN ACK if it is configured.

The following new flags are introduced as part of this feature; these flags are supported in GTPCv2 Indication IE:

- Pending Network Initiated PDN Connection Signaling Indication (PNSI): The source MME supports sending of PNSI flag in GTPCv2 Indication IE of Context response.
- UE Available for Signaling Indication (UASI): The MME supports sending of the UASI flag in GTPCv2 Indication IE of Create Session Request and Modify Bearer Request.
- Delay Tolerant Connection Indication (DTCI): The MME supports receiving the DTCI flag in Create Session Response from the SGW. The MME supports receiving of the DTCI flag in Context Response and Forward Relocation Request from peer MME or S4-SGSN.

The MME rejects CBR/UBR when PPF is False. The cause "UE is temporarily not reachable due to power saving" is sent in the response by the MME if the corresponding PDN was marked "Delay tolerant" by PGW.

How It Works

A subscriber is PSM enabled only when:

- UE sends T3324 timer in ATTACH/TAU.
- Power Saving Mode is enabled in configuration by providing T3324 active and T 3412 extended timers or by configuring "UE requested" timer values.

A CLI-based configuration is provided to configure the T 3324 active and T 3412 extended timers. The CLI provides an option to either accept UE requested values or MME configured values for these timers. The CLI is also used to configure either to send or not send the Downlink Buffer Duration in DDN Ack, the DDN Ack Optional IE "Downlink Suggested Packet Count" can also be configured. When the PSM CLI configuration is enabled, the MME accepts the use of PSM and a UE requested value of T3324 is received in Attach/TAU request. If the CLI is configured to accept UE requested values of timers and if T3412 extended timer is not received from the UE along with T3324 in Attach/TAU request, then MME uses the same value of T3412 timer available in MME service configuration. The values of T3324 and T3412 timers extended are determined based on the configuration. If the MME has allocated an Active Time (T3324) to the UE, then the MME starts the Active timer with the value of T3324 whenever the UE enters IDLE mode. If this timer expires, then MME clears the PPF (Paging Proceed Flag). When the PPF is clear, the MME does not page the UE on receiving a Downlink Data Notification message and sends a Downlink Data Notification Ack message with cause "Unable to page UE" to the Serving GW with DL buffering duration and DL suggested packet count IEs as per the operator configuration. The MME rejects network initiated PDN connections during power saving mode. The MME sends the cause "UE is temporarily not reachable due to power saving" if the corresponding PDN was marked Delay Tolerant (DTCI flag set) by PGW. The source MME sets the PNSI flag in Context Response if there are any pending network initiated PDN connections (For example, Create Bearer Request/Update Bearer Request). The MME sets the UASI flag in the Create Session Request or Modify Bearer Request message when UE is available for end-to-end signaling. The UE is in PSM until a mobile originated event (for example periodic RAU/TAU, mobile originated data or detach) requires the UE to begin any procedure towards the MME.

Limitations

UE Power Saving Mode is not supported in the CS domain on the network side. A UE that uses mobile terminated IMS or CS services other than SMS should not use PSM as neither IMS nor the CS domain provide support for mobile terminated CS voice or IMS services to UEs that are in PSM.

Standards Compliance

The Power Saving Mode feature complies with the following standards:

- 3GPP TS 24.301 Release 13.5.0
- 3GPP TS 23.401 Release 13.5.0
- 3GPP TS 29.274 Release 13.5.0

Configuring UE Power Saving Mode

This section describes how to configure the UE Power Saving Mode feature. The following CLI command is introduced in the Call Control Profile to configure the UE Power Saving Mode parameters.

configure
call-control-profile *profile_name*
[remove] psm {ue-requested [dl-buf-duration [packet-count *packet_value* **]]| t3324-timeout** *t3324_value* **t3412-extended-timeout** *t3412_ext_value* **[dl-buf-duration [packet-count** *packet_value* **]]}**
exit

Notes:

- The operator can use the keyword **ue-requested**, when UE requested values for Active and Extended Periodic timers are to be accepted.
- The keyword **dl-buf-duration** is used to send Downlink Buffer Duration in DDN ACK when unable to page UE. If this keyword is not configured buffer duration will not be sent in DDN-ACK. By default buffer duration is not sent in DDN ACK.
- The keyword **packet-count** is used to send 'DL Buffering Suggested Packet Count' in DDN ACK when unable to page UE. The packet count value is an integer value from “0” up to “65535”.
- The keyword **t3324-timeout** is used to configure the T3324 active timer value. The T3324 active timer is an integer value in the range 0 up to 11160 seconds.
- The keyword **t3412-timeout** is used to configure the T3412 Extended timer value. The T3412 extended timer is an integer value in the range 0 up to 35712000 seconds.
- This command is not enabled by default.
- The keyword **remove** is used to disable UE power saving mode.

Monitoring and Troubleshooting

This section provides information on how to monitor the UE Power Saving Mode feature and to determine that it is working correctly.

Show Command(s) and/or Outputs

This section provides information regarding show commands and/or their outputs updated in support of the UE Power Saving Mode feature.

The show commands in this section are available in support of this feature:

show call-control-profile full name

The PSM parameters are added to this show command:

- UE Power Saving Mode: This section displays all the PSM related parameters.
- T3324 Timeout: Displays the T3324 timer value in seconds.
- T3412 Extended Timeout: Displays the T3412 extended timer value in seconds.

- Downlink Buffer Duration in DDN ACK: Displays if Downlink Buffer Duration in DDN ACK is either enabled or disabled.
- DL Buffering Suggested Packet Count in DDN ACK: Displays the DL buffering suggested packet count in DDN ACK.

show mme-service session all

The following new parameters are added to this show command:

- UE Reachability Timer (PSM UE)
- T3412 Extended Timer

Note These timers are calculated based on operator configuration in the psm command under the Call-Control-Profile configuration mode.

show mme-service statistics

The following new parameters are added to this show command:

- PSM Subscribers: Displays information related to PSM subscribers.
- Attached Calls: Displays the number of attached subscribers for whom PSM is enabled.
- DDN Rejects: Displays the number of DDN rejects that have occurred for PSM enabled subscribers. A Downlink Data Notification (DDN) is rejected when an UE is in power saving mode.

show egtpc statistics verbose

The following new parameter is added to this show command:

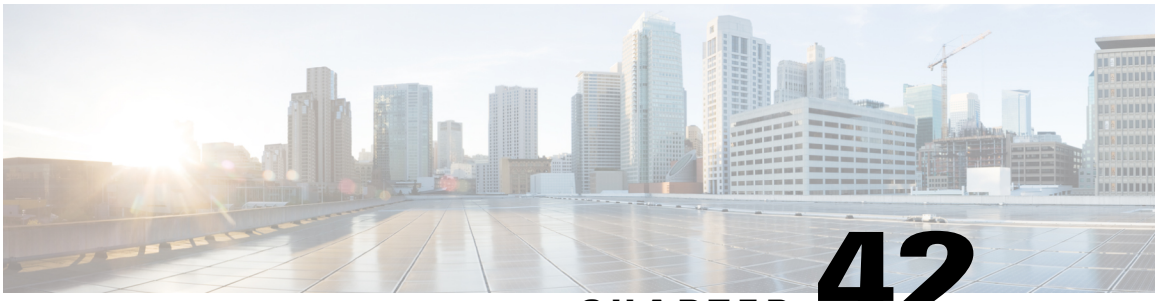
- UE not reachable due to PSM

The Create Bearer Request and Update Bearer Request are rejected when the UE is in Power Saving Mode. The MME sends the cause "EGTP_CAUSE_UE_TEMP_NOT_REACHABLE_DUE_TO_POWER_SAVING" in the reject message if that PDN is marked "Delay Tolerant" by PGW (DTCI flag enabled in PDN Connection Indication IE of Create Session Response). Otherwise the MME sends the cause "EGTP_CAUSE_UNABLE_TO_PAGE_UE" to SGW in CBR/UBR Reject.

UE Power Saving Mode Bulk Statistics

The following statistics are included in the MME Schema in support of the UE Power Saving Mode feature:

- attached-psm-subscriber
- ddn-rejects-psm



CHAPTER 42

QoS Profile Support

Feature Description

Release 19.2 introduces the MME "QoS Profile" feature for support of Quality of Service (QoS) profiles and Bearer Control profiles. The QoS profile can be defined for a given APN for EPS or 4G subscribers. One or more Bearer Control profiles can be associated to a QoS profile on the basis of a QoS class identifier (QCI) or a range of QCI. Together, these profiles allow PDN-level and bearer-level control of APN-AMBR and QoS parameters received from an HSS and/or a PGW.

A QoS profile is defined by:

- a list of bearers to be rejected based on QCI, and
- operator-provided values for capping AMBR (UL and DL).

Bearer Control profile is defined by:

- remapping matrix for QCI,
- operator-provided values for capping ARP PL/PCI/PVI, and
- operator-provided values for capping MBR and GBR (UL and DL).

Important For Release 19.2, this feature is released with a feature license that will not be enforced until Release 20.0.

How It Works

Operational Controls

The MME provides the flexibility to configure a Quality of Service (QoS) profile for an APN and multiple Bearer Control profiles to associate with the QoS profile.

Profile Controls

QoS profile allows control of

- PDN-level QoS parameters, such as APN-AMBR,
- rejection of bearers based on QCI or range of QCI.

Bearer Control profile allows control of

- bearer-level QoS parameters such as ARP, ARP-PVI, ARP-PCI, MBR, and GBR, as well as the action to be taken, such as prefer-as-cap or pgw-upgrade
- remapping a QCI value for default and/or dedicated bearer, and pgw-upgrade action for QCI

Notes:

- For default bearer, the QCI of the bearer is initially determined by the subscription from the HSS or the value received from the peer-MME/S4-SGSN during inbound relocation.
- For dedicated bearer, the QCI of the bearer is initially determined by the QCI value received from the PGW during dedicated bearer activation or the value received from the peer-MME/S4-SGSN
- One or more Bearer Control profiles can be associated with a QoS profile for a specific QCI or a range of QCIs

Backward Compatibility

When a QoS Profile is associated to an APN profile for an EPS network then all QoS parameter configurations are taken from the QoS profile and override the APN profile QoS configurations. However, if there is no QoS profile for the given APN in EPS network, then QoS control falls back to the QoS configuration contained in the APN profile.

Flow for 4G QoS Control on Subscribed QoS Received from HSS

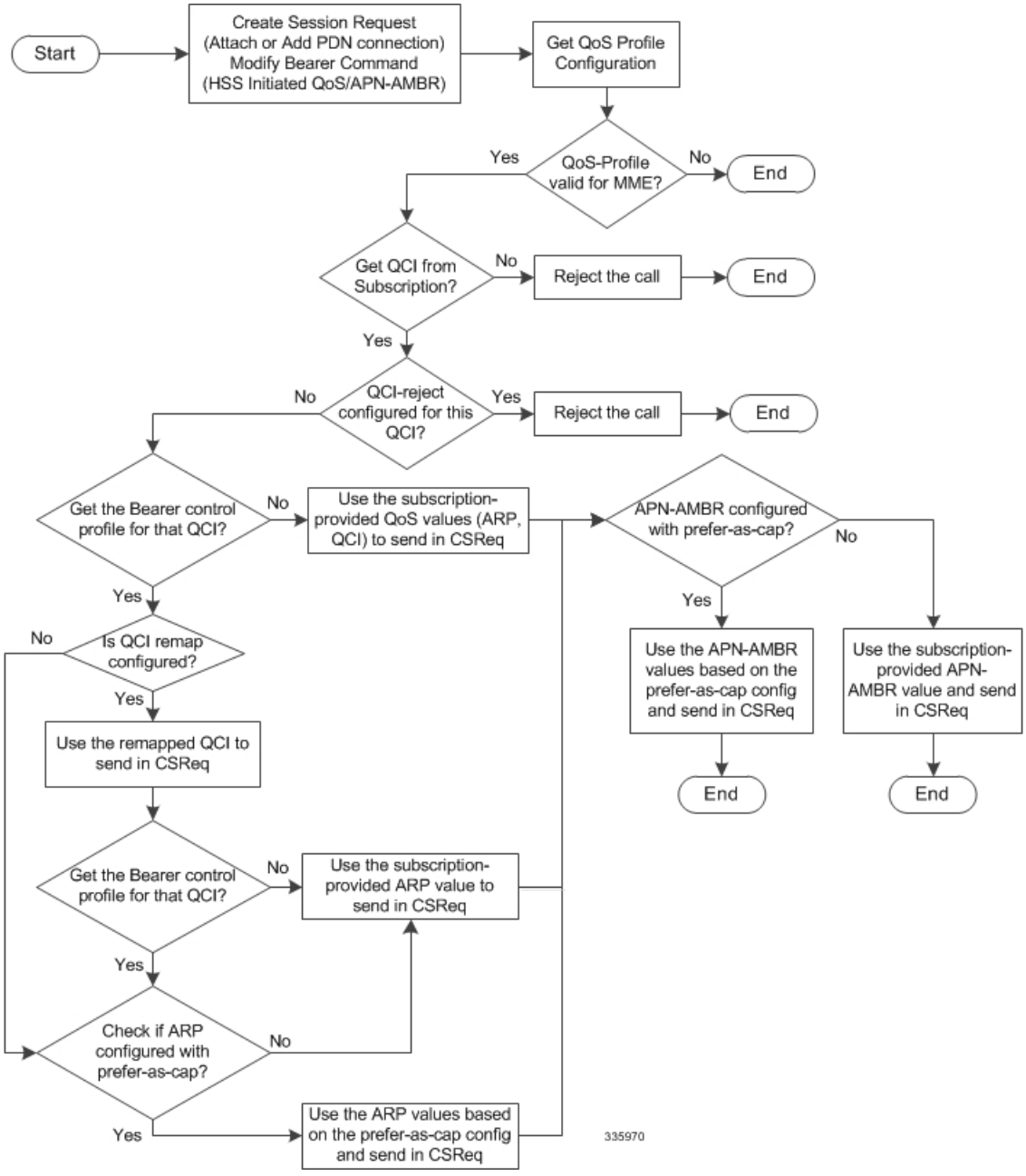
With this feature, the MME can override the EPS QoS profile (QCI, ARP) and APN-AMBR UL/DL received from the HSS, before applying the QoS to a Default Bearer (to be established or modified due to HSS). The overridden EPS QoS is sent in a Create Session Request message for either an Attach or an Additional PDN Connectivity procedure or in a Modify Bearer Command message in the case of an HSS-initiated QoS modification procedure. The following controls are available in MME QoS profile and Bearer Control profile for default bearers:

- Reject any default/dedicated bearers based on QCI

- Apply QCI Remapping
- Use operator-provided configured values for ARP (PL/PCI/PVI) and APN-AMBR instead of subscription or the minimum of the two (operator-provided and HSS) or reject if subscription exceeds operator-provided configured values.

The following diagram illustrates how QoS control is applied after QoS data is received from the HPLMN HSS over the S6a interface.

Figure 37: Flow for 4G QoS Control on Subscribed QoS Received from HSS



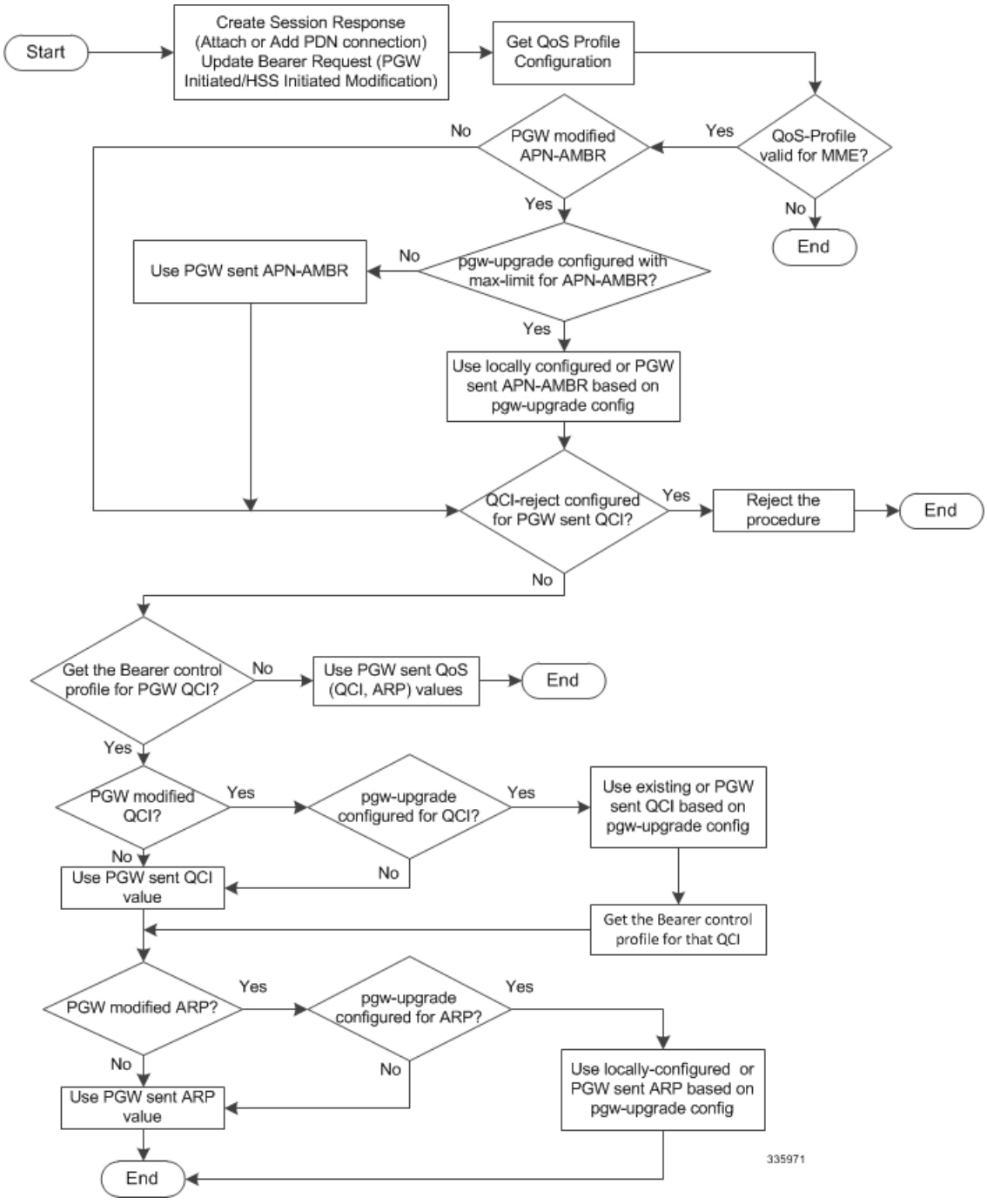
Flow for 4G QoS Control on QoS Received from PGW for non-GBR Default and Dedicated Bearers

The MME can control EPS Bearer QoS (QCI, ARP) and APN-AMBR UL/DL that is received from the PGW (via SGW) in a Create Session Response or a Create/Update Bearer procedure that has been initiated by the PGW. The QoS control is applied and the resultant QoS is sent towards the UE in E-RAB modify message. The following controls are available in MME QoS profile or Bearer Control profile for default/dedicated bearers:

- If QCI provided by the PGW is in the QCI-reject list, reject the procedure.
- Apply QCI Remapping (only for Create Bearer procedure)
- Use operator-provided values for ARP (PL/PCI/PVI) and APN-AMBR instead of PGW values or the minimum of the two (operator-provided and PGW) or reject if PGW provided value exceeds operator-provided values.

The following diagram illustrates how QoS control is applied after QoS data is received from the HPLMN PGW during Create Session Response or Update Bearer Request:

Figure 38: Flow for 4G QoS Control on QoS Received from PGW for non-GBR Default and Dedicated Bearers



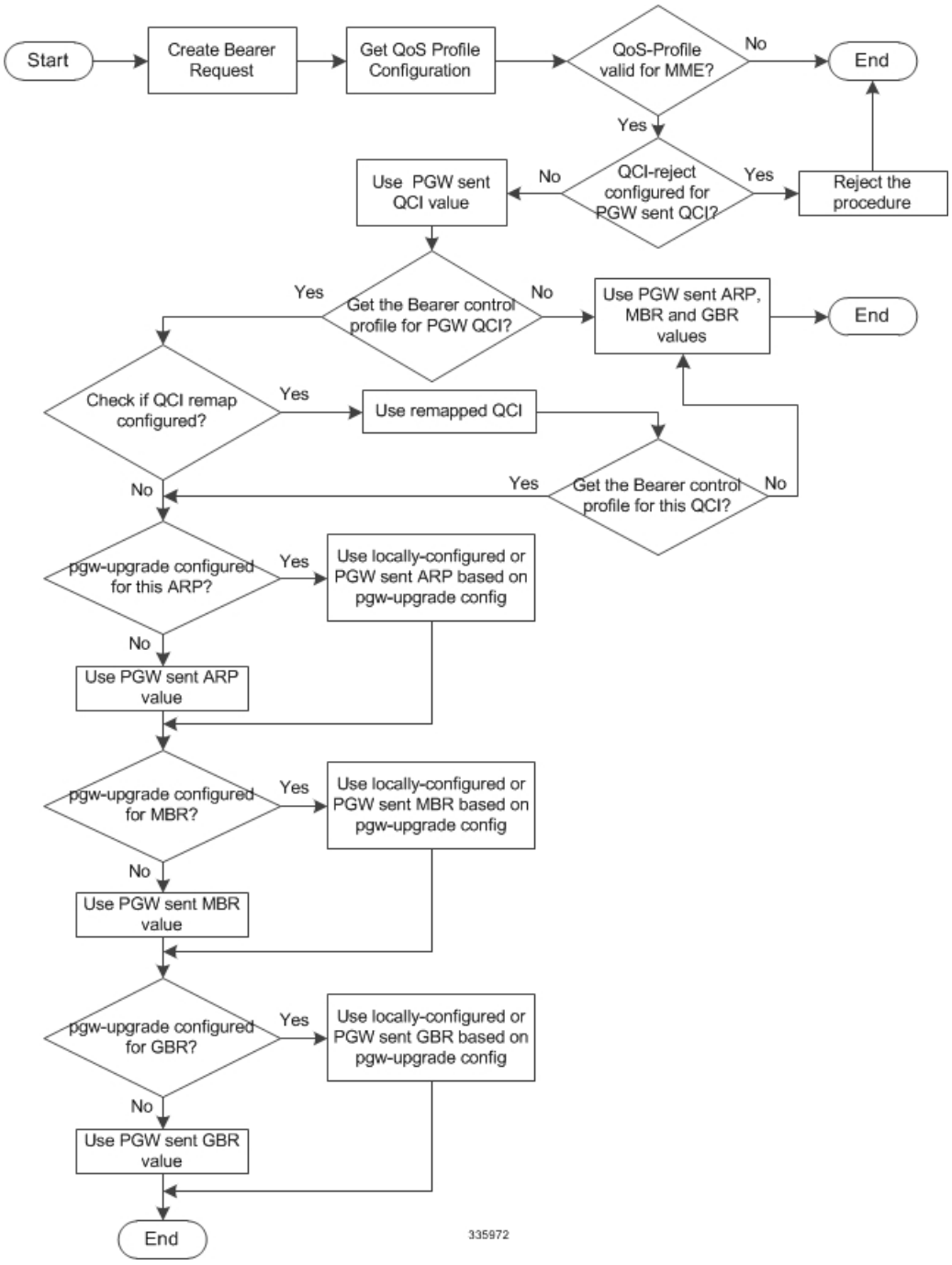
Flow for 4G QoS Control on QoS Received from PGW for GBR Dedicated Bearers

The MME can also control the EPS Bearer QoS (QCI, ARP) and MBR/GBR UL/DL received from the PGW (via SGW) in Create/Update Bearer procedures initiated by the PGW. The QoS control is applied and the resultant QoS is sent towards the UE in an E-RAB Setup/Modify message. The following controls are available in MME QoS profile or Bearer Control profile for dedicated bearers:

- If QCI provided by the PGW is in the QCI-reject list, reject the procedure.
- Apply QCI Remapping (only for Create Bearer procedure)
- Use operator-provided values for ARP (PL/PCI/PVI), MBR and GBR instead of PGW values or the minimum of the two (operator-provided and PGW) or reject if PGW provided value exceeds operator-provided values.

The following diagram illustrates how QoS control is applied after QoS data is received from the HPLMN PGW during Create Bearer Request:

Figure 39: Flow for 4G Control on QoS Received from PGW for GBR Dedicated Bearers



Limitations

- Currently, 4G QoS controls are not applied during hand-off scenarios for dedicated bearers.
- Bearer-level QoS parameters are part of the Bearer Control profile, which is selected based on QCI. If subscription does not provide QCI, then the Bearer Control profile lookup fails resulting in Attach failure.

Standards Compliance

The QoS profile functionality complies with the following standard:
3GPP TS 23.401 v 12.0.0, Section 4.7.2.1

Configuring QoS Profile and Bearer Control Profile

There are multiple components that need to be configured to take full advantage of all aspects of this feature:

Important During configuration, to avoid the requirement to enter **-noconfirm** each time you create an entity (e.g., a profile), enter **autoconfirm** from the Global Configuration mode.

Creating the QoS Profile

This command is now available for the use of the MME in the Global Configuration mode. This command enables the operator to create and configure an instance of a QoS profile for the MME.

configure
quality-of-service-profile *qos_profile_name*
end
Notes:

- *qos_profile_name* - The defined value identifies the name of the QoS profile being created for the MME. The name must be an alphanumeric string of 1 through 100 characters and we recommend that the profile name be unique for the system. This profile name will be needed for other configuration tasks. The system enters the QoS Profile configuration mode and presents the following prompt: [local]*host_name*(quality-of-service-profile-*qos_profile_name*)#.
- Multiple QoS parameters can be configured for the QoS profile. Refer to the *QoS Profile* section of the *Command Line Interface Reference* for command information.

Creating the Bearer Control Profile

This command is new in the Global Configuration mode. This command enables the operator to create and configure an instance of a Bearer Control profile as part of the MME QoS Profile feature.

configure
bearer-control-profile *bc_profile_name*
end
Notes:

- *bc_profile_name* - The defined value identifies the name of the Bearer Control profile being created for the MME. The name must be an alphanumeric string of 1 through 64 characters and we recommend that the profile name be unique for the system. This profile name will be needed for other configuration tasks. The system enters the Bearer Control Profile configuration mode and presents the following prompt: [local]*host_name*(bearer-control-profile-*bc_profile_name*)#.
- The Bearer Control Profile configuration mode provides commands to configure QoS parameters for dedicated bearers (see **dedicated-bearer** section below) and for default bearers (see **default-bearer** section below.
- Bearer level parameters such as ARP-PL, ARP-PVI, ARP-PCI, MBR, GBR, remap QCI value can be configured here independently for default/dedicated bearer along with the action to be taken, such as prefer-as-cap or pgw-upgrade.. Bearer Control profile can be applied for specific QCIs or range of QCIs.

Mapping QCI or QCI Range to the Bearer Control Profile

Use the new **associate** command in Quality of Service Profile configuration mode to associate the Bearer Control profile with the QoS profile and map a specific QCI or a range of QCI to the Bearer Control profile being associated with the QoS profile.

configure
quality-of-service-profile *qos_profile_name*
associate bearer-control-profile *bc_profile_name* **qci** *qci_value* **[to** *end_qci_value* **]**
remove associate bearer-control-profile *bc_profile_name*
end
Notes:

- *qos_profile_name* - Identifies the name of the QoS profile.
- *bc_profile_name* - Identifies the name of the Bearer Control profile being associated with the QoS profile.
- **qci** - Identifies either a specific QoS class identifier (QCI) or a range of QCI:
  - *qci_value* - Enter an integer from 1 through 9 to identify a specific QCI.

  - **to** *end_qci_value* - Type "to" and then enter an integer from 2 through 9 that is greater than the QCI value entered for the beginning of the range.

- A specific QCI cannot be associated to more than one bearer control profile. The QCI of the bearer is used to identify the applicable bearer control profile.
  - For dedicated bearer, the QCI of bearer is initially determined by the QCI value received from PGW during dedicated bearer activation or the value received from peer MME/S4-SGSN.
  - For default bearer, the QCI of bearer is initially determined by the subscription from HSS or the value received from peer MME/S4-SGSN during inbound relocation.

- To delete the Bearer Control profile association with the QoS profile, issue the following command: **remove associate bearer-control-profile** *bc_profile_name*

Earlier, MME rejected SRVCC procedures if a QCI value is not received from the subscription when a QoS profile is available. From Release 20 onwards, a new CLI **qci-when-missing-in-subscription** is added to the Quality of Service Profile Configuration mode to assign a default QCI value when a QCI value is not received from the subscription. If this CLI is enabled, the configured QCI value is used as a default value for an available QoS profile.

A default QCI value can be assigned using the following configuration:

configure
  quality-of-service-profile *profile_name*
    [remove] qci-when-missing-in-subscription *qci_value*
    end

Note

- By default, this command is not enabled.
- **remove** disables its following configuration.
- **qci-when-missing-in-subscription** is used to assign a default QCI value when no value is received from the subscription for an available QoS profile.
- *qci_value* in this configuration is considered as a default QCI value. The QCI value accepted is either a Standard QCI value or Operator Specific value. The Standard QCI values range from 1 to 9, and new Standard QCI values - 65, 66, 69 and 70. The Operator Specific values range from 128 to 254. The configuration does not accept any other value apart from the ones mentioned above. For more information on Operator Specific QCI values, refer to *Operator Specific QCI* chapter in the *MME Administration Guide.*

Configuring Rejection of Bearer Establishment per QCI

Use the new **qci-reject** command in Quality of Service Profile configuration mode to identify a specific QCI or a range of QCI for which the MME must reject bearer establishment or modification.

configure
  quality-of-service-profile *qos_profile_name*
    qci-reject { default-bearer | dedicated-bearer } qci *qci_value* **[to** *end_qci_value* **]**

remove qci-reject
end

Notes:

- *qos_profile_name* - Identifies the name of the QoS profile.
- **dedicated-bearer qci** - Identifies either a specific QoS class identifier (QCI) or a range of QCI for the dedicated-bearer:
  - *qci_value* - Enter an integer from 1 through 9 to identify a specific QCI.
  - **to** *end_qci_value* - Type "to" and then enter an integer from 2 through 9 that is greater than the QCI value entered for the beginning of the range.
- **default-bearer qci** - Identifies either a specific QoS class identifier (QCI) or a range of QCI for the default-bearer:
  - *qci_value* - Enter an integer from 5 through 9 to identify a specific QCI.
  - **to** *end_qci_value* - Type "to" and then enter an integer from 6 through 9 that is greater than the QCI value entered for the beginning of the range.
- The MME can reject default-bearers and dedicated-bearers based on QCI received from the subscription or the peer-MME/S4-SGSN during inbound relocation or the Create Session Response / Update Bearer Request / Create Bearer Request procedure.
- To delete the QCI rejection configuration issue the following command:
  remove qci-reject

Configuring APN-AMBR Capping

Use the **apn-ambr** command in Quality of Service Profile configuration mode to set local values for capping type and action to be taken for APN-AMBR.

configure
quality-of-service-profile *qos_profile_name*
apn-ambr max-ul *max_ul_val* **max-dl** *max_dl_val* **{ pgw-upgrade | prefer-as-cap } { local | minimum | rej-if-exceed }**
remove apn-ambr
end

Notes:

- This keyword **max-ul** sets the local value for the maximum uplink bitrate. *max_ul_val* must be an integer from 0 through 1410065408.
- This keyword **max-dl** sets the local value for the maximum downlink bitrate. *max_dl_val* must be an integer from 0 through 1410065408.
- This command sets the QoS capping mechanism to be applied for APN-AMBR received from HSS/PGW/peer-node. One or both **prefer-as-cap** and/or **pgw-upgrade** must be configured to override the default behavior, which is to accept the received value from the HSS/peer-node/PGW.
- **prefer-as-cap** - This keyword configures the capping that is applied on the subscription value received from the HSS or the value received from the peer-node (MME/S4-SGSN) during inbound relocation. One of the following actions must be configured under **prefer-as-cap** -- Note that the resulting value is

used for the QoS parameter and sent in the Create Session Request or the Modify Bearer Command (in case of HSS-initiated QoS/APN-AMBR modification) message:

- **local** - The configured local value will be used.
- **minimum** - The minimum (lowest) value of the configured local value or the HSS-provided value will be used.
- **reject-if-exceed** - The request/procedure is rejected if the HSS-provided value exceeds the configured local value.

- **pgw-upgrade** - This keyword configures the QoS capping to be applied on the values received from the PGW during Attach / PDN-connectivity / Bearer-creation / Bearer-modification procedures. One of the following actions must be configured under **pgw-upgrade** -- Note that the resulting value is used for the QoS parameter and sent to the UE:
  - **local** - The configured local value will be used.
  - **minimum** - The minimum (lowest) value of the configured local value or the PGW-provided value will be used.
  - **reject-if-exceed** - The request/procedure is rejected if the PGW-provided value exceeds the configured local value.

- To delete the APN-AMBR capping configuration issue the following command:
  remove apn-ambr

Configuring ARP / GBR / MBR / QCI Capping for Dedicated/Default Bearers

The **dedicated-bearer** and **default-bearer** commands, in the Bearer Control Profile configuration mode, configure the QoS control parameters separately for the default-bearers and dedicated-bearers. The operator-provided values are configured for ARP-PL, ARP-PCI, ARP-PVI, MBR, GBR, and QCI, along with their prefer-as-cap or pgw-upgrade capping

configure
bearer-control-profile *bc_profile_name*
dedicated-bearer { arp { preemption-capability | preemption-vulnerability | priority-level } pgw-upgrade | gbr gbr-up *gbr_up_value* **gbr-down** *gbr_down_value* **pgw-upgrade | mbr mbr-up** *mbr_up_value* **mbr-down** *mbr_down_value* **pgw-upgrade| qci { remap | pgw-upgrade { local | minimum | rej-if-exceed } } }**
default-bearer { arp { preemption-capability | preemption-vulnerability | priority-level } { prefer-as-cap | pgw-upgrade } { local | minimum | rej-if-exceed } | qci { remap | pgw-upgrade { local | minimum | rej-if-exceed } } }
remove { dedicated-bearer | default-bearer } { arp | gbr | mbr | qci }
end

Notes:

- Repeat the commands with different keywords to configure as many parameters as needed.
- The command **dedicated-bearer** sets the capping for the dedicated-bearer with the following parameters.
- The command **default-bearer** sets the capping for the default-bearer with the following parameters.
- The **arp** keyword configures the allocation and retention priority parameters:

- **preemption-capability** - Enter and integer, either **0** (may) to specify that this bearer may pre-empt other lower priority bearers if required, or **1** (shall-not) to specify that this bearer shall not pre-empt other lower priority bearers.
- **preemption-vulnerability** - Enter an integer, either **0** (pre-emptible) to specify that this bearer is pre-emptible by other high priority bearers, or **1** (not-pre-emptible) to specify that this bearer is not pre-emptible by other high priority bearers.
- **priority-level** - Enter an integer 1 through 15, with 1 as the highest priority, to specify the allocation/retention priority level.

- The **pgw-upgrade** keyword can be included in the command with any of the other keywords. It identifies the capping mechanism to be used when QoS parameters are received from the PGW and the options include:
  - **local** - Instructs the MME to select locally configured values for QoS capping.
  - **minimum** - Instructs the MME to select the lower value, of the two values locally configured or received value, to use as the QoS capping value.
  - **rej-if-exceed** - Instructs the MME to reject the call if the received value exceeds the locally configured value.

- The **prefer-as-cap** keyword identifies the capping mechanism to be used when QoS parameters are received from the HSS and the options include:
  - **local** - Instructs the MME to select locally configured values for QoS capping.
  - **minimum** - Instructs the MME to select the lower value, of the two values locally configured or received value, to use as the QoS capping value.
  - **rej-if-exceed** - Instructs the MME to reject the call if the received value exceeds the locally configured value.

- The **gbr** keyword configures the Guaranteed Bit Rate values. This keyword is only used for the dedicated-bearer configuration.
  - **gbr-up** - Enter an integer from 1 though 256000 to identify the desired uplink data rate in kbps.
  - **gbr-down** - Enter an integer from 1 though 256000 to identify the desired downlink data rate in kbps.

- The **mbr** keyword configures the Maximum Bit Rate values. This keyword is only used for the dedicated-bearer configuration.
  - **mbr-up** - Enter an integer from 1 though 256000 to identify the desired uplink data rate in kbps.
  - **mbr-down** - Enter an integer from 1 though 256000 to identify the desired downlink data rate in kbps.

- The **qci remap** keyword maps an incoming QCI or a range of QCI to a configured QCI or range of QCI. QCI remap is the first configuration that is applied, among the bearer profile configuration, and it is applicable only during Create Session Request and Create Bearer Request procedures. The bearer control profile associated to the remapped QCI value is used for capping the remaining QoS parameters. Enter an integer from 1 through 9.

- Use the following command to delete either the default-bearer or dedicated bearer configuration: **remove { dedicated-bearer | default-bearer } { arp | gbr | mbr | qci }**
- **QoS Computation** - The following explains how the resultant QoS values are derived for the **minimum** and **reject-if-exceed** actions configured under **prefer-as-cap** or **pgw-upgrade**.
  - **QCI**
    - Every standard GBR/non-GBR QCI is associated with a priority level as per 3GPP TS 23.203 v12.10.0, Table 6.1.7.

QCI	Resource Type	Priority
1	GBR	2
2	GBR	4
3	GBR	3
4	GBR	5
5	non-GBR	1
6	non-GBR	6
7	non-GBR	7
8	non-GBR	8
9	non-GBR	9

    - Priority Level 1 has the highest priority and in case of congestion lowest priority level traffic would be the first to be discarded.
    - **minimum**: The QCI with lower priority level will be used.
    - **rej-if-exceed**: If the received QCI has higher priority level than the configured local QCI, then the procedure will be rejected.
  - **ARP Priority Level**
    - ARP Priority level decreases on increasing value (1 to 15). ARP Priority level 1 has the highest priority value.
    - **minimum**: The lower ARP Priority level (i.e. higher value) will be used.
    - **rej-if-exceed**: If the received ARP Priority level is higher (i.e. value is lesser) than the CLI configured local ARP Priority level, then the procedure will be rejected.
  - **ARP-PCI**
    - Pre-emption capability indicator can have either of the following two values, where may (0) > shall-not (1)
      - *may* - specifies that this bearer may pre-empt other lower priority bearers, if required
      - *shall-not* - specifies that this bearer shall-not pre-empt other lower priority bearers.

- Following table indicates the resultant pre-emption capability for the *minimum* prefer-as-cap or pgw-upgrade

Received value	Configured local value	Resultant value to be used
may	may	may
may	shall-not	shall-not
shall-not	may	shall-not
shall-not	shall-not	shall-not

- *rej-if-exceed*: If the received ARP-PCI value is *may* and the configured local value is *shall-not*, then the procedure will be rejected.
- Default value set by MME if not provided by HSS/PGW : *shall-not*

- **ARP-PVI**
  - Pre-emption vulnerability indicator can have either of the following two values, where *not-pre-emptible* (1) > *pre-emptible* (0)
    - *pre-emptible* - specifies that this bearer is pre-emptible by other high priority bearers
    - *not-pre-emptible* - specifies that this bearer is NOT pre-emptible by other high priority bearers
  - Following table indicates the resultant pre-emption vulnerability for the *minimum* prefer-as-cap or pgw-upgrade:

Received value	Configured local value	Resultant value to be used
pre-emptible	pre-emptible	pre-emptible
pre-emptible	not-pre-emptible	pre-emptible
not-pre-emptible	pre-emptible	pre-emptible
not-pre-emptible	not-pre-emptible	not-pre-emptible

  - *rej-if-exceed*: If the received ARP-PVI value is *not-pre-emptible* and the configured local value is *pre-emptible*, then the procedure will be rejected.
  - Default value set by the MME if not provided by the HSS/PGW : *pre-emptible*

- **MBR / GBR**
  - *minimum*:
    - Uplink - The lower of the values, comparing the received values and the configured local value, will be used for APN-AMBR/MBR/GBR.
    - Downlink - The lower value of the received value and configured local value will be used for APN-AMBR/MBR/GBR.

- *rej-if-exceed*: If the received Uplink value is greater than the configured local Uplink value or the received Downlink value is greater than the configured local Downlink value, then the procedure will be rejected.

Verifying the Configuration for the QoS Profile

Use the **show quality-of-service-profile full all | name** *profile_name* command to view the configuration created for the QoS capping:

```
[local]MME# show quality-of-service-profile full all
Quality of Service (QoS) Profile Name    :  mmeQOS1
Quality of Service Capping
  Prefer Type                            :  Not ConfiguredQoS APN-AMBR:
QoS APN-AMBR                             :
  Max uplink                             : 3444
  Max downlink                           : 5266
  prefer-as-cap                          : rej-if-exceed
```

Verifying the Configuration for the Bearer Control Profile

Use the **show bearer-control-profile full all | name** *bcprofile_name* command to view the configuration created for the Bearer Control profile:

```
Bearer Control Profile Name: bcprofile_name
Default Bearer:
  QCI Remap Value : <val>
  QCI pgw-upgrade : local/minimum/rej-if-exceed
  ARP Priority Level : <val>
  prefer-as-cap : local/minimum/rej-if-exceed
  pgw-upgrade : local/minimum/rej-if-exceed
  ARP Preemption Capability : 0/1
  prefer-as-cap : local/minimum/rej-if-exceed
  pgw-upgrade : local/minimum/rej-if-exceed
  ARP Preemption Vulnerability: 0/1
  prefer-as-cap : local/minimum/rej-if-exceed
  pgw-upgrade : local/minimum/rej-if-exceed

Dedicated Bearer:
  MBR UP : <val> Kbps MBR DOWN: <val> Kbps
  pgw-upgrade : local/minimum/rej-if-exceed
  GBR UP : <val> Kbps GBR DOWN: <val> Kbps
  pgw-upgrade : local/minimum/rej-if-exceed
  QCI Remap Value : <val>
  QCI pgw-upgrade : local/minimum/rej-if-exceed
  ARP Priority Level : <val>
  pgw-upgrade : local/minimum/rej-if-exceed
  ARP Preemption Capability : 0/1
  pgw-upgrade : local/minimum/rej-if-exceed
  ARP Preemption Vulnerability : 0/1
  pgw-upgrade : local/minimum/rej-if-exceed
```

Associating the QoS Profile with an APN Profile

Use the **associate** command in the APN Profile Configuration Mode to associate the MME's QoS profile with an APN profile. A new option, **eps**, has been provided for the **access-type** keyword to indicate the QoS profile supports 4G/EPS network requirements.

configure
apn-profile *apn_profile_name*
associate quality-of-service-profile *qos_profile_name* **access type eps**
remove associate quality-of-service-profile access type eps
end

Notes:

- *qos_profile_name* This value identifies the name of the QoS profile for the MME. The name must be an alphanumeric string of 1 through 100 characters and we recommend that the profile name be unique for the system.

Important Only one QoS profile for the MME can be associated with a single APN profile.

- The **eps** option for the **access-type** keyword associates the EPS network-type with this QoS profile. Selecting this type is required to enable the MME QoS Profile support functionality.
- To delete the QoS profile association with the APN profile, issue the following command: **remove associate quality-of-service-profile access-type eps**
- For additional information about the **apn-profile** commands and the QoS parameters that can be configured under the APN profile, refer to the section on *APN Profile Configuration Commands* in the *Command Line Interface Reference*.

Important Once the MME's QoS profile is configured, these QoS parameter values override the QoS configurations in the APN profile.

Important The APN profile, hence the QoS profile, will not be valid until the APN profile is associated with an operator policy via the **apn** command . For more information, refer to the *Operator Policy Configurtion Mode* section in the *Command Line Interface Reference*

Verifying the Association Configuration

Use the **show apn-profile full { all | name** *apn_profile_name* **}** to verify the association of the MME's QoS profile with the APN profile. The output of this command will provide information similar to the following:

```
[local]MME# show apn-profile full all
APN Profile Name                                    : apnprof3
Associated Quality of Service Profile Name (EPS)    : MMEqos
  Validity                                          : Invalid
Resolution Priority                                 : dns-fallback
```

Note that the Validity is "Invalid". This will switch to "Valid" once the QoS profile is associated with an APN profile.

Monitoring and Troubleshooting the QoS/Bearer Control Profiles

This section indicates how to troubleshoot the QoS profile and/or the Bearer Control profiles.

The MME sends out the QoS parameters (QCI, ARP, APN-AMBR/MBR, GBR) values based on the configuration from QoS and Bearer Control profiles in the following GTPv2 messages during bearer creation/modification/pdn connectivity/handover procedures:

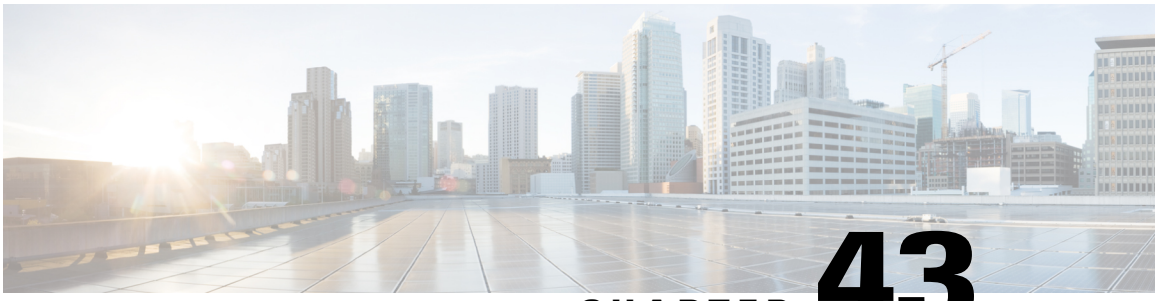
- Create Session Request
- Modify Bearer Command
- Context Response
- Forward Relocation Request

The MME applies the 4G QoS control, based on the configuration from the QoS and Bearer Control profiles, over the received the QoS parameters (QCI, ARP, APN-AMBR or MBR, GBR) from the PGW/Peer node in the following GTPv2 messages during dedicated bearer creation/pgw-initiated QoS modification for default or dedicated bearer:

- Create Session Response or Update Bearer Request or Create Bearer Request

However, if the QoS profile and Bearer Control profile configurations are not enforced in the above messages, verify the following:

- Ensure subscriber-map is configured properly, for the particular set of users and includes an associated operator policy.
- Ensure the APN profile has been created and associated with an operator policy.
- Ensure the QoS profile is created with the access type as "eps" and associated under the APN Profile.
- Ensure the Bearer Control profile is created with required QoS parameters for QCI value received from HSS/PGW and remapped QCI value, if applicable, and ensure the Bearer Control profile is associated under the QoS profile.



CHAPTER 43

S13 Additional IMEI Check

The Cisco MME supports the 3GPP-standard S13 interface towards an Equipment Identity Register (EIR) server. This document describes an MME enhancement to send additional mobile equipment identity checking requests to the EIR server over the S13 interface.

Feature Description

The 'S13 Additional IMEI Check' feature is an MME enhancement to send additional International Mobile Equipment Identity (IMEI) check requests - Mobile Identity check Request (MICR) towards the EIR server over the S13 interface. The additional MICR will include additional information, non-standard AVPs: the Mobile Station International Subscriber Directory Number (MSISDN) and the e-UTRAN Cell Global Identifier (e-CGI). As well, the sending of the additional information will be triggered by various UE procedures (Attach, TAU, and Handover).

Use of the 'S13 Additional IMEI Check' feature is CLI controlled. By default, the Cisco MME supports the 3GPP-standard S13 interface towards an EIR server, which includes sending IMEI check requests containing the two AVPs, IMEI and IMSI, as defined in 3GPP TS 29.272 section 6.2.1.1.

For additional information about the two additional AVPs, please refer to:

- MSISN, the standard Diameter AVP, is defined in section 6.3.2 of 3GPP TS 29.329.
- eCGI is defined in section 7.3.117 of 3GPP TS 29.272.

No feature-specific license is required for this feature.

How It Works

Overview

This 'S13 Additional IMEI Check' feature uses the S13 interface between the MME and the EIR to send an addition al IMEI check request (MICR) containing not the two but four AVPs: IMEI, IMSI, MSISDN, and eCGI.

There is no change in the call flow for this additional MICR. Attach/TAU/HO procedures continue as defined by 3GPP TS 29.272. This means that if this feature is accidentally enabled in the configuration, there is no impact on subscriber call flows.

Existing Diameter statistics (as well as existing bulk statistics) for EIR messaging are still applicable and can be used for monitoring. New statistics have been added to help monitor and troubleshoot this feature (see *Monitoring and Troubleshooting* section).

Operational Criteria

The MME will

- support the S13 Additional IMEI Check functionality, in addition to the default functionality, if the feature is enabled via CLI.
- continue to support the standard IMEI Check Request procedure with the EIR to ensure the MME continues the UE procedure even if the additional MICR procedure with the EIR fails due to error response or timeout.
- send the additional IMEI check request with the additional AVPs only if **all four AVPs** mentioned are available.
- send the additional IMEI check request with the additional AVPs to EIR during any one of the following procedures:
    - Initial Attach
    - GUTI Attach (normal)
    - Inter TAU
    - Periodic TAU
    - Handover (S1, X2)

Operational Requirements

1. The MME must be configured to enable the S13 Additional IMEI Check feature (refer to *Configuration* section).
2. The MME service must be configured to fetch IMEI numbers in advance to use during additional MICR (refer to *Configuration* section).
3. The custom2 dictionary must be selected for the EIR-endpoint under the HSS Peer Service to enable sending of the MSISDN and eCGI values (refer to *Configuration* section).

4 This feature reuses the Mobile Identity check Request (MICR) towards the EIR and adds two AVPs in addition to those defined by the 3GPP standards. So, the receiving EIR needs to be capable of handling and understanding the additional AVPs.

Note Not every EIR is capable of handling the additional AVPs. Hence, it is likely that this feature will not be useful to all operators.

Configuration

All configurations listed below must be completed to enable S13 Additional IMEI Checking functionality.

Enabling S13 Additional IMEI Check Request

A command has been added to the MME Service configuration mode to enable the MME to send additional Mobile Identity check Requests (MICR) towards the EIR over the S13 interface. You must choose at least one triggering UE procedure.

```
configure
    context context_name
        mme-service service_name
            [ no ] s13 additional-id-check { attach | handover | tau }
            end
```

Notes:

- *service_name* - Service names for all services should be unique per chassis.
- **no** - This command filter instructs the MME to remove the specified feature configuration from the MME Service configuration.
- **attach** - This keyword instructs the MME to send additional MICR in response to an Attach procedure.
- **handover** - This keyword instructs the MME to send additional MICR in response to a Handover procedure.
- **tau** - This keyword instructs the MME to send additional MICR in response to a Tracking Area Update procedure.
- The command can be repeated to configure multiple triggering procedures.
- For additional command information, refer to the *Command Line Interface Reference*.

Enabling Fetching of IMEI Number

This feature uses the existing syntax that configures the MME service to query the UE to fetch the IMEI during Attach and Tracking Area Update (TAU) procedures. The fetched IMEI is used in the additional MICR during the Attach and/or TAU procedures.

```
config
 context context_name
  mme-service service_name
   policy attach imei-query-type { imei | imei-sv | none }
```

```
policy tau imei-query-type { imei | imei-sv | none }
default policy [ attach | tau ] imei-query-type
end
```

Notes:

- *service_name* - Service names for all services should be unique per chassis.
- **policy attach imei-query-type** - This command string configures the IMEI query type during UE Attach:
  - **imei :** Specifies that the MME is required to fetch the UE's International Mobile Equipment Identity (IMEI).
  - **imei-sv:** Specifies that the MME is required to fetch the UE's International Mobile Equipment Identity - Software Version (IMEI-SV).
  - **none:** Specifies that the MME does not need to query the UE to fetch either the IMEI or IMEI-SV. This is the default setting.
- **default** - Including this command filter returns the command to its default setting of 'none' for **imei-query-type**.
- For additional command information, refer to the *Command Line Interface Reference*.

Enabling custom2 Dictionary as EIR End-point

Use the following syntax to select the 'custom2' dictionary for the EIR end-point, under the HSS-Peer service configuration, to send MSISDN and eCGI values in the additional MICR.

```
config
  context context_name
    hss-peer-service service_name
      diameter hss-dictionary dictionary eir-dictionary custom2
      default diameter hss-dictionary eir-dictionary
    end
```

Notes:

- *context_name* - It is not required to configure the MME and HSS-Peer services to be in the same context.
- *service_name* - Service names for all services should be unique per chassis.
- **hss-dictionary** *dictionary* - This keyword identifies the dictionary to be used for the HSS Peer Service. Enter the name of the dictionary to be used as the HSS Diameter dictionary.
- **eir-dictionary** - This keyword specifies that an Equipment Identity Register (EIR) dictionary is to be used in conjunction with the HSS Diameter dictionary.
- **custom2** - This keyword selects the **custom2** dictionary, created for the MME's S13 Additional IMEI Check feature, to be used as the EIR dictionary.
- **default** - This command filter instructs the MME to reset the HSS Diameter dictionary and the EIR dictionary to the **standard** dictionary.
- For additional command information, refer to the *Command Line Interface Reference*.

Monitoring and Troubleshooting

Verifying Configuration

Use the following show command, from the Exec mode, to verify the configuration for this feature. The output generated by this command will look similar to the following to indicate the features configuration:

show mme-service name *service_name*

```
s13-additional-id-check :
  Attach: Enabled/Disabled
  TAU: Enabled/Disabled
  Handover: Enabled/Disabled
```

Monitoring Additional IMEI Check Request-related Statistics

Use the following show command, from the Exec mode, to use the monitoring statistics created for this feature. The output generated by this command will look similar to the following:

show mme-service statistics mme-service *service_name*

```
S13 statistics:
 Additional ME Identity Check Procedures (Attach):
  Requests: 0    Answer : 0
  Success : 0   Failure : 0
  Timeout : 0

 Additional ME Identity Check Procedures (TAU):
  Requests: 0    Answer : 0
  Success : 0   Failure : 0
  Timeout : 0

 Additional ME Identity Check Procedures (Handover):
  Requests: 0    Answer : 0
  Success : 0   Failure : 0
  Timeout : 0
```

Monitoring Additional IMEI Check Request-related Bulk Statistics

The following bulk statistics have been created in the MME schema to monitor additional IMEI check functions:

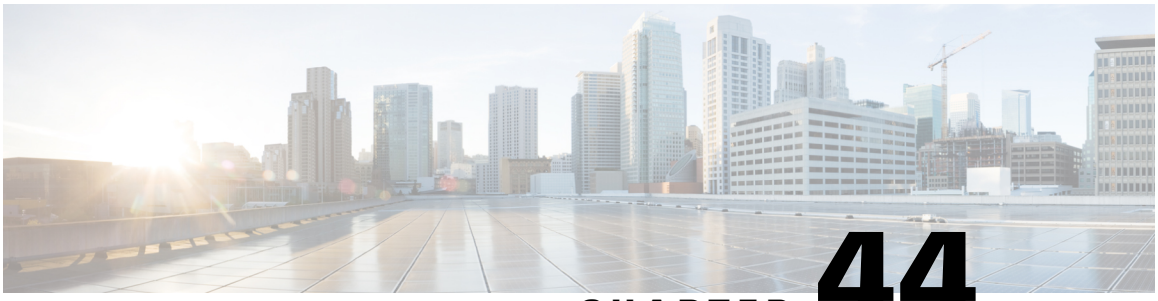
- msg-addtnl-mic-req
- msg-addtnl-mic-ans
- msg-addtnl-mica-success
- msg-addtnl-mica-failure
- msg-addtnl-mica-timeout

Monitoring Default IMEI Check Request Functionality

The default functionality is not new. You can use the existing bulk statistics in the HSS schema for tracking the MICR messaging for the default MICR functionality:

- msg-mic-req
- msg-mic-ans

- msg-micr-retries
- msg-mica-timeout
- msg-mica-drop



CHAPTER 44

Selective Authentication

This chapter describes configuration of Selective Authentication of the UE on the MME is based on time and frequency of access attempts.

Feature Description

The MME performs UE authentication on receiving NAS requests. Authentication procedures can be defined for Attach procedures, Service requests and Tracking Area Update (TAU) procedures. These authentication procedures increase signaling towards the RAN and HSS. Selective Authentication is adopted to reduce signaling traffic towards the RAN and HSS. Selective Authentication is achieved by implementing frequency and periodicity based authentication of UE.

In a frequency-based selective authentication scenario the UE is authenticated based on configured frequency of access attempts. The configured frequency specifies the access-attempts per-UE and not across UEs. For example if the configured frequency is "n", the UE is authenticated for every n^{th} NAS request received. The decision to authenticate is based on every n^{th} request and not based on 'n' requests since last authentication. Where the n^{th} request is equal to a multiple of n. (for example if n = 2, it will be 2,4,6,8 and so on)

In a periodicity-based selective authentication scenario the UE is authenticated based on configured periodicity. For example if the configured periodicity is "t", the UE is authenticated at every "t" minutes.

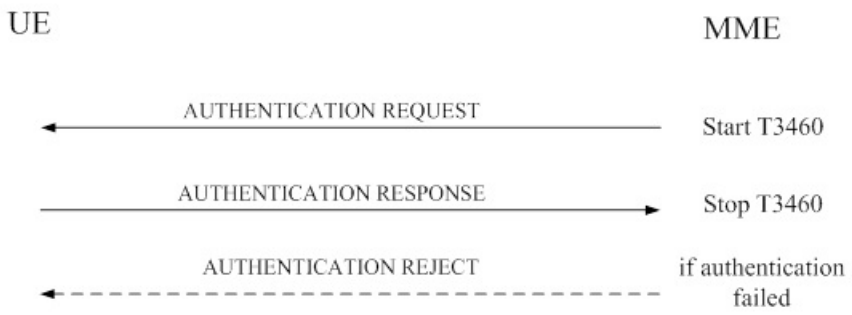
The frequency-based authentication is independent of the configured periodicity. However, periodicity-based authentication attempts are relative to the last UE authentication time. The last UE authentication attempt time is updated whenever an UE authentication is attempted irrespective of the authentication trigger.

How It Works

Flows

The following diagram illustrates the messages exchanged during network-initiated authentication:

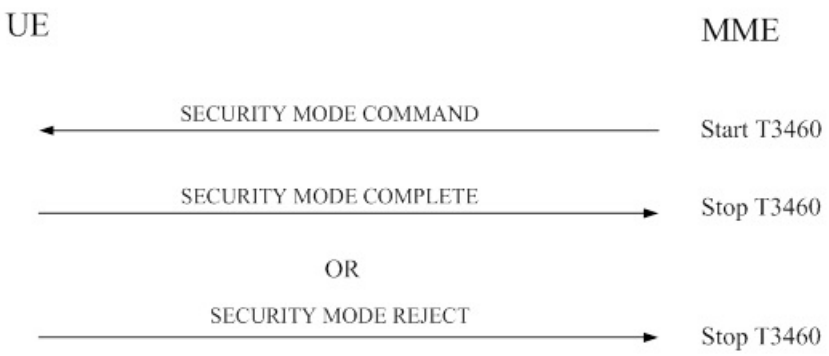
Figure 40: Network-initiated Authentication



1. The MME sends an AUTHENTICATION REQUEST message to the UE. The time duration for the T3460 timer starts. This timer starts when the network initiates the authentication procedure by sending an AUTHENTICATION REQUEST message to the UE and stops upon receipt of the AUTHENTICATION RESPONSE message.
2. The UE responds with an AUTHENTICATION RESPONSE message to the MME, the T3460 timer stops once the MME receives the AUTHENTICATION RESPONSE message.
3. If the authentication procedure fails, the MME sends an AUTHENTICATION REJECT message to the UE.

If the authentication procedure is successful the MME performs the security mode control procedure to utilize the new EPS security context. The following diagram depicts the security mode control procedure:

Figure 41: Security mode control procedure



1. The MME sends a SECURITY MODE COMMAND message to the UE. The time duration for the T3460 timer starts. This timer starts when the network initiates the security mode control procedure by sending a SECURITY MODE COMMAND message to the UE and stops upon receipt of the SECURITY MODE COMPLETE message.
2. The UE responds with a SECURITY MODE COMPLETE message to the MME, the T3460 timer stops once the MME receives the SECURITY MODE COMPLETE message.
3. If the security mode control procedure fails, the MME sends a SECURITY MODE REJECT message to the UE.

Limitations

The MME does not maintain periodicity and frequency across session recovery.

The **frequency** and **periodicity** configured to trigger authentication/GUTI reallocation requires the new session setup message (NAS Attach/TAU) to be processed by the Session Manager instance which has the corresponding MME DB for the subscriber. If the MME DB is not available the **frequency** and **periodicity** triggers will not work. For example, if the mobile identifier in the NAS Attach/TAU message is a foreign GUTI and additional GUTI is not present, the MME does not trigger authentication/GUTI reallocation for the subscriber based on frequency/periodicity.

Configuring Selective Authentication

The following sections describe various procedures to configure selective authentication procedures on the MME.

Selective authentication is not set up by default for any of the following procedures.

Configuring Selective Authentication during Attach Procedures

config
call-control-profile *profile_name*
[remove] authenticate attach [inter-rat] { frequency *frequency*| **periodicity** *duration* **}**
no authenticate attach
end

Notes:

- The **frequency** keyword specifies the frequency that authentication is performed for the Attach Procedures; how many Attach Requests occur before the next authentication. The frequency value is an integer from 1 through 16. If the frequency is set for 12, then the service skips authentication for the first 11 events and authenticates on the twelfth event.
- The **periodicity** keyword specifies authentication periodicity; the number of minutes between the times the MME authenticates the UE. The periodicity value is an integer from 1 through 10800. For example, if the configured periodicity is "20" minutes, the UE is authenticated at every "20" minutes.
- The **remove** command prefix instructs the MME to delete the defined authentication procedures for Attach Requests from the call control profile configuration file.
- The **no** command prefix instructs the MME to disable authentication for the attach procedures.

Configuring Selective Authentication during TAU Procedures

The following command is used to configure the frequency and periodicity for selective UE authentication during TAU Procedures:

config
call-control-profile *profile_name*
[remove] authenticate tau [{ inter-rat | intra-rat | normal | periodic }] [{ frequency *frequency* **| periodicity** *duration* **}]**
no authenticate tau
end

Notes:

- The keyword **inter-rat** specifies authentication to be applied for Inter-RAT TAU.
- The keyword **intra-rat** specifies authentication to be applied for Intra-RAT TAU.
- The keyword **normal** specifies authentication to be applied for normal (TA/LA update) TAU.
- The keyword **periodic** specifies authentication to be applied for periodic TAU.
- The **frequency** keyword specifies how often authentication is performed for tracking area update (TAU) procedures; specifically, how many TAUs occur before the next authentication. The frequency value is an integer from 1 through 16; for example, if the frequency is set for 12, then the service skips authentication for the first 11 events and authenticates on the twelfth event.
- The **periodicity** keyword specifies the period of time, in minutes, between the times the MME authenticates the UE. The periodicity value is an integer from 1 through 10800. For example, if the configured periodicity is "20" minutes, the UE is authenticated every "20" minutes.
- The **remove** command prefix instructs the MME to delete the defined authentication procedures for TAUs from the call control profile configuration file.

- The **no** command prefix disables the authentication procedures specified in the call control profile configuration.

Configuring Selective Authentication during All Events

The following command is used to configure the frequency and periodicity for selective UE authentication for all events (Attach or TAU):

config
call-control-profile *profile_name*
[remove] authenticate all-events [{ frequency *frequency* **| periodicity** *duration* **}]**
no authenticate all-events
end

Notes:

- The **frequency** keyword sets how often authentication is performed for any event. The frequency value is an integer from 1 through 16 and if set for 5, then authentication is not done till the 5th event.
- The **periodicity** keyword instructs the MME how many minutes to wait between each UE authentications. The periodicity value is an integer from 1 through 10800.
- The **remove** command prefix instructs the MME to delete the defined authentication procedures for all events from the call control profile configuration file.
- The **no** command prefix instructs the MME to disable authentication for all events.

Configuring Selective Authentication during Service Requests

The following command is used to configure the frequency and periodicity for selective UE authentication for all Service Requests:

config
call-control-profile *profile_name*
[remove] authenticate service-request [service-type { data | page-response | signaling }] [frequency *frequency* **| periodicity** *duration* **}]**
no authenticate service-request
end

Notes:

- The keyword **service-type** specifies the service-type classification.
- The keyword **data** specifies service-type for data service requests.
- The keyword **page-response** service-type for service requests in response to paging.
- The keyword **signaling** specifies service-type for service requests due to other signaling.
- The **frequency** keyword sets how often (frequency) UE authentication occurs. The frequency value must be an integer from 1 through 16; and if the frequency is set for 12, then the service skips authentication for the first 11 events and authenticates on the twelfth event.
- The **periodicity** keyword defines the amount of time (in minutes) between UE authentications. The periodicity value must be an integer from 1 through 10800 minutes; for example, if the configured periodicity is "20" minutes, the UE is authenticated every "20" minutes.

- The **remove** command prefix instructs the MME to delete the Service Request authentication procedures specified in the call control profile configuration.
- The no command prefix instructs the MME to disable the Service Request authentication procedures.

Monitoring and Troubleshooting Selective Authentication in MME

Selective Authentication Show Command(s) and/or Outputs

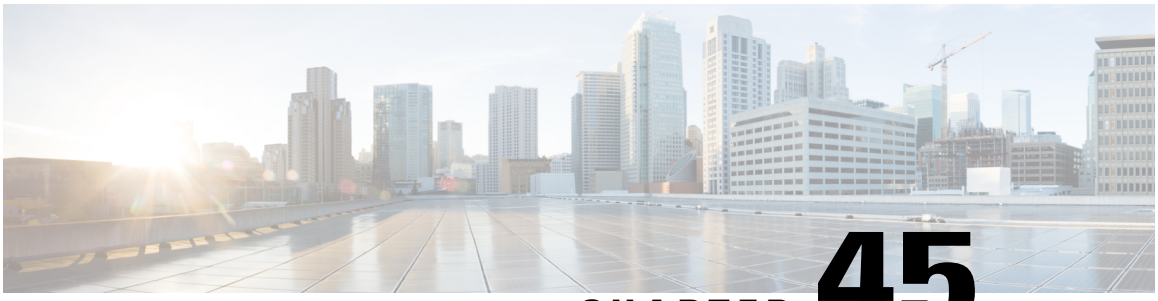
This section provides information regarding show commands and/or their outputs in support of the Selective Authentication feature in MME.

show call-control-profile full all

The following fields show output to illustrate the configured Selective Authentication parameters:

- Authentication All-Events ANY (UMTS/GPRS/EUTRAN) Frequency
- Authentication All-Events ANY (UMTS/GPRS/EUTRAN) Frequency Value
- Authentication All-Events ANY (UMTS/GPRS/EUTRAN) Periodicity
- Authentication All-Events ANY (UMTS/GPRS/EUTRAN) Periodicity Value
- Authentication Attach ANY Frequency
- Authentication Attach ANY (UMTS/GPRS/EUTRAN) Frequency Value
- Authentication Attach ANY Periodicity
- Authentication Attach ANY Periodicity Value
- Authentication Attach Inter-rat ANY (UMTS/GPRS/EUTRAN) Frequency
- Authentication Attach Inter-rat ANY (UMTS/GPRS/EUTRAN) Frequency Value
- Authentication Attach Inter-rat ANY Periodicity
- Authentication Attach Inter-rat ANY Periodicity Value
- Authentication Service Req Frequency
- Authentication Service Req Frequency Value
- Authentication Service Req Periodicity
- Authentication Service Req Periodicity Value
- Authentication Service Req Data Frequency
- Authentication Service Req Data Frequency Value
- Authentication Service Req Data Periodicity
- Authentication Service Req Data Periodicity Value

- Authentication Service Req Signaling Frequency
- Authentication Service Req Signaling Frequency Value
- Authentication Service Req Signaling Periodicity
- Authentication Service Req Signaling Periodicity Value
- Authentication Service Req Page Response Frequency
- Authentication Service Req Page Response Frequency Value
- Authentication Service Req Page Response Periodicity
- Authentication Service Req Page Response Periodicity Value
- Authentication TAU Frequency
- Authentication TAU Frequency Value
- Authentication TAU Periodicity
- Authentication TAU Periodicity Value
- Authentication Inter-RAT TAU Frequency
- Authentication TAU Frequency Value
- Authentication TAU Inter-rat Periodicity
- Authentication TAU Inter-rat Periodicity Value
- Authentication Intra-RAT TAU Frequency
- Authentication Intra-RAT TAU Frequency Value
- Authentication TAU Intra-rat Periodicity
- Authentication TAU Intra-rat Periodicity Value
- Authentication Normal TAU Frequency
- Authentication Normal TAU Frequency Value
- Authentication TAU Normal Periodicity
- Authentication TAU Normal Periodicity Value
- Authentication Periodic TAU Frequency
- Authentication Periodic TAU Frequency Value
- Authentication TAU Periodic Periodicity
- Authentication TAU Periodic Periodicity Value



CHAPTER 45

Session Tracing

Session Tracing allows an operator to trace subscriber activity at various points in the network and at various levels of detail in an EPS network. This chapter provides information on how the MME implements subscriber Session Tracing functionality in the LTE service.

Feature Description

The Session Tracing feature provides a 3GPP standards-based subscriber session-level trace function for call debugging and testing new functions and access terminals in an LTE environment.

In general, the Session Trace 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.

The EPC network entities like MME, S-GW, P-GW support 3GPP standards based session-level trace capabilities to monitor all call control events on the respective monitored interfaces including S6a, S1-MME and S11 on MME, S5, S8, S11 at S-GW and S5 and S8 on P-GW. The trace can be initiated using multiple methods:

- Management initiation via direct CLI configuration
- Management initiation at HSS with trace activation via authentication response messages over S6a reference interface
- Signaling-based activation through signaling from subscriber access terminal

Important Once the trace is provisioned it can be provisioned through the access cloud via various signaling interfaces.

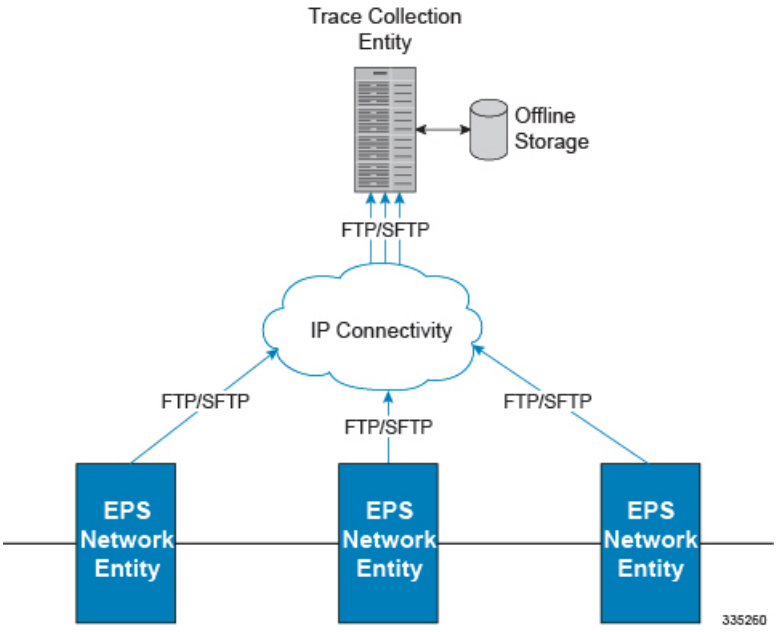
The session level trace function consists of trace activation followed by triggers. The time between the two events is where the EPC network element buffers the trace activation instructions for the provisioned subscriber

in memory using camp-on monitoring. Trace files for active calls are buffered as XML files using non-volatile memory on the local dual redundant hard drives on the chassis. The trace depth defines the granularity of data to be traced. Six levels are defined including maximum, minimum and medium with ability to configure additional levels based on vendor extensions.

Important Only maximum trace depth is supported in the current release.

The following figure shows a high-level overview of the session-trace functionality and deployment scenario:

Figure 42: Session Trace Function and Interfaces



All call control activity for active and recorded sessions is sent to an off-line Trace Collection Entity (TCE) using a standards-based XML format over a FTP or secure FTP (SFTP) connection.

Note: In the current release the IPv4 interfaces are used to provide connectivity to the TCE. trace activation is based on IMSI or IMEI.

Supported Functions

This section provides the list of supported functionality of this feature support:

- Support to trace the control flow through the access network.
  - Trace of specific subscriber identified by IMSI
  - Trace of UE identified by IMEI(SV)
- Ability to specify specific functional entities and interfaces where tracing should occur.
- Scalability and capacity

    - Support up to 32 simultaneous session traces per MME
    - Each MME is equipped with a storage buffer of size 40 MB to collect trace files locally
- Statistics and State Support
- Session Trace Details
- Management and Signaling-based activation models
- Trace Parameter Propagation
- Trace Scope (EPS Only)
    - MME: S10, S11, S13, S1-MME, S3, S6A
    - S-GW: S4, S5, S8, S11, Gxc
    - PDN-GW: S2a, S2b, S2c, S5, S6b, Gx, S8, SGi
- Trace Depth: Maximum, Minimum, Medium (with or without vendor extension)
- XML Encoding of Data as per 3GPP standard 3GPP TS 32.422 V8.6.0 (2009-09)
- Trace Collection Entity (TCE) Support
    - Active pushing of files to the TCE
    - Passive pulling of files by the TCE
- 1 TCE support per context
- Trace Session Recovery after Failure of Session Manager

Standards Compliance

Support for the following standards and requests for comments (RFCs) have been added with this interface support:

- 3GPP TS 32.421 V10.5.0: 3rd Generation Partnership Project Technical Specification Group Services and System Aspects Telecommunication management Subscriber and equipment trace: Trace concepts and requirements (Release 10)
- 3GPP TS 32.422 V10.5.0: 3rd Generation Partnership Project Technical Specification Group Services and System Aspects Telecommunication management Subscriber and equipment trace Trace control and configuration management (Release 10)
- 3GPP TS 32.423 V10.5.0: 3rd Generation Partnership Project Technical Specification Group Services and System Aspects Telecommunication management Subscriber and equipment trace: Trace data definition and management (Release 10)

How Session Tracing Works

This section describes the various functionality involved in tracing subscriber sessions on EPC nodes.

Operation

The session trace functionality is separated into two steps - activation and trigger.

Before tracing can begin, it must be activated. Activation is done either via management request or when a UE initiates a signaled connection. After activation, tracing actually begins when it is triggered (defined by a set of trigger events).

Trace Session

A trace session is the time between trace activation and trace de-activation. It defines the state of a trace session, including all user profile configuration, monitoring points, and start/stop triggers. It is uniquely identified by a Trace Reference.

The Trace Reference id is composed of the MCC (3 digits) + the MNC (3 digits) + the trace Id (3 byte octet string).

Important On a session manager failure, the control activity that have been traced and not written to file will be lost. However, the trace sessions will continue to persist and future signals will be captured as expected.

Trace Recording Session

A trace recording session is a time period in which activity is actually being recorded and traceable data is being forwarded to the TCE. A trace recording session is initiated when a start trigger event occurs and continues until the stop trigger event occurs and is uniquely identified by a Trace Recording Session Reference.

Network Element (NE)

Network elements are the functional component to facilitate subscriber session trace in mobile network.

The term network element refers to a functional component that has standard interfaces in and out of it. It is typically shown as a stand-alone AGW. Examples of NEs are the MME, S-GW, and P-GW.

Currently, subscriber session trace is not supported for co-located network elements in the EPC network.

Activation

Activation of a trace is similar whether it be via the management interface or via a signaling interface. In both cases, a trace session state block is allocated which stores all configuration and state information for the trace session. In addition, a (S)FTP connection to the TCE is established if one does not already exist (if this is the first trace session established, odds are there will not be a (S)FTP connection already established to the TCE).

If the session to be traced is already active, tracing may begin immediately. Otherwise, tracing activity concludes until the start trigger occurs (typically when the subscriber or UE under trace initiates a connection). A failure to activate a trace (due to max exceeded or some other failure reason) results in a notification being sent to the TCE indicating the failure. If the (S)FTP connection is not established with the TCE, the TCE connectivity needs to checked. Nevertheless, the MME continues to send the trace files to the TCE, and tries

to establish an (S)FTP connection. The MME provides a storage buffer of size 40 MB to collect the trace files locally.

Management Activation

The Operator can activate a trace session by directly logging in to the NE and enabling the session trace (for command information, see *Enabling Subscriber Session Trace on EPC Network Element* section below). The NE establishes the trace session and waits for a triggering event to start actively tracing. Depending upon the configuration of the trace session, the trace activation may be propagated to other NEs.

Signaling Activation

With a signaling based activation, the trace session is indicated to the NE across a signaling interface via a trace invocation message. This message can either be piggybacked with an existing bearer setup message (in order to trace all control messages) or by sending a separate trace invocation message (if the user is already active).

Start Trigger

A trace recording session starts upon reception of one of the configured start triggers. Once the start trigger is received, the NE generates a Trace Recording Session Reference (unique to the NE) and begins to collect and forward trace information on the session to the TCE.

List of trigger events are listed in 3GPP standard 3GPP TS 32.422 V8.6.0 (2009-09).

Deactivation

Deactivation of a Trace Session is similar whether it was management or signaling activated. In either case, a deactivation request is received by the NE that contains a valid trace reference results in the de-allocation of the trace session state block and a flushing of any pending trace data. In addition, if this is the last trace session to a particular TCE, the (S)FTP connection to the TCE is released after the last trace file is successfully transferred to the TCE.

Stop Trigger

A trace recording session ends upon the reception of one of the configured stop triggers. Once the stop trigger is received, the NE will terminate the active recording session and attempt to send any pending trace data to the TCE. The list of triggering events can be found in 3GPP standard 3GPP TS 32.422 V8.6.0 (2009-09).

Data Collection and Reporting

Subscriber session trace functionality supports data collection and reporting system to provide historical usage and event analysis.

All data collected by the NE is formatted into standard XML file format and forwarded to the TCE via (S)FTP. The specific format of the data is defined in 3GPP standard 3GPP TS 32.423 V8.2.0 (2009-09)

Trace Depth

The Trace Depth defines what data is to be traced. There are six depths defined: Maximum, Minimum, and Medium all having with and without vendor extension flavors. The maximum level of detail results in the entire control message getting traced and forwarded to the TCE. The medium and minimum define varying subsets of the control messages (specific decoded IEs) to be traced and forwarded. The contents and definition of the medium and minimum trace can be found in 3GPP standard 3GPP TS 32.423 V8.2.0 (2009-09).

Important Only Maximum Trace Depth is supported in the current release.

Trace Scope

The Trace Scope defines what NEs and what interfaces have the tracing capabilities enabled on them. This is actually a specific list of NE types and interfaces provided in the trace session configuration by the operator (either directly via a management interface or indirectly via a signaling interface).

Network Element Details

Trace functionality for each of the specific network elements supported by this functionality are described in this section.

This section includes the trace monitoring points applicable to them as well as the interfaces over which they can send and/or receive trace configuration.

MME

The MME supports tracing of the following interfaces with the following trace capabilities:

Interface Name	Remote Device	Trace Signaling (De)Activation RX	Trace Signaling (De)Activation TX
S1a	eNodeB	N	Y
S3	SGSN	Y	Y
S6a	HSS	Y	N
S10	MME	Y	Y
S11	S-GW	N	Y
S13	EIR	N	N

S-GW

The S-GW supports tracing of the following interfaces with the following trace capabilities:

Interface Name	Remote Device	Trace Signaling (De)Activation RX	Trace Signaling (De)Activation TX
S1-U	eNodeB	Y	N
S4	SGSN	N	N
S5	P-GW (Intra-PLMN)	Y	N
S8	P-GW (Inter-PLMN)	N	N
S11	MME	Y	N
S12	RNC	Y	N
Gxc	Policy Server	Y	N

P-GW

The P-GW supports tracing of the following interfaces with the following trace capabilities:

Interface Name	Remote Device	Trace Signaling (De)Activation RX	Trace Signaling (De)Activation TX
S2abc	Various NEs	N	N
S5	S-GW (Intra-PLMN)	Y	N
S6b	AAA Server/Proxy	Y	N
S8	S-GW (Inter-PLMN)	N	N
Gx	Policy Server	Y	N
SGi	IMS	Y	N

Session Trace Configuration

This section provides a high-level series of steps and the associated configuration examples for configuring the system to enable the Subscriber Session Trace collection and monitoring function on network elements s in LTE/EPC networks.

Important This section provides the minimum instruction set to enable the Subscriber Session Trace functionality to collect session traces on network elements on EPC networks. Commands that configure additional function for this feature are provided in the *Command Line Interface Reference*.

These instructions assume that you have already configured the system level configuration as described in the *System Administration Guide* and specific product Administration Guide.

To configure the system to support subscriber session trace collection and trace file transport on a system:

Step 1 Enable the subscriber session trace functionality with NE interface and TCE address at the Exec Mode level on an EPC network element by applying the example configurations presented in the *Enabling Subscriber Session Trace on EPC Network Element* section.

Step 2 Configure the network and trace file transportation parameters by applying the example configurations presented in the *Trace File Collection Configuration* section.

Step 3 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command save configuration. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Step 4 Verify the configuration of Subscriber Session Trace related parameters by applying the commands provided in the *Verifying Your Configuration* section of this chapter.

Enabling Subscriber Session Trace on EPC Network Element

This section provides the configuration example to enable the subscriber session trace on a system. Enter a command similar to the following in the Exec mode:

session trace subscriber network-element mme template-name *template_name* **{ imei** *imei_id* **| imsi** *imsi_id* **} trace-ref** *trace_ref_id* **collection-entity** *ip_address*

Notes:

- *template_name* specifies the name of the session trace template. This template must be configured by using the **template-session-trace** command in the Global Configuration mode.
- **imsi** *imsi_id* specifies the International Mobile Subscriber Identification Number for the subscriber.
- **imei** *imei_id* specifies the International Mobile Equipment Identification Number for the subscriber.
- **trace-ref** *trace_ref_id* is the configured Trace Id to be used for the present trace collection instance. It is composed of MCC (3 digit)+MNC (3 digit)+Trace Id (3 byte octet string).
- **collection-entity** *ip_address* specifies the IP address of the Trace Collection Entity (TCE) to which the trace file generated will be sent. The IP address must be in IPv4 format.

Configuring a Session Trace Template for the MME

Operators have the option of creating a template for a management trace in configuration mode for the MME. Session traces executed in the Exec mode will use this template. Once created, the template can be associated with different subscribers to trace the interfaces configured in the template.

Important To activate subscriber session traces for specific IMSI/IMEI, the operator must use the Exec mode **session trace subscriber** command specifying a pre-configured template and the IMSI/IMEI, trace reference and TCE address.

To configure a template-session-trace, use the following configuration:

configure
template-session-trace network-element mme template-name *template_name*
interface { all | s10 | s11 | s13 s1mme | s3 | s6a
target-ne { all | enb | pgw | sgwall | sgw } [target-interface [all | s1mme | uu | x2] } } **end**
end

Notes:

- Available **interface** options for MME include:
  - **all:** Sets the trace to be performed on all interfaces from the MME.
  - **s10:** Sets the trace to be performed on the S10 interface between the MME and another MME.
  - **s11:** Sets the trace to be performed on the S11 interface between the MME and the S-GW.
  - **s13:** Sets the trace to be performed on the S13 interface between the MME and the EIR.
  - **s1mme:** Sets the trace to be performed on the S1-MME interface between the MME and the eNodeB.
  - **s3:** Sets the trace to be performed on the S3 interface between the MME and an SGSN.
  - **s6a:** Sets the trace to be performed on the S6a interface between the MME and the HSS.
- **target-ne** initiates tracing towards peer network elements and available options include:
  - **all:** Initiates the trace towards all NEs.
  - **enb:** Initiates the trace towards the eNodeBs.
  - **pgw:** Initiates the trace towards the P-GWs.
  - **sgw:** Initiates the trace towards the S-GWs.
- Available **target-interface** specifies the interface for the selected Network Element for tracing and options for **enb** are as follows:
  - **all:** Identify all interfaces between the MME and eNodeB.
  - **s1mme:** Specifies that the interface where the trace will be performed is the S1-MME interface between the MME and the eNodeB.
  - **uu:** Specifies that the interface where the trace will be performed is the UU interface between the MME and the eNodeB.

- **x2:** Specifies that the interface where the trace will be performed is the X2 interface between the MME and the eNodeB.

- Available **target-interface** options for **pgw** are as follows:
  - **all**
  - **gx:** Specifies that the interface where the trace will be performed is the Gx interface between the P-GW and the PCRF.
  - **s2a:** Specifies that the interface where the trace will be performed is the S2a interface between the PGW and the HSGW.
  - **s2b:** Specifies that the interface where the trace will be performed is the S2b interface between the PGW and an ePDG.
  - **s2c:** Specifies that the interface where the trace will be performed is the S2c interface between the PGW and a trusted, non-3GPP access device.
  - **s5:** Specifies that the interface where the trace will be performed is the S5 interface between the P-GW and the S-GW.
  - **s6b:** Specifies that the interface where the trace will be performed is the S6b interface between the PGW and the 3GPP AAA server.
  - **s8:** Specifies that the interface where the trace will be performed is the S8b interface between the PGW and the S-GW.
  - **sgi:** Specifies that the interface where the trace will be performed is the SGi interface between the PGW and the PDN.

- Available **target-interface** options for **sgw** are as follows:
  - **all**
  - **gxc:** Specifies that the interface where the trace will be performed is the Gx interface between the PGW and the PCRF.
  - **s11:** Specifies that the interface where the trace will be performed is the S11 interface between the MME and the S-GW.
  - **s4:** Specifies that the interface where the trace will be performed is the S4 interface between the S-GW and the SGSN.
  - **s5:** Specifies that the interface where the trace will be performed is the S5 interface between the P-GW and the S-GW.
  - **s8:** Specifies that the interface where the trace will be performed is the S8b interface between the PGW and the S-GW.

Trace File Collection Configuration

This section provides the configuration example to configure the trace fil e collection parameters and protocols to be used to store trace files on TCE through FTP/S-FTP:

configure
session trace subscriber network-element { all | ggsn | mme | pgw | sgw } [collection-timer *dur* **] [tce-mode { none | push transport { ftp | sftp } path** *string* **username** *name* **{ encrypted password** *enc_pw* **] | password** *password* **} }]**
end

Notes:

- *string* is the location/path on the trace collection entity (TCE) where trace files will be stored on TCE. For more information, refer to the session trace command in the *Command Line Interface Reference*.

Verifying Your Configuration

This section explains how to display and review the configurations after saving them in a .cfg file as described in the *System Administration Guide* and also to retrieve errors and warnings within an active configuration for a service.

Important All commands listed here are under Exec mode. Not all commands are available on all platforms.

These instructions are used to verify the Subscriber Session Trace configuration.

Step 1 Verify that your subscriber session support is configured properly by entering the following command in Exec Mode:
show session trace statistics
The output of this command displays the statistics of the session trace instance.

```
Num current trace sessions: 5
Total trace sessions activated:  15
Total Number of trace session activation failures:  2
Total Number of trace recording sessions triggered:  15
Total Number of messages traced:  123
Number of current TCE connections:  2
Total number of TCE connections: 3
Total number of files uploaded to all TCEs:  34
```

Step 2 View the session trace references active for various network elements in an EPC network by entering the following command in Exec Mode:
show session trace trace-summary
The output of this command displays the summary of trace references for all network elements:

```
MME
    Trace Reference:  310012012345
    Trace Reference:  310012012346
SGW
    Trace Reference:  310012012345
    Trace Reference:  310012012346
PGW
    Trace Reference:  310012012347
```

Monitoring and Troubleshooting the Session Trace

The following section describes commands available to monitor Session Trace functionality on the MME.

Session Trace Show Command(s) and/or Outputs

show session trace statistics

On running the above mentioned show command, statistics similar to the following are displayed:

- Number of current trace sessions
- Number of total trace sessions
- Total sessions activated
- Number of activation failures
- Number of sessions triggered
- Total messages traced
- Number of current TCE connections
- Total number of TCE connections
- Total number of files uploaded to all TCEs

show session trace subscriber network-element trace-ref

This command shows detailed information about a specific trace, based on the trace-ref value of the session and network element type. It includes activation time, IMSI, start time, number of trace messages, and total number of files created. It also lists the interfaces that this session trace is configured to track.

The following command displays the summary of a Session Trace for a particular Reference Id

show session trace subscriber network-element mme trace-ref 310012012345

```
Trace Reference:    310012012345
      Activation time:  Fri Jul 10 16:19:10 2009
      IMSI:  0000012345
      Actively Tracing:  yes
      Trace Recording Session Reference:  1
      Recording start time:  Fri Jul 10 16:19:10 2009
      Total number of trace recording sessions triggered:  1
      Total number of messages traced:  32
      Total number of files created:  5
      Traced Interfaces:
            S1mme
            S6a
            S11
      Trace Triggers:
            service-request
            initial-attach
            ue-disconnect
            bearer-activation
            handover
      Target Network Elements:
```

```
SGW
Target Interfaces
     S8b
     S11
```

show session trace tce-summary

This command provides the IP address and index information for all configured TCEs. The following fields are displayed on executing the above command:

```
TCE IP Address:
      Index 1
TCE IP Address:
      Index 5
```

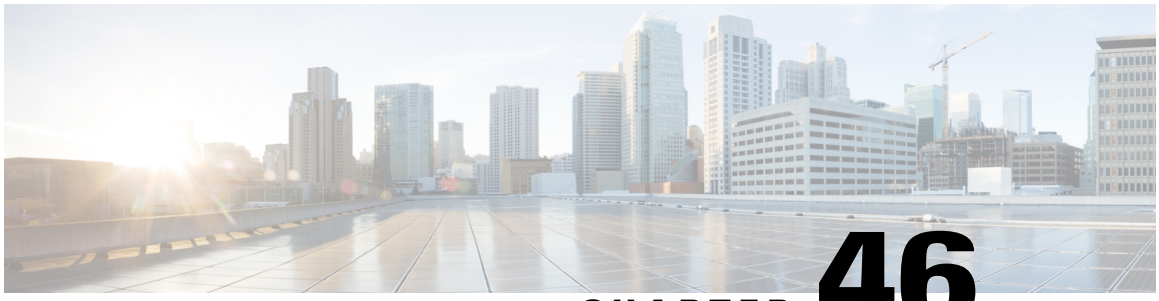
show session trace tce-address

This command provides detailed information about a specific TCE, including IP address, start time, and total number of files uploaded.

The following example displays the summary of a Session Trace for a particular Refernence Id

show session trace tce-address 10.172.1.5 tce-index 5

```
TCE IP Address:    10.172.1.5
      Start time:  Fri Jul 10 16:19:10 2009
      Total number of files uploaded:  12
```



CHAPTER 46

SGW Blacklisting on the MME

This chapter describes how MME blacklists un-accessible and un-responsive SGWs in the following sections:

Feature Description

The SGW Blacklisting is a proprietary feature of StarOS. In this feature, the MME blacklists un-accessible or un-responsive SGWs for a configured time. The MME does not select these blacklisted SGWs during any procedures that requires SGW selection so that there is minimal latency during the procedures. SGW Blacklisting is supported for both Static and Dynamic IP addresses.

To support SGW blacklisting, a new CLI sgw-blacklist is added under the MME Service Configuration mode. When this feature is enabled, SGW blacklisting takes place using the following methods in the MME:

- Node Level Blacklisting
- Session Manager Level Blacklisting

A valid license key is required to enable SGW Blacklisting on the MME. Contact your Cisco Account or Support Representative for information on how to obtain a license.

How It Works

On identifying an unreachable SGW, the SGW is blacklisted for a configured amount of time. The show CLI discussed in the Monitoring and Troubleshooting section displays the expiry timestamp of this SGW, indicating the blacklisting duration. This feature is based on a per mme-service configuration, therefore a separate list to store blacklisted SGWs is created for every mme-service.

During the ATTACH, TAU and Handover procedures, the MME selects an SGW that is not blacklisted. If all SGWs are blacklisted, then the MME attempts to use one of the blacklisted SGWs instead of directly rejecting the call. If the Create Session Response time expires, the call is rejected.

The blacklisted SGWs are completely removed from the MME based on the following configuration changes/execution:

- If the sgw-blacklist configuration is removed – SGW blacklisting feature is disabled.
- If the sgw-blacklist configuration is reconfigured, that is, if the timeout or the msg-timeouts-per-min values are changed.
- If mme-service is stopped; a critical parameter is removed from its configuration.
- If the clear CLI is executed, refer to Monitoring and Troubleshooting section.

Note The MME does not remove the blacklisted SGWs based on any SGW initiated request/response message.

The following functionalities are also included for SGW blacklisting:

- Weight based load distribution with the available SGWs when some of the SGWs are blacklisted.
- Session manager recovery is added to recover node-level blacklisted SGWs.

SGW blacklisting takes place using the following methods in the MME:

Node Level Blacklisting

When no echo response is received from the SGW, a node-level path failure indication is sent to all SESSMGRs.

Based on the node-level path failure indication, the MME blacklists the SGW for the configured time and stores it as a node-level blacklisted type.

Session Manager Level Blacklisting

Along with node-level blacklisting, MME supports blacklisting of SGW based on Create Session Response timeout per SESSMGR instance. The Session Manager Level blacklisting is local to a specific SESSMGR instance and its particular mme-service where the Create Session Response times out.

To avoid broadcasting among SESSMGRs, session manager level blacklisting is not shared among SESSMGRs.

Along with “sgw-blacklist timeout” configuration, "msg-timeouts-per-min” configuration is configured, which is only required for sgmr-level blacklisting. Instead of blacklisting an SGW in the first Create Session Response timeout, the MME blacklists an SGW if the number of Create Session Response timeouts within a minute reaches the configured msg-timeouts-per-minute value. For more information, refer to Configuring SGW Blacklisting on the MME section.

Configuring SGW Blacklisting on the MME

The following CLI configures SGW blacklist timeout value, and the number of Create Session Response timeouts per minute to blacklist an SGW locally in a SESSMGR instance.

The configuration is provided under the MME Service Configuration mode.

```
config
    context context_name
        mme-service service_name
            [ no ] sgw-blacklist timeout timer_value msg-timeouts-per-min number_of_timeouts
            end
```

- **no** disables the SGW Blacklisting configuration.
- **sgw-blacklist** specifies the configurable parameters required for SGW blacklisting.
- **timeout** specifies the period of time the blacklisted SGW cannot be used for call procedures. The timeout value is an integer ranging from 5 to 86400 seconds.
- **msg-timeouts-per-min** configures the number of message timeouts to wait, before blacklisting a SGW locally in a session manager instance. Only Create Session Response timeout is considered. The number of message is an integer ranging from 1 to 5000.
- By default, this configuration is not enabled.

Verifying SGW Blacklisting on the MME

The below given command displays the following new fields that are added to support the SGW Blacklisting feature:

show mme-service sgw-blacklist [mme-service-name *name* **] [smgr-instance** *number* **]**

```
MME service name: mmesvc
    Node-level: 0     Instance-level: 1
    SGW IP              : 192.168.20.2
    Blacklist type      : Sessmgr-level
    Expiry timestamp    : Monday June 13 02:27:57 EDT 2016
    Blacklist time left : 777 seconds
```

Notes:

- **sgw-blacklist** displays information on blacklisted SGWs.
- **mme-service-name** displays node level blacklisted SGWs for a specified mme-service
- **smgr-instance** displays node-level and session manager level blacklisted SGWs for a specific SESSMGR instance.
- Blacklist Type can either be Node level or Sessmgr-level.
- If smgr-instance option is selected, both Node-level and Sessmgr-level blacklisted SGWs are displayed, otherwise only Node-Level blacklisted SGWs are displayed.

Monitoring and Troubleshooting SGW Blacklisting on the MME

SGW Blacklisting Show Command(s) and /or Outputs

This section provides information regarding show commands and their outputs for the SGW blacklisting feature.

show mme-service name *name*

Executing the above command displays the following fields for this feature:

- SGW Blacklist Parameters
- Timeout
    - msg-timeouts-per-min

show mme-service statistics emm-only

Executing the above command displays the following fields for this feature:

```
SGW Selection:
    Blacklisted SGW chosen:  0
```

Notes:

- The SGW Selection specifies the number of times a blacklisted SGW is selected when all SGWs are blacklisted.

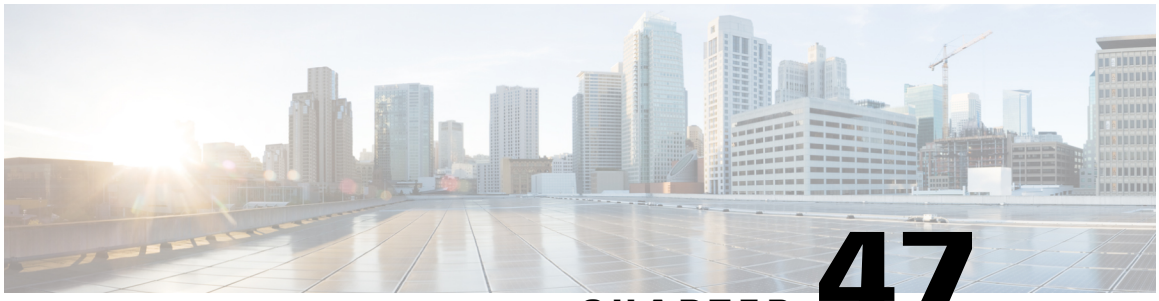
clear mme-service sgw-blacklist [mme-service-name *name*] [sgw-ip]

Executing the above command clears the selected SGW or all blacklisted SGWs from the system.

Notes:

- sgw-blacklist clears the blacklisted SGWs.
- mme-service-name clears the blacklisted SGWs that belong to a particular mme-service.
- sgw-ip clears the specified blacklisted SGW based on the IP address.

A trace level event ID: 147153 has been added for this feature to log when any SGW address is blacklisted.



CHAPTER 47

SGSN-MME Combo Optimization

This section describes Combo Optimization available for a co-located SGSN-MME node. It also provides detailed information on the following:

Feature Description

The SGSN and MME can be enabled simultaneously in the same chassis and, though co-located, they each behave as independent nodes. This Combo Optimization feature enables the co-located SGSN and MME to co-operate with each other in order to achieve lower memory and CPU utilizations and to reduce signaling towards other nodes in the network. When functioning as mutually-aware co-located nodes, the SGSN and the MME can share UE subscription data between them.

Important This feature is supported by both the S4-SGSN and the Gn-SGSN. For the feature to apply to a Gn-SGSN, the Gn-SGSN must be configured to connect to an HSS. Combo Optimization for an SGSN-MME node is a licensed Cisco feature. 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*.

Overview

The load on S6d/S6a interfaces towards an HSS is reduced effectively by utilizing the resources in a co-located SGSN-MME node scenario. Requests for subscription data in Update Location Request (ULR) are skipped by setting the 'skip-subscriber-data' bit in the ULR flags this, in turn, reduces the load on the HSS. The Skip Subscriber Data AVP is used and the subscriber data is shared across the SGSN and the MME services.

As per 3GPP TS 29.272, setting the 'skip-subscriber-data' bit in the ULR indicates that the HSS may skip sending subscription data in Update Location Answer (ULA) to reduce signaling. If the subscription data has changed in the HSS after the last successful update of the MME/SGSN, the HSS ignores this bit and sends the updated subscription data. If the HSS skips sending the subscription data, then the GPRS-Subscription-Data-Indicator flag can be ignored.

Important The SGSN supported the Skip-Subscription-Data bit prior to Release 18.0. Support for this functionality was added to the MME in Release 18.0.

Ensuring that packets are routed internally reduces network latency for S3/Gn interface messages. This is achieved by configuring the SGTP and EGTP services in the same context for the SGSN and the MME configurations.

For outbound Inter-RAT SRNS Relocations, the MME gives preference to the co-located SGSN, irrespective of the order/priority or preference/weight configured for the SGSN entry in DNS Server. When Inter-RAT handovers take place between the co-located MME and the SGSN, the new call arrives at the same Session Manager that hosted the call in the previous RAT. If the subscription data is available for a given UE at the co-located SGSN, then the MME does not need to request this data from the HSS and provides UE subscription data obtained from the SGSN. This optional function can be turned on or off through the MME Service configuration.

Combo Optimization is available for subscribers with an EPC-enabled UE and an EPC subscription configured at the HSS. During handoff from 4G to 3G or 4G to 2G, the EPC subscription will be copied from the MME. Combo Optimization is also applicable for Non-EPC subscribers if core-network-interface is selected as S4 for the EPS-subscription.

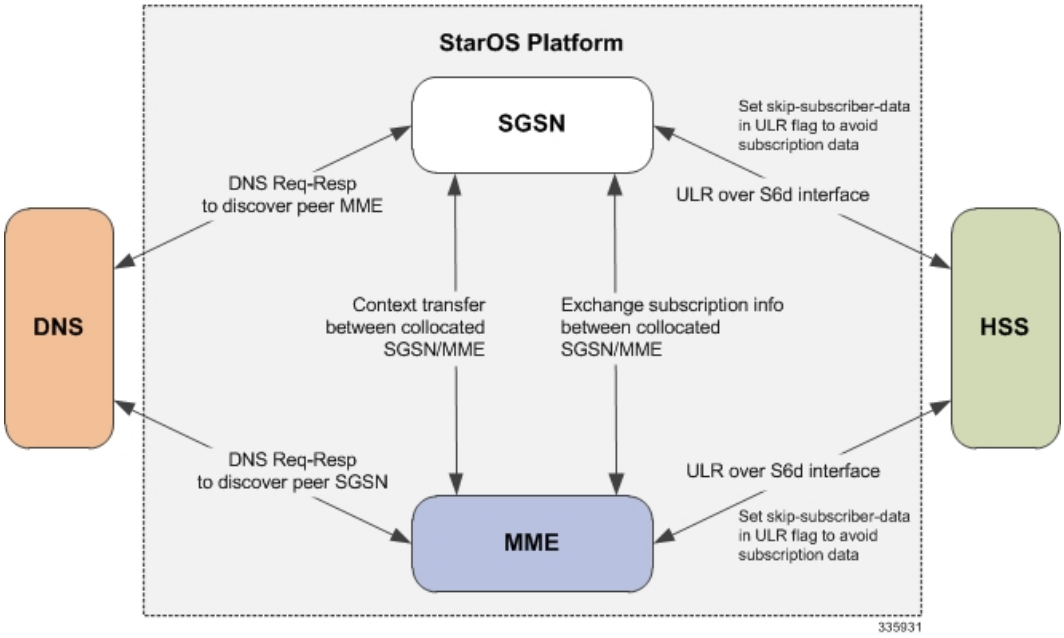
How It Works

Subscriber Movement from MME to SGSN: Subscription information is first fetched by the MME. On subscriber movement to a co-located SGSN, the SGSN sends a ULR with "skip-subscriber-data" flag set and the HSS sends a ULA (with or without subscription data depending on time of MME update).

Subscriber Movement from SGSN to MME: Subscription information is first fetched by the SGSN. On subscriber movement to a co-located MME, the MME sends a ULR with "skip-subscriber-data" flag set and the HSS sends a ULA (with or without subscription data depending on time of SGSN update).

Architecture

Figure 43: SGSN-MME Combo Node



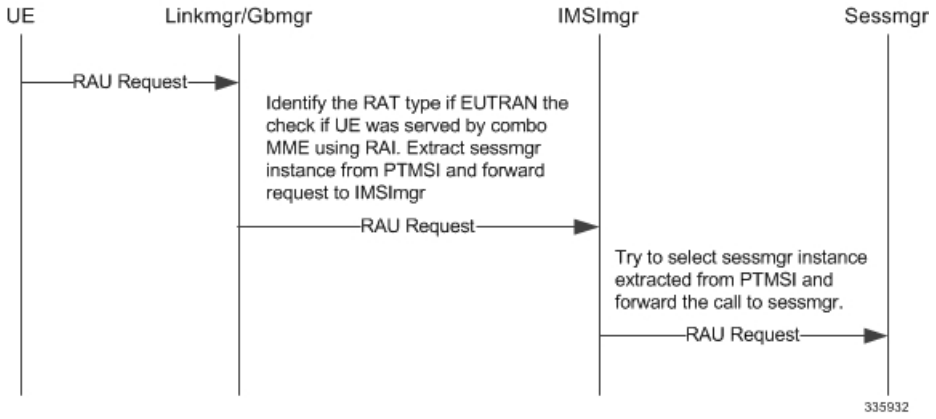
The above diagram displays the interworking of various modules when the Combo Optimization feature is enabled in a co-located SGSN-MME setup.

When the subscriber does RAU from MME to SGSN, or vice versa, a DNS query is initiated to fetch the address of the peer node. Based on the IP address obtained, the peer MME or SGSN is selected. When a DNS response is received with a list of peer SGSN addresses, the MME matches the configured EGTP/SGTP SGSN service address in the system and uses it for the S3/Gn UE Context Transfer procedures. If a DNS response is not received and a locally configured EGTP/SGTP SGSN service is present as a peer-SGSN, the peer-SGSN will be selected. Context transfer and copying of subscription information happens internally between the SGSN and the MME nodes. The SGSN maintains the s6d interface towards the HSS and the MME maintains the S6a interface towards the HSS. All network-initiated messages are sent separately towards the SGSN and the MME nodes respectively.

Flows

This section includes various diagrams that illustrate the session manager (SessMgr) selection logic during RAU, SRNS, and Attach procedures:

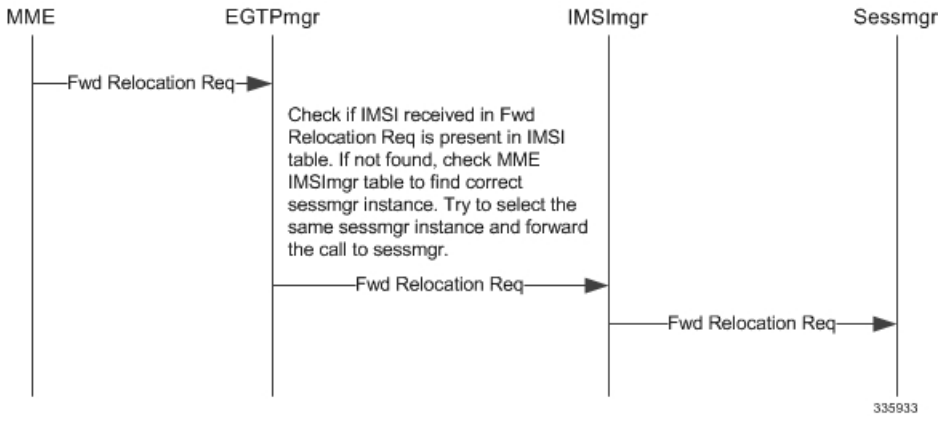
Figure 44: Selection of SessMgr Instance during RAU from MME to SGSN



Listed below is the SessMgr instance selection logic during a RAU procedure from the MME to SGSN:

1. A RAU request from UE is forwarded to the LinkMgr or GbMgr.
2. The LinkMgr identifies if the RAU is local and extracts the SessMgr instance from the PTMSI and forwards the request to IMSIMgr.
3. The IMSIMgr tries to select the SessMgr instance extracted from the PTMSI and forwards the request to the selected SessMgr.

Figure 45: Selection of SessMgr Instance during SRNS

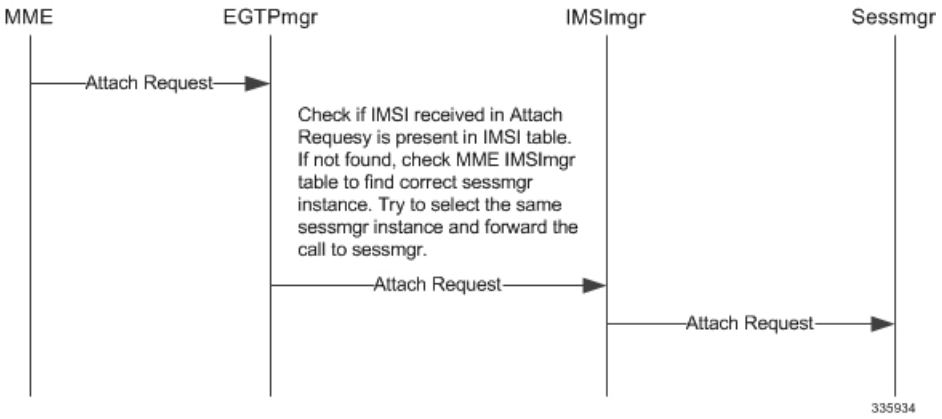


Listed below is the SessMgr instance selection logic during an SRNS procedure:

1. During an SRNS procedure, the MME service sends a Forward Relocation Request to the EGTPCMgr.
2. The EGTPCMgr forwards the request to the IMSIMgr.

3 The IMSIMgr uses the IMSI received in the request message to identify the SessMgr instance and forwards the request to the appropriate SessMgr instance.

Figure 46: Selection of SessMgr Instance during Attach



Listed below is the SessMgr instance selection logic during an Attach procedure:

1 During Attach procedure, the LinkMgr/GbMgr forwards the request to the IMSIMgr.
2 The IMSIMgr first verifies if the IMSI is present in the SGSN's IMSI table. If it is not present, the MME's IMSI table is verified. Once the entry is found the request is forwarded to the appropriate SessMgr.
3 If the entry is not found in either table, then an alternate SessMgr instance is used to process the call.

Limitations

Subscription information is shared between MME and SGSN only when both are connected to an HSS. Combo Optimization is not be applicable if either the MME or the SGSN is connected to an HLR. Though the subscription information is shared between the SGSN and MME services, a separate HSS service and diameter endpoint will be maintained for both the SGSN and the MME. All network-initiated messages are received separately for both the MME and the SGSN. Subscription data is copied based on time-stamp validation.

A small impact on the performance is observed during Inter-RAT handoffs as subscription data is exchanged between the SGSN and the MME. This impact is a limited increase in the number of instructions per handoff per UE depending on the number of APNs configured for the UE in the HSS.

It is necessary that the HSS honors the request from the MME/SGSN and not send subscription data when 'Skip-Subscriber-Data' flag is set in the ULR. However, there are some known and valid cases where the HSS ignores this flag for example, if the UE's subscription data changed since the last time the UE attached in 4G. (Typically, UE subscription data does not change frequently, therefore, HSS overrides are less frequent.)

Configuring the Combo Optimization

This section describes how to configure the Combo Optimization for an SGSN-MME combo node.

By default, Combo Optimization is not enabled. This command both enables or disables Combo Optimization on an SGSN-MME combo node.

config
lte-policy
[no] sgsn-mme subscriber-data-optimization
end

Note:

- **no** as a command prefix disables Combo Optimization.

Verifying Combo Optimization Configuration

Execute the following command to verify the configuration of this feature.

show lte-policy sgsn-mme summary

The following field value indicates if data optimization on the SGSN-MME combo node is "Enabled" or "Disabled":

- subscriber-data-optimization

Monitoring and Troubleshooting Combo Optimization

This section provides information on the show commands and bulk statistics available to monitor and troubleshoot Combo Optimization for the SGSN-MME combo node, and for each element separately.

Monitoring Commands for the SGSN-MME Combo Node

This section provides information regarding show commands and/or their outputs in support of the Combo Optimization feature on the SGSN-MME Combo Node:

show hss-peer-service statistics all

The following new fields are added to the show output to display the subscription data statistics:

- Subscription-Data Stats
- Skip Subscription Data
- Subscription-Data Not Received

The Skip Subscription Data statistic is incremented when the ULR is sent with the skip-subscription-data flag set. The Subscription-Data Not Received statistic is incremented if the HSS does not send the subscription data in the ULA when skip-subscription-data flag is set in ULR. The difference between the Skip Subscription Data and Subscription-Data Not Received gives us the number of times HSS does not honor the skip-subscription-data flag.

Monitoring Commands for the MME

This section provides information regarding show commands and/or their outputs in support of the Combo Optimization feature on the **MME**:

show mme-service statistics handover

The following new statistics are added to the show output to display the information about Inter-RAT Optimized Handoffs between the co-located SGSN and MME:

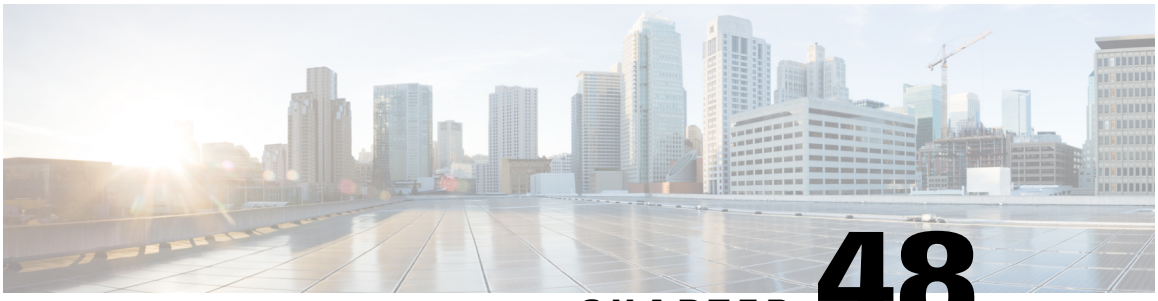
- Inter-RAT Optimized Handoffs Between Co-located MME and SGSN
- Outbound MME to SGSN RAU procedure
- Attempted
- Success
- Failures
- Inbound SGSN to MME TAU procedure
- Attempted
- Success
- Failures
- Outbound MME to SGSN Connected Mode Handover
- Attempted
- Success
- Failures
- Inbound SGSN to MME Connected Mode Handover
- Attempted
- Success
- Failures

Bulk Statistics for Monitoring the MME in an SGSN-MME Combo Node

The following bulk statistics in the MME schema facilitate tracking MME optimization functionality for the SGSN-MME nodes when co-located in the same chassis with the Combo Optimization functionality enabled:

- optimized-out-rau-ho-4gto2g3g-attempted
- optimized-out-rau-ho-4gto2g3g-success
- optimized-out-rau-ho-4gto2g3g-failures
- optimized-in-tau-ho-2g3gto4g-attempted
- optimized-in-tau-ho-2g3gto4g-success

- optimized-in-tau-ho-2g3gto4g-failures
- optimized-out-s1-ho-4gto2g3g-attempted
- optimized-out-s1-ho-4gto2g3g-success
- optimized-out-s1-ho-4gto2g3g-failures
- optimized-in-s1-ho-2g3gto4g-attempted
- optimized-in-s1-ho-2g3gto4g-success
- optimized-in-s1-ho-2g3gto4g-failures



CHAPTER 48

Single Radio Voice Call Continuity

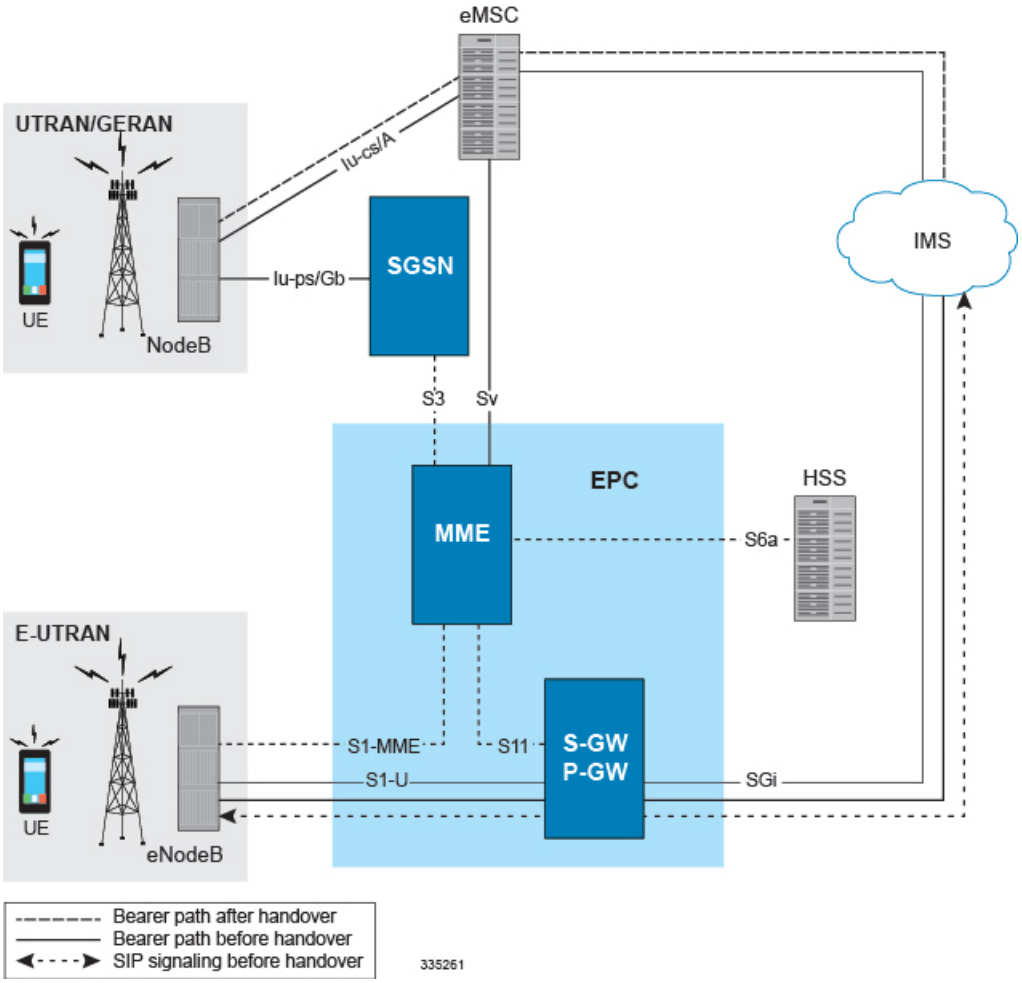
Voice over IP (VoIP) subscribers anchored in the IP Multimedia Subsystem (IMS) network can move out of an LTE coverage area and continue the voice call over the circuit-switched (CS) network through the use of the Single Radio Voice Call Continuity (SRVCC) feature. Unlike other methods like CSFB, it does not require a dual-mode radio.

Feature Description

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

To support SRVCC functionality on the MME, an Sv interface is created to the Mobile Switching Center (MSC) server responsible for communicating with the MME during the handover process.

Figure 47: SRVCC Architecture



Supported SRVCC Features

The MME supports the following SRVCC features:

SRVCC CS-PS Handover Continuity on PS Handover Failure: During S1-based CS-PS SRVCC handover, if one of the following types of failures occurs

- Peer SGSN DNS query failed
- Fwd Relocation Response timeout
- Fwd Relocation Response was received with a failure cause

then the handover will continue for CS calls if CS handover on the Sv interface succeeds. This means that the S1 SRVCC handover will continue as partially successful and the handover command message will not carry any bearer related information.

MSC Selection using DNS: As defined in 3GPP TS 29.303 V10.4.0, the MME supports DNS-based MSC selection. In the NAPTR query response, the MME will analyze the "Service Parameter" of "x-3gpp-msc:x-sv", and select a specific MSC from a pool list provided in the DNS response. The provisioned weights and priorities on the DNS server are used to load share proportionally between the MSC servers.

If DNS lookup fails, the MSC will be selected from local configuration. If an MSC pool area has been configured, the selection logic for the pool area will be used.

MSC Pool Areas: MSC pool areas can be configured for load balancing and intelligent selection of MSC servers based on PLMN and/or IMSI hash values. Up to 24 MSC servers can be defined per MME service. Each pool-area can optionally be associated with a PLMN, which is the target PLMN as specified in the SRVCC Handover request.

The MME attempts to select an MSC using the following selection order: 1) Pool-area that matches the PLMN and of type hash 2) Pool-area that matches the PLMN and of type round-robin 3) Pool-area that does not have PLMN and of type hash 4) Pool-area that does not have PLMN and of type round-robin.

MSC Offload: The MME allows an administrator to place one or more MSC server in maintenance mode. This action removes the MSC server as a possible selection target.

MSC Fallback on Failure: The MME automatically attempts to resend the Sv PS to CS Request to a different MSC if: 1) no response is received (timeout) from the MSC to a Sv PS to CS Request, or 2) any failure response is received from the MSC to a Sv PS to CS Request.

If no alternate MSC is configured, or if the second MSC fails as well, the SRVCC handover fails. A new MSC is attempted only for the initial PS to CS Request. No additional configuration is needed to enable this functionality.

When an MSC is selected by DNS, and multiple results are returned, the second MSC result will be used for fallback. In case DNS selection returns just one MSC, the second MSC for fallback will be from local configuration if it exists. If DNS lookup fails, the MSC for fallback will be selected from local configuration.

Disabling MSC Fallback on Failure: If so configured, the MME rejects handover based on the SRVCC failure cause received from the MSC. So that ***in some situations***, the MME will ignore MSC fallback procedures outlined above. If a voice call can be handed over to one of multiple MSC IP addresses during SRVCC handover, and if the PS-CS Response from the first MSC returns with a negative cause, and if that cause has been included in the MME's Call-Control Profile configuration with the **msc-fallback-disable** command, then the MME fails the SRVCC HO and does not try the next available MSC. For configuration details, refer to 'Disabling MSC Fallback Based on SRVCC Cause' in the section on *Configuring an MSC Pool Area*.

Other Supported SRVCC Features: The MME implementation of SRVCC also supports:

- IMS Centralized Service call handling as specified in 3GPP TS 29.280, enabling call flow handling for advanced scenarios.
- Emergency Calls as defined in 3GPP TS 29.280.
- GTP echo path management messages as defined in 3GPP TS 29.280.
- GTP-C DSCP marking.

MSC Fallback on Sv Interface

In Release 20.0, MME is modified to maintain 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 does not select the MSCs in the DOWN 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.

Relationships to Other Features

If the UE supports circuit-switch fallback (CSFB) and/or IMS voice, or both, the UE shall include the information element "Voice domain preference and UE's usage setting" in Attach Request and Tracking Area Update Request messages. The UE's usage setting indicates whether the UE behaves in a voice centric or data centric way. The voice domain preference for E-UTRAN indicates whether the UE is configured as CS Voice only, CS Voice preferred and IMS PS Voice as secondary, IMS PS Voice preferred and CS Voice as secondary, or IMS PS Voice only. The purpose of this information element is to signal to the network the UE's usage setting and voice domain preference for E-UTRAN.

The UE also includes the SRVCC capability indication as part of the "MS Network Capability" in the Attach Request message and in Tracking Area Updates. This capability needs to be accessed and stored on the MME.

If the UE reflects SRVCC along with IMS voice in the "Voice domain preference" in a Combined Attach, the MME will treat it as a EPS Attach with SRVCC capability.

How It Works

The existing eGTP-C service is enhanced to support the Sv reference point. A new instance of the eGTP-C service must be configured for Sv messages.

SRVCC requires the following elements:

- SRVCC requires the STN-SR to be sent to the MSC for all non-emergency calls. If the STN-SR is not present in the HSS during the Attach procedure, SRVCC handover will not be allowed for non-emergency calls. In case of situations like STN-SR not being configured for non-emergency calls, the MME will send a HANDOVER PREPARATION FAILURE message back with the cause code set to Handover Failure in Target System.
- MSC Server that has been enhanced for SRVCC.

- UE that has ICS (IMS Service Continuity) capabilities with single radio access. The UE includes the ICS Capability indication as part of the UE network capability in the Attach Request message. The MME stores this information for SRVCC operation.
- IMS network and SCC-AS in which the call is anchored. The MME signals to the UE the presence of VoIMS in the Attach Response

SRVCC is agnostic as to the whether S3 or GnGP is used for the SGSN interface.

Flows

The following SRVCC call flows are supported:

- SRVCC from E-UTRAN to GERAN without DTM support (TS 23.216 V10.5.0; Section 6.2.2.1).
- SRVCC from E-UTRAN to GERAN with DTM but without DTM HO support and from E-UTRAN to UTRAN without PS HO (TS 23.216 V9.6.0; Section 6.2.2.1A).
- SRVCC from E-UTRAN to UTRAN with PS HO or GERAN with DTM HO support (TS 23.216 V9.6.0; Section 6.2.2.1A).
- Emergency calls for all of the above three SRVCC scenarios

Standards Compliance

The MME implementation of SRVCC complies with the following standards:

- 3GPP TS 23.216 Single Radio Voice Call Continuity (SRVCC) V10.5.0
- 3GPP TS 29.280 Sv Interface (MME to MSC and SGSN to MSC) for SRVCC V10.4.0
- 3GPP TS 36.413 S1 Application Protocol (S1AP) V10.5.0
- 3GPP TS 29.303 Domain Name System Procedures; Stage 3 V10.4.0

Configuring Single Radio Voice Call Continuity

- Configuring SRVCC, on page 455
- Configuring MSC Selection Using DNS, on page 456
- Configuring an MSC Pool Area, on page 457
- MSC Offload, on page 460
- Verifying the SRVCC Configuration , on page 461

Configuring SRVCC

Use the following example to configure basic SRVCC support on the MME, including:

- Creating the eGTP-C Sv service and binding it to an IPv4/v6 address.
- Associating the eGTP-C service to the MME service.
- Configuring one or more MSC servers within the MME service.

```
configure
    context mme_context_name
        interface sv_intf_name
            ip address ipv4_address
            exit
        egtp-service egtpc_sv_service_name
            interface-type interface-mme
            gtpc bind ipv4-address sv_infc_ip_address
            exit
        mme-service mme_service_name
            associate egtpc-sv-service egtpc_sv_service_name
            msc name msc_name ip-address ip_address
            exit
        exit
    port ethernet slot_number/port_number
        no shutdown
        bind interface sv_intf_name mme_context_name
        end
```

Notes:

- The **gtpc bind** command can be specified as an IPv6 address using the **ipv6-address** keyword. The **interface** specified for Sv communication must also be the same IP address type.

Configuring MSC Selection Using DNS

DNS based MSC selection can be defined for an MME service, or for a Call Control Profile. Both configuration options specify the context in which a DNS client configuration has been defined.

Refer to *Configuring Dynamic Peer Selection* in the *MME Configuration* chapter of this document for details on configuring the DNS client.

Configuration via Call Control Profile takes precedence in cases where both options are configured.

MSC selection using DNS take precedence over MSC pool-areas and locally configured MSCs.

To configure DNS selection of an MSC for a specific MME service, refer to the following example:

```
configure
    context ctxt_name
        mme-service service_name
            dns msc context <ctxt_name>
            end
```

To configure DNS selection of an MSC based on a Call Control Profile, refer to the following example.

```
configure
    call-control-profile profile_name
        dns-msc context ctxt_name
        end
```

Notes:

- Configuration via Call Control Profile takes precedence if DNS is configured via both mme-service and call control profile.

To define an MSC server that should be selected by DNS, the **msc** command must be used without the **ip-address** keyword, as follows

```
configure
   context ctxt_name
      mme-service mme_service_name
         msc name msc_name
         end
```

Configuring an MSC Pool Area

In order to support pooling, multiple MSC servers and pool-areas for Sv interface are allowed to be configured within the MME service. A maximum of 24 MSC servers can be configured for a given MME Service. Each MME Service can also have be a maximum of 24 pool areas. Each pool-area can have a maximum of 24 MSC's.

The pool can be either based on IMSI hash or a round-robin scheme. In the IMSI hash scheme, an MSC is chosen based on the result of the IMSI [(IMSI div 10) modulo 1000]. In case of round-robin, the MME selects the next MSC based on the round-robin scheme.

Each pool-area is associated with a unique name. Within a pool-area of type hash, up to 24 hash-values can be defined. Pool-area of type round-robin can have up to 24 entries.

Each pool-area can be associated with a PLMN which is the target PLMN as specified in the SRVCC Handover request.

MME attempts to select a MSC using the following selection order:1) Pool-area that matches the PLMN and of type hash2) Pool-area that matches the PLMN and of type round-robin3) Pool-area that does not have PLMN and of type hash4) Pool-area that does not have PLMN and of type round-robin

IMSI Hash MSC Pool

Use the following example to configure an MSC server pool with a selection scheme based on the IMSI hash value.

```
configure
   context ctxt_name
      mme-service service_name
         pool-area pool_area_name type hash-value
            hash-value { hash_value | range start_value to end_value } use-msc msc_id
            plmnid mcc code mnc code
            end
```

Notes:

- The **pool-area** command creates a Mobile Switching Center (MSC) server pool area and defines that the MSC servers be selected from within the pool using the result of the IMSI (using the **hash-value** keyword).
- The optional **plmnid** command associates a Public Land Mobile Network (PLMN) identifier with this Mobile Switching Center (MSC) pool area. This is used to select an MSC based on the target PLMN as specified in the SRVCC handover request. If a pool does not have any PLMN id associated with it, the pool area is assumed to be able to serve any PLMN.

If this command is used, the PLMN id values specified must be unique within a given MSC pool area type. For example, multiple pool areas of type hash cannot use the same PLMN. However, you can configure one pool area of type hash and another of type round-robin and have both use the same PLMN id.

- The **hash-value** command configures the selection of a Mobile Switching Center (MSC) server in a MSC pool area based on the hash value derived from the IMSI [(IMSI div 10) modulo 1000].

  The **use-msc** keyword associates an MSC to use for this hash value, where *msc_name* is the name of the MSC as previously configured in the MME service using the **msc** command. A maximum of 24 MSCs can be defined per pool area.

- See the *MME MSC Server Pool Area Configuration Mode* chapter of the *Command Line Interface Reference* for more information.

Round-Robin MSC Pool

Use the following example to configure an MSC server pool with a round-robin selection scheme.

```
configure
   context ctxt_name
      mme-service service_name
         pool-area pool-area-name type round-robin
            plmnid mcc code mnc code
            use-msc msc_id
            end
```

Notes:

- The **pool-area** command creates a Mobile Switching Center (MSC) server pool area and defines that the MSC servers be selected from within the pool using a round-robin scheme (using the **round-robin** keyword).
- The optional **plmnid** command associates a Public Land Mobile Network (PLMN) identifier with this Mobile Switching Center (MSC) pool area. This is used to select an MSC based on the target PLMN as specified in the SRVCC handover request. If a pool does not have any PLMN id associated with it, the pool area is assumed to be able to serve any PLMN.

  If this command is used, the PLMN id values specified must be unique within a given MSC pool area type. For example, multiple pool areas of type hash cannot use the same PLMN. However, you can configure one pool area of type hash and another of type round-robin and have both use the same PLMN id.

- The **use-msc** command associates an MSC with this pool area, where *msc_name* is the name of the MSC as previously configured in the MME service using the **msc** command. A maximum of 24 MSCs can be defined per pool area.
- See the *MME MSC Server Pool Area Configuration Mode* chapter of the *Command Line Interface Reference* for more information.

Configuring MSC Fallback on Sv Interface

This section describes the configuration to enable the MSC Fallback feature.

To enable the MSC Fallback feature, the echo parameters should be configured under the MME Service Configuration Mode.

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

To configure the echo parameters use the following configuration:

```
configure
    context context_name
        mme-service service_name
            [ no ] msc-echo-params interval echo_interval retransmission-timeout timer_value
max-retransmission number_of_retries reconnect-interval interval_value
            end
```

Notes:

- By default, the MSC Fallback feature is disabled.
- **msc-echo-params** configures EGTPC echo parameters for MSC Fallback. The msc-echo-params configuration overrides any echo parameter configured in the egtp-service configuration for the corresponding SV service.
- **interval** is used to configure the time interval to send echo requests to an MSC. The interval ranges from 2 to 3600 seconds.
- **retransmission-timeout** configures the echo retransmission timeout in seconds. The timer value ranges from 1 to 20 seconds.
- **max-retransmission** configures the maximum number of echo retransmissions. The number of retransmissions is an integer from 0 to 15.
- **reconnect-interval** configures the echo interval to be used once an MSC is detected to be unreachable. The time interval ranges from 60 to 86400 seconds.
- Retransmission of ECHO requests is not applicable during the reconnect interval.

Disabling MSC Fallback Based on SRVCC Cause

By default, the MME supports MSC Fallback on Failure -- as explained in the section under *Supported SRVCC Features*. With the following configuration, the operator can selectively disable MSC fallback on failure during voice call handover.

The selection process is based on the SRVCC cause codes configured in the call-control profile. It there is a match with the MSC failure cause received in the PS-CS Response from the first MSC, then the MME fails the SRVCC HO and does not try the next available MSC.

```
configure
    call-control-profile profile_name
        msc-fallback-disable srvcc-cause cause
    end
```

Notes:

- **srvcc-cause**: Use this keyword to define a single SRVCC cause code. The *cause* must be any integer from 0 to 255, as defined in 3GPP TS 29.280.
- Repeat the command as needed to define additional SRVCC cause codes in the call-control profile.
- This command is only applicable for PS-CS Requests and not for PS to CS complete messages.

MSC Offload

The MME allows an administrator to place one or more MSC server in maintenance mode. This action removes the MSC server as a possible selection target.

To offload and MSC, use the **offline** keyword at the end of the **msc** configuration command .

When the configuration is changed back to **online**, the MSC will be added back as a selection target and normal operation is returned.

configure
context <*ctxt_name*>
mme-service <*service_name*>
msc *name* **[ip-address** *address* **] [offline | online]**
end

Notes:

- No actual GTPv2 messages are generated when the configuration is changed to offline. The MSC is only removed as a selection target for future load sharing.

HSS Purge After SRVCC Handoff

The MME supports an optional configuration capability to perform the Purge UE procedure to the HSS for UEs which support Dual Transfer Mode (DTM). This feature is configurable via the CLI and is disabled by default. If configured, the MME initiates an HSS Purge after the following two SRVCC HO scenarios:

- For SRVCC Handoff with PS Handoff support, the Purge S6a message is sent immediately after successful completion of the Handoff. For this scenario, the configurable purge timer is not used.
- For SRVCC Handoff without PS Handoff support, a configurable timer is initiated and the Purge S6a message is sent if a SGSN Context Request is received prior to timer expiry. If a Context Failure occurs, no HSS Purge S6a message is sent.

This feature ensures the HSS has a reliable UE status on whether it is currently operating on the LTE network.

The following commands configure the MME to initiate an HSS Purge after the SRVCC HO where the UE supports DTM. It also allows configuration of a purge timeout value in seconds.

configure
context *ctxt_name*
mme-service *service_name*
policy srvcc purge-timer *seconds*
[no] policy srvcc purge-timer
end

Notes:

- **purge-timer** *seconds*: defines how long in seconds the Purge Timer will run. This is applicable only for SRVCC Handoff without PS Handoff support scenarios.
- For example, if **purge-timer** is set to 20 seconds :

  If the Context Transfer happens 10 seconds after SRVCC HO, the MME initiates an HSS Purge.

  If the Context Transfer happens 30 seconds after SRVCC HO, the MME will NOT initiate an HSS Purge because the Purge Timer has expired.

Verifying the SRVCC Configuration

The following command displays the MSC servers configured in the specified MME service:

show mme-service name *service_name*
In the following example output:

- **msc1**, **msc2**, and **msc3** are configured with an IPv4 address.
- **msc3** is currently configured for MSC offload (offline).

```
SCTP Alternate Accept Flag           : Enabled
MSC                                  : msc1  10.10.1.1
MSC                                  : msc2  10.10.1.2
MSC                                  : msc3  10.10.1.3   Offline
```

The same command displays the context in which the DNS client configuration has been defined for the specified MME Service for DNS based MSC selection.

```
SGW DNS Context                      : Not defined
MSC DNS Context                      : ingress
```

The following command displays the context in which the DNS client configuration has been defined for the specified Call Control Profile for DNS based MSC selection:

show call-control-profile full name *profile_name*

```
DNS MSC Context                      : ingress
```

Monitoring and Troubleshooting SRVCC

SRVCC Show Command(s) and/or Outputs

This section provides information regarding show commands and/or their outputs in support of SRVCC.

show mme-service all name

On executing the above command the following new fields are displayed:

- MSC Echo Parameters:
  - Interval
  - retransmission-timeout
  - max retransmissions
  - reconnect interval

show mme-service msc-status

On executing the **show mme-service msc-status [mme-service-name** *name* **| msc-name** *name* **]** command, the following status information is displayed:

```
MSC Status
Name:                msc1
```

```
IP:                  192.80.80.57
Node Status:         Online
Path State:          up
MME Service Name:    mmesvc
Static/DNS IP:       Static
```

Note

- When the MSC Fallback Feature is enabled, that is, when msc-echo-params is configured, the possible Path State values indicated are - Up, Down, and Unknown.
- The Path State will indicate 'NA' if msc-echo-params is not configured or if the node is made "offline" using suitable commands.
- New trace level logging event-id(s):
  - 147151 has been added in the MME-APP facility to monitor reachability status of the MSC, when the status changes.
  - 141120 to 141123 has been added for EGTPC layer debugging.
  - 143802 to 143815 for has been added for EGTPMGR layer debugging.

show mme-service statistics

This command displays SRVCC statistics for CS handovers with no Dual Transfer Mode (DTM), CS-only transfers, and CS and PS transfers.

```
EUTRAN-> UTRAN/GERAN using Sv Interface:
      CS only handover with no DTM support:
            Attempted:                        0  Success:                        0
            Failures:                         0
      CS only handover:
            Attempted:                        0  Success:                        0
            Failures:                         0
      CS and PS handover:
            Attempted:                        0  Success:                        0
            Failures:                         0
```

show egtpc statistics

This command displays EGTPC Sv interface statistics statistics for CS handovers with no Dual Transfer Mode (DTM), CS-only transfers, and CS and PS transfers.

```
SRVCC Messages:
PS to CS  Request:
 Total   TX:                          0
 Initial TX:                          0
 Retrans TX:                          0
  Discarded:                          0
 No Rsp Rcvd:                         0
PS to CS Response:
 Total   RX:                          0
 Initial RX:                          0
   Accepted:                          0
     Denied:                          0
  Discarded:                          0
PS to CS Complete Notification:
 Total   RX:                          0
 Initial RX:                          0
 Retrans RX:                          0
  Discarded:                          0
```

```
PS to CS Complete Acknowledge:
 Total   TX:                          0
 Initial TX:                          0
   Accepted:                          0
     Denied:                          0
 Retrans TX:                          0
  Discarded:                          0
PS to CS Cancel Notification:
 Total   TX:                          0
 Initial TX:                          0
 Retrans TX:                          0
  Discarded:                          0
 No Rsp Rcvd:                         0
PS to CS Cancel Acknowledge:
 Total   RX:                          0
 Initial RX:                          0
   Accepted:                          0
     Denied:                          0
  Discarded:                          0
```

SRVCC Bulk Statistics

eGTP-C Schema

The following statistics are included in the eGTP-C Schema in support of SRVCC:

For descriptions of these variables, see "eGTP-C Schema Statistics" in the *Statistics and Counters Reference*.

- srvcc-sent-pstocsreq
- srvcc-sent-retranspstocsreq
- srvcc-recv-pstocsrsp
- srvcc-recv-pstocsrspDiscard
- srvcc-recv-pstocsrspaccept
- srvcc-recv-pstocsrspdenied
- srvcc-recv-pstocscmpnotf
- srvcc-recv-pstocscmpnotfDiscard
- srvcc-recv-retranspstocscmpnotf
- srvcc-sent-pstocscmpack
- srvcc-sent-retranspstocscmpack
- srvcc-sent-pstocscmpackaccept
- srvcc-sent-pstocscmpackdenied
- srvcc-sent-pstocscancelnotf
- srvcc-sent-retranspstocscancelnotf
- srvcc-recv-pstocscancelack
- srvcc-recv-pstocscancelackDiscard
- srvcc-recv-pstocscanelackaccept

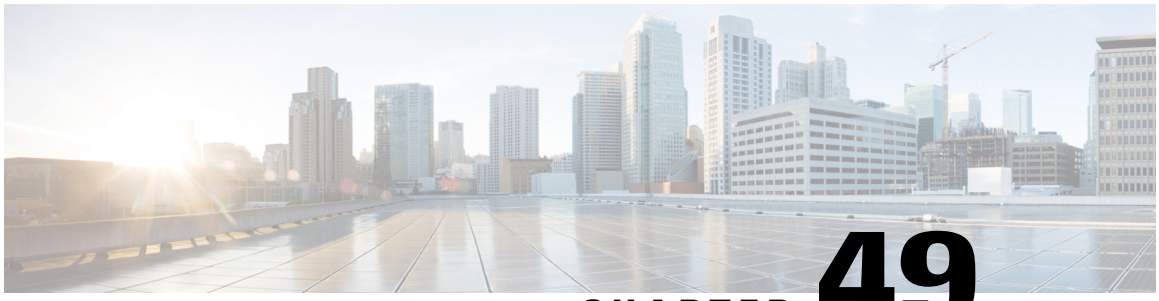
- srvcc-recv-pstocscancelackdenied

MME Schema

The following statistics are included in the MME Schema in support of SRVCC:

For descriptions of these variables, see "MME Schema Statistics" in the *Statistics and Counters Reference*.

- s1-ho-4gto3g-cs-nodtm-sv-attempted
- s1-ho-4gto3g-cs-nodtm-sv-success
- s1-ho-4gto3g-cs-nodtm-sv-failures
- s1-ho-4gto3g-cs-sv-attempted
- s1-ho-4gto3g-cs-sv-success
- s1-ho-4gto3g-cs-sv-failures
- s1-ho-4gto3g-csps-sv-attempted
- s1-ho-4gto3g-csps-sv-success
- s1-ho-4gto3g-csps-sv-failures



CHAPTER 49

SRVCC for 1xRTT

The MME supports single radio voice call continuity (SRVCC) for CDMA2000 1x (single-carrier) radio transmission technology (1x-RTT) networks.

Feature Description

Overview

SRVCC functionality is required within VoLTE systems to enable the packet domain calls received in LTE to be handed over to a legacy circuit-switched (CS) voice system, such as CDMA2000 1xRTT. SRVCC for 1xRTT, also referred to as enhanced SRVCC, enables the MME to move a VoLTE UE between an LTE and a 1xRTT network with smooth, seamless handovers. The MME acts as a relay agent to ensure CDMA2000 messages received from the UE are delivered to the interworking solution function (for 3GPP2, 1xCS IWS) associated with the mobile switching center (1x RTT MSC) (or vice-versa) through the S1-AP and S102 interfaces.

By using the MME's SRVCC for 1xRTT capabilities, the operator performs handovers while maintaining existing quality of service (QoS) and ensuring call continuity that meets the critical requirements for emergency calls.

This feature is license-controlled and the commands to configure and manage the feature interfaces require a feature license key. Speak with your Cisco Representative for information about this license. For information about the commands and their use, refer to the *Configuring SRVCC for 1xRTT* section later in this chapter.

Supported Features

The MME provides the following features in support of SRVCC for 1xRTT functionality:

MSC Pool Areas: Multiple MSCs would be handled by pooling all the MSCs mapping to a particular cell for load distribution. MSC pool areas can be configured for load balancing and intelligent selection of MSC servers based on IMSI hash values. Up to 10 MSC servers can be defined per S102 service.

MSC Non-Pool Areas: MSC selection, based on local MSC configuration.

MSC Selection: If an MSC pool area has been configured, the selection logic for the pool area is based on the CDMA2000 sector cell ID (includes the MSC ID and the Cell ID) in the CDMA2000 1xRTT network

Both the MSC ID and the cell ID are used to locate the pool / non-pool area. The MME attempts to select an MSC using the following selection order:

1 The MME attempts to match the MSC ID and the Cell ID:
   - If the match is found in the non-pool area configuration, then the configured MSC is selected.
   - If the match is found in the pool area configuration,
     - then IMSI hashing is used to select the MSC.
     - if no hash corresponds, then the MSC selected is the one configured for the 'non-configured-values'.

2 If no MSC is found, a failure message is returned.

Important When the UE attaches with IMEI, the MSC configured for the non-pool area is always selected because IMSI hashing cannot be performed for that UE.

Relationships to Other Features

SRVCC for 1xRTT is related to the CSFB for 1xRTT feature. Each requires a separate license to take advantage of the separate functionality and use the configuration commands.

If licenses for both features are installed in the system and both features are configured, then the MME can use the S102 interface for both CSFB for 1xRTT and SRVCC for 1xRTT.

1xRTT SRVCC and 1xRTT CSFB calls will be decided based on the presence or absence of the CDMA2000 1xRTT SRVCC Info IEs in an Uplink S1 CDMA2000 Tunneling message. This IE should not present for a 1xRTT CSFB call. If only one feature is licensed and configured and if the above condition is not appropriately satisfied for any received call, then that call will be dropped.

The CSFB for 1xRTT feature is described elsewhere in this administration guide.

How It Works

Functional Overview

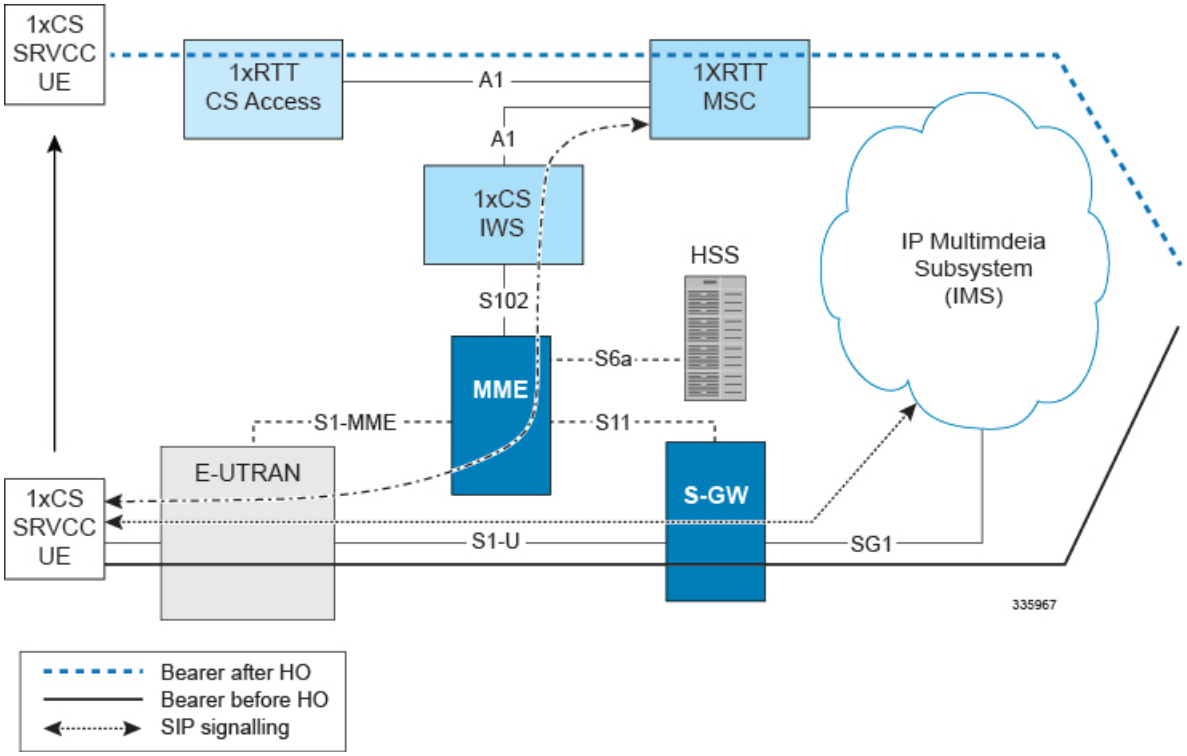
The call originating from the UE, and anchored as part of the voice-call continuity,.is part of a bidirectional process. The MME communicates with the 1xCS IWS (a circuit-switched fallback interworking solution

function for 3GPP2 1xCS) to enable a single radio UE (an eSRVCC-enabled UE) to communicate in parallel with both the source system and the target system.

- On the originating source side, the 1xCS signaling messages are tunneled from the UE across the E-UTRAN to the MME.
- Moving from the originating side to the target side, the messages tunnel from the MME through the S102 interface via the A21 protocol to reach the 1xCS IWS at the target side.
- At the target side, from the 1xCS IWS, the messages tunnel through the A1 interface to the 1xRTT MSC. From the MSC, signaling moves towards the VLR/HLR for registration and authorization, if needed, or towards call setup procedures.

Architecture

Figure 48: MME's Architecture for SRVCC for 1xRCC



Flows

SRVCC for 1xRTT complies with the following call flows procedures as defined by 3GPP TS 23.216, Release 10:

- **E-UTRAN Attach Procedure:**

- An SRVCC UE includes the SRVCC capability indication as part of the 'UE Network Capability' in the EPS Attach Request.
- The MME includes an 'SRVCC Operation Possible' indication in the S1-AP Initial Context Setup Request.
- The request is followed by eSRVCC HO, with eNB sending an Uplink CDMA2000 message with 1xSRVCC Info IE on S1-AP.
- The MME copies the contents transparently and sends an A21 Air Interface message towards 1xIWS.
- MEID is sent as IMSI towards the MSC.

- **PS Handover (S1-based):**
  - The target MME includes an 'SRVCC Operation Possible' indication in the S1-AP Handover Request message. This indicates that both the UE and the target MME are SRVCC-capable.
  - If the S1-HO is successful, then the Request message is followed by an Uplink CDMA2000 message with 1xSRVCC Information from the target eNB.
  - If an MME change is required, the a Forward Relocation Request is sent towards the target MME with the UE Network capability, inside the MM Context message, indicating 1xSRVCC support.

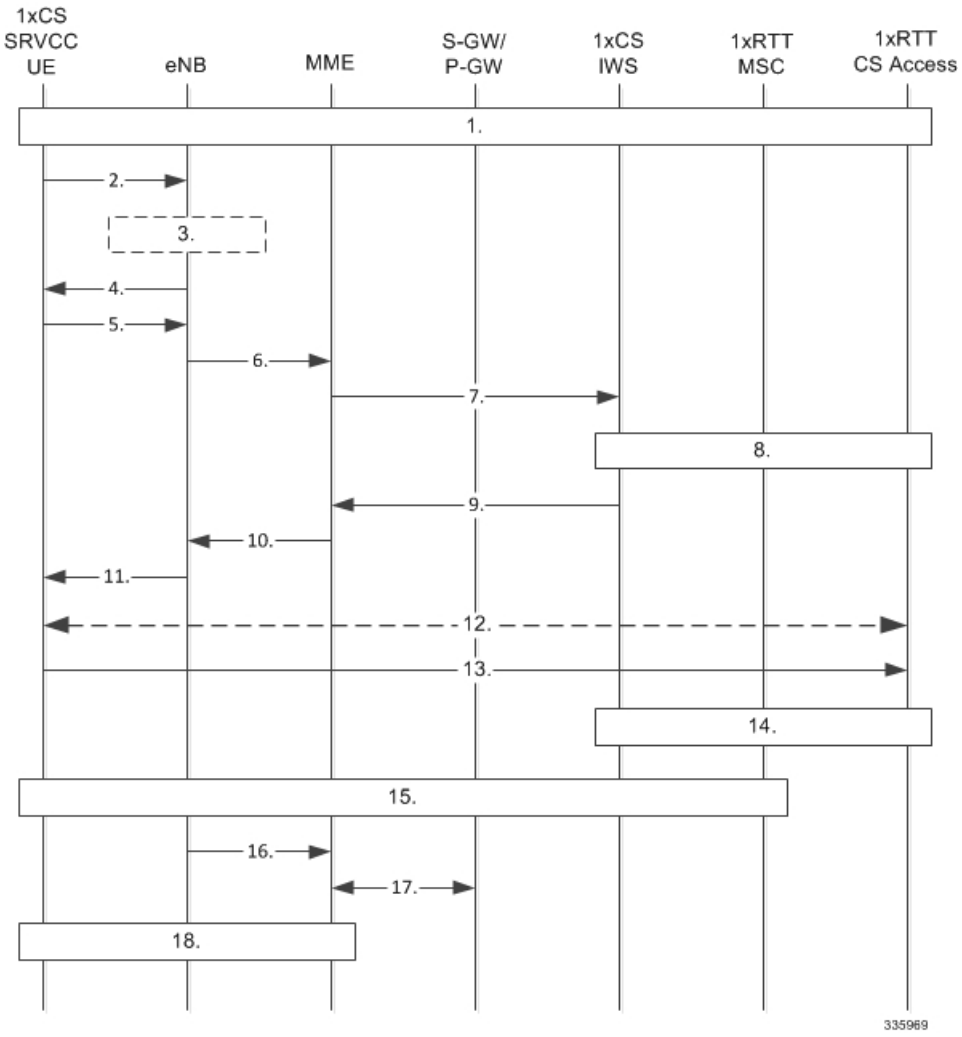
- **PS Handover (X2-based):** The source eNodeB includes an 'SRVCC Operation Possible' indication in the X2-AP Handover Request message to the target eNodeB.

Important The MME is not participate in carrying the SRVCC information in the X2-based PS Handover. This is a direct eNB-to-eNB transfer.

- **Service Request Procedure:** The MME includes an 'SRVCC Operation Possible' indication in the S1-AP Initial Context Setup Request during the Service Request Procedure.
- **E-UTRAN Emergency Attach Procedure:**
  - The SRVCC UE includes the SRVCC capability indication as part of the 'UE Network Capability' in the Emergency Attach Request with IMEI/IMSI as the identity.
  - The MME includes an 'SRVCC Operation Possible' indication in the S1-AP Initial Context Setup Request.
  - The request is followed by eSRVCC HO, with the NB sending an Uplink CDMA2000 message with the 1xSRVCC Info IE on S1-AP.
  - The MME copies the contents transparently and sends an A21 Air Interface message towards the 1xIWS.
  - MEID is sent as IMEI/IMSI towards the MSC.

Typical SRVCC Call Flow

Figure 49: SRVCC Call Flow



The following notes on the flow definition are derived from section 6 of the 3GPP spec and for details we recommend you refer to TS 23.216:

1 ongoing VoIP session over the IMS access leg established over E-UTRAN access

2 measurement reports to eNB

3 determination to handover

4 E-UTRAN signals handover to UE handover

5 UE sends UL Handover Preparation Transfer message containing 1xRTT origination message (if appropriate, includes Request-Type = 'emergency handover' and the MEID (e.g. IMEI))

6 MME notified handover preparation has started - Uplink S1 CDMA2000 Tunneling (RAT Type, Sector ID, RAND, PDU, 1x Origination and 1xSRVCC Info IE containing MEID and mobile subscription information) message to the MME.S102 Direct Transfer message (1x Air Interface Signaling (origination))

7 S102 Direct Transfer message (1x Air interface Signaling (origination))

8 1x traffic assignment / handoff initiation
9 S102 Direct Transfer (1x Air interface Signaling (handoff direction)
10 DL CDMA2000 Tunneling message (handoff direction)
11 Mobility from EUTRA command (handoff direction)
12 1x radio interface procedures to acquire traffic channel
13 1x handoff completion message
14 1x handoff completed
15 ongoing voice call over the CS access leg established over 1xRTT access
16 S1 UE Context Release Request with release cause 'Redirect towards 1xRTT'.
17 Suspend Request / Ack
18 S1 UE Context Release

Limitations

Step 19 of the SRVCC Call Flow procedure (outlined above), as defined by TS 23.216, provides a Subscriber Location Report to the GMLC. This function is currently not supported by the MME.

Standards Compliance

The MME's SRVCC for 1xRTT complies with the following standards:

- A21 Interface spec A.S0009-C
- 3GPP TS 36.413, Release 10
- 3GPP TS 24.301, Release 10
- 3GPP TS 29.274, Release 10
- 3GPP TS 23.272, Release 10
- 3GPP TS 23.216, Release 10

Configuring SRVCC for 1xRTT

If you have the appropriate license, you will be able to see and configure the commands identified below to

- setup an S102 service for the use of an S102 interface.
- associate the S102 service configuration with the MME service.
- configure MSC selection.

All three sets of configuration must be completed for this feature to function.

Important For more details on commands and keywords indicated below, we recommend that you refer to the *Command Line Interface Reference, StarOS Release 19* or higher.

Configuring the S102 Service

This configuration enables you to define the characteristics for a specific S102 interface as an S102 service instance, including:

- configuring the interface to work with SRVCC for the 1xRTT CDMA2000 messaging.
- binding or unbinding a logical IPv4 address and ports to the S102 service.
- configuring an IPv4 address and ports for the IWS/MSC in the S102 service configuration.

```
config
    context context_name
        [ no ] s102-service service_name
            [ no ] 1xRTT srvcc
            [ no ] bind ipv4-address ipv4_address port port_number
            [ no ] msc msc_name
                [ no ] ipv4-address ipv4_address port port_number
                exit
            [ no ] msc msc_name
                [ no ] ipv4-address ipv4_address port port_number
                exit
            end
```

Notes:

- *context_name* enter a string of 1 to 79 alphanumeric characters to define the name of the context in which the S102 service is configured. You can configure the S102 service in the same context in which the associated MME service is configured.
- *service_name* enter a string of 1 to 63 alphanumeric characters to define the name. We recommend that each service name be unique on this MME.
- The MME supports configuration of an undefined number of S102 services (interfaces). As there is a 1-to-1 correlation between S102 service configurations and MME services, the only limiting factor is the maximum number of MME services that can be configured per system maximum number is 8.
- **1xrtt** configures the S102 interface to provide either SRVCC or CSFB capabilities for the 1xRTT CDMA2000 network. The **1xrtt** command can be repeated so that a single S102 interface provides both CSFB and SRVCC functionality.
- **bind ipv4-address** *ipv4_address* **port** *port_number* binds the S102 interface to the specified source (MME) IPv4 interface address, and optionally to a specific port number if the port option is included. The value for the IPv4 address must be entered in standard IPv4 dotted-decimal notation and, if included, the port number must be an integer from 1 to 65535.
- **msc** *msc_name* enter 1 to 63 alphanumeric characters to define a unique name for the MSC. Executing the **msc** command causes the system to enter the S102-MSC configuration mode to define the target IPv4 address (and optionally the port ID). This associates the S102 interface to the specified MSC.
- **ipv4-address** *ipv4_address* **port** *port_number* identifies IPv4 interface address of the MSC, and optionally a specific port number if the port option is include. The value for the IPv4 address must be entered in standard IPv4 dotted-decimal notation and, if included, the port number must be an integer from 1 to 65535.
- It is possible to associate up to 10 IWS/MSCs with the S102 interface/service configuration. Repeat the **msc**, **ipv4-address**, and **exit** commands sequence as often as needed to identify all MSCs.

- **no** prefix included with a command, disables and/or erases the specified configuration from the MME's configuration.
- **default** prefix is unused at this time and is available for future development.

Verify the S102 Service Configuration

Use the **show s102-service name** *s102_service_name* command to verify the S102 configuration that you have entered following the steps outlined above. The output will appear *similar* to the following:

```
[local]MMEhost# show s102-service name s102-mme1
Service name      : s102-mme1
Context           : test
Status            : NOT STARTED
1xRTT type        : SRVCC
Bind              : Done
IP Address        : nnn.nnn.nnn.1
Port              : 54321
```

Associating the S102 Service

Use the following to add an association between a previously configured MME service and an S102 service.

config
context *context_name*
mme-service *mme_service_name*
associate s102-service *s102_service_name* [**context** *context_name* **]**
end

Notes:

- **context** *context_name* : enter a string of 1 to 79 alphanumeric characters to identify the name of the context in which the S102 service is configured. We recommend that you identify the context if it is not the same one in which the associated MME service is configured.

Verifying the S102 Association

Use the **show mme-service name** *mme_service_name* command to verify the S102 association that you have entered following the steps outlined above. The output will appear *similar* to the following:

```
[local]MME show mme-service name mme1
Service name                          : mme1
Context                               : test
Status                                : NOT STARTED
Bind                                  : Not Done
. . .
. . .
IPNE Service                          : Not defined
S102 Context                          : test
S102 Service                          : s102-A
Max bearers per MS                    : 11
. . .
. . .
```

Configuring MSC Selection

The following process configures up to 10 MSC pool/non-pool areas per S102 service in support of MSC selection. Both the MSC-Id and the Cell-Id are used to locate the pool or non-pool area for the MSC selection process.

Prerequisite: Each of the MSCs must have been defined and associated with an S102 service (see *Configuring the S102 Service* noted above) before the MSC can be included in the non-pool-area or pool-area configuration.

Defining a Non-Pool Area

config
context *context_name*
[no] s102-service *service_name*

Important The **plmn** option that is visible in the code is not supported at this time and is included for future development.

non-pool-area *non_pool_area_name* `msc` *msc_name* `msc-id` *msc_id* **cell-id** *cell_id* `+`
no non-pool-area *non_pool_area_name* **cell-id** *cell_id* **+**

Notes:

- *non_pool_area_name* enter a string of 1 to 63 alphanumeric characters to uniquely identify the non-pool-area definition used for MSC selection.
- **msc** *msc_name* enter a string of 1 to 63 alphanumeric characters to identify one of the MSCs previously configured in the S102 service configuration.
- **msc-id** *msc_id* cell-id *cell_id* +
  - *msc_id* enter an integer from 1 through 16777215 to identify the unique numeric ID for the MSC.
  - *cell_id* + enter an integer from 1 through 65535 to identify a CDMA2000 sector cell ID that you are assigning to this non-pool area configuration. Enter up to 24 cell IDs, separated by a single blank space, in the same command.
- **plmnid { any | mcc** *mcc_id* **mnc** *mnc_id* **}** is not operationally supported at this time. The code is included for future development.
- **no** prefix included with the command, erases or disables the specified configuration from the MME's configuration.

Defining a Pool Area

config
context *context_name*
s102-service *service_name*
[no] pool-area *pool_area_name*
[no] cell-id *cell-id cell-id*
[no] hash-value { *hash_value* **| non-configured-values | range** *lower_hash_value* **to** *higher_hash_value* **} { msc** *msc_name* **}**
[no] msc-id *msc-id*
[no] plmnid { any | mcc *mcc_id* **mnc** *mnc_id* **}**
end

Notes:

- **pool-area** *pool_area_name* enter a string of 1 through 63 alphanumeric characters to create a unique name of an MSC pool area configuration. After the command is entered, the system enters the S102-Pool-Area configuration mode.
- **cell-id** *cell-id* **[** *cell-id* **+]** enter an integer from 1 through 65535 to identify a CDMA2000 reference cell ID that you are assigning to this pool area configuration. Enter up to 24 cell IDs, separated by a single blank space, in the same command.
- **hash-value**
  - *hash_value* enter an integer from 0 through 999 to identify a specific MSC.
  - **non-configured-values msc** *msc_name* assigns all non-configured hash values to use the named MSC.
  - **range** *lower_hash_value* **to** *higher_hash_value* **msc** *msc_name* specifies the range of hash values for an MSC:
    - *lower_hash_value* enter an integer from 0 through 999 to identify the start value for a range of hash. The *lower_hash_value* must be lower than *higher_hash_value*.
    - *higher_hash_value* enter an integer from 0 through 999 to identify the end value for a range of hash. The *higher_hash_value* must be higher than *lower_hash_value*.
- *msc_id* enter an integer from 1 through 16777215 to identify the unique numeric ID for the MSC.
- **plmnid { any | mcc** *mcc_id* **mnc** *mnc_id* **}** is not operationally supported at this time. The code is included for future development.
- **no** prefix included with the command, erases the specified configuration from the MME's configuration.

Verifying Pool and Non-Pool Area Configuration

Use the **show configuration** command to view the S102 pool area and S102 non-pool area configuration. It should appear similar to the following:

```
[local]MME# show configuration
 ...
     s102-service s102test
       bind ipv4-address 123.123.123.1 port 54321
       1xrtt srvcc
       msc msc1
         ipv4-address nn2.nn2.nn2.2 port 33333
       exit
       msc msc10
         ipv4-address nn1.nn2.nn1.2 port 23272
       exit
       pool-area poolone
         cell-id 2 4 5
         hash-value 34 msc msc10
       exit
       non-pool-area np1 msc msc1 msc-id 1233 cell-id 223
       non-pool-area np3 msc msc1 msc-id 14441 cell-id 6 7 8
```

Monitoring and Troubleshooting the SRVCC for 1xRTT

Monitoring Protocol

When using the monitor protocol command, enable option 86 to see all A21 messages.

Show Command(s) and/or Outputs

show s102-service statistics name *s102_service_name*

The command noted above generates statistical output indicating the status and activity of the interface. The output generated will appear similar to the following:

```
S102-AP Statistics:
  S102-AP Data:                              Tx    ReTx    Rx
    A21-1x Air Interface Signaling message   0      0      0
     A21-Ack message                         0      0      0
Unknown MSG                                  0      0      0
Error Statistics:
  Encoding Errors:                              0
  Mismatch in Correlations:                     0
  Decoding Errors:                              0
    Missing Mandatory IEs:                      0
    Syntax Errors:                              0
  Misc Errors:                                  0
```

Bulk Statistics

Bulk statistics are described in the *Statistics and Counters Reference*.

MME Schema

The MME tracks the number of SRVCC 1xRTT calls and 4G-to-1xRTT handovers using the following variables:

- s1ap-transdata-dlinktunnel
- s1ap-recdata-ulinktunnel
- s1-ho-4gto1xrtt-cs-srvcc-attempted
- s1-ho-4gto1xrtt-cs-srvcc-success
- s1-ho-4gto1xrtt-cs-srvcc-failures

S102 Schema

The MME will use the S102 interface to tunnel the 1xRTT messages between the MME and IWS/MSC. The S102 schema has been created to track performance over this interface and includes all of the following stat variables (which are described in detail in the *Statistics and Counters Reference*) :

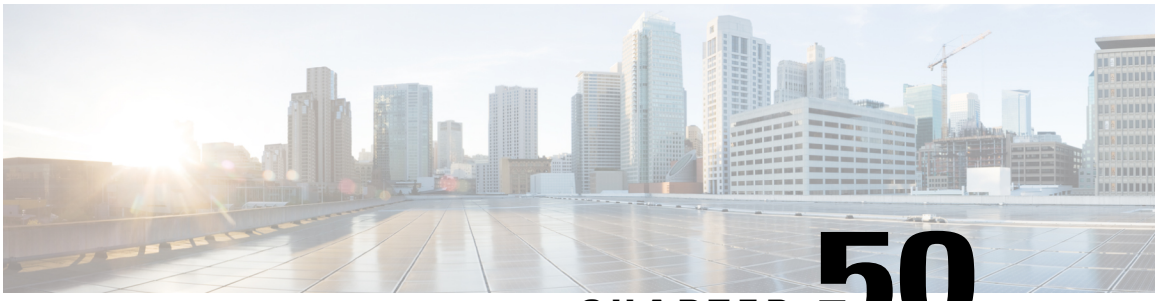
- vpnname

- vpnid
- servname
- servid
- s102ap-tx-a21-air-signal-msg
- s102ap-tx-a21-ack-msg
- s102ap-tx-a21-evt-ntfy-msg
- s102ap-tx-unknown-msg
- s102ap-retx-a21-air-signal-msg
- s102ap-retx-a21-ack-msg
- s102ap-retx-a21-evt-ntfy-msg
- s102ap-retx-unknown-msg
- s102ap-rx-a21-air-signal-msg
- s102ap-rx-a21-ack-msg
- s102ap-rx-a21-evt-ntfy-msg
- s102ap-rx-unknown-msg
- s102ap-encode-errors
- s102ap-missing-mandatory-ies
- s102ap-corelation-mismatch
- s102ap-decode-errors
- s102ap-syntax-errors
- s102ap-misc-errors

Traps

Traps are defined to indicate when an S102 service starts or stops. The trap information includes the context identification in which the S102 service is configured the unique identification of the S102 service. The following are examples of how the traps would appear :

```
Internal trap notification <XXXX> (S102ServiceStop) context S102 service s102-service
Internal trap notification <YYYY> (S102ServiceStart) context S102 service s102-service
```



CHAPTER 50

State-Location Information Retrieval Flag

The MME indicates in the ULR command that it supports State/Location Information Retrieval so the HSS sets the "EPS User State Request", "EPS Location Information Request" and "Current Location Request" bits in IDR-Flags AVP in IDR commands towards that MME. This chapter explains how the MME supports this flag.

Feature Description

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.

How It Works

MME Behavior for IDR-initiated Paging

Upon receipt of an IDR message with the "Current Location Request" bit set in the IDR-Flags AVP, the MME behavior complies with Feature-List AVP, IDR-Flags AVP, and EPS-Location-Information AVP sections as specified in 3GPP TS 29.272 v11.9.0. So when the IDR messages are received with "EPS Location Information Request" and "Current Location Request" bits set in IDR-Flags AVP, the MME sends the UE's current location information or the UE's last known location information in the "EPS-Location-Information" AVP of the IDA message

If IDR is received with "EPS Location Information Request" and "Current Location Request" flags set in IDR-Flags AVP, the MME's IDA response depends on whether :

- the UE is in connected mode with Location Reporting active making location information available, then the MME sends the IDA message without "Current-Location-Retrieved" AVP in "EPS-Location-Information" AVP.
- the UE is in connected mode without Location Reporting active so location information is not available, then the MME sends a Location-Reporting-Control message to the eNB to get the ECGI and the TAI.
  - If the MME receives a Location-Report message, then the MME sends an IDA message without "Current-Location-Retrieved" AVP and the "Age-Of-Location-Information" is set to zero in the "EPS-Location-Information" AVP sent to the HSS.
  - If the MME does not receive a Location-Report message, then the MME sends IDA message with last known location information with "Age-Of-Location-Information" AVP and without "Current-Location-Retrieved" AVP to the HSS.
- the UE is in idle mode, then the MME pages the UE to bring the UE to connected mode.
  - If paging is successful, then the MME sends an IDA message with "Age-Of-Location-Information" and "Current-Location-Retrieved" both set to zero in the "EPS-Location-Information" AVP to the HSS.
  - If paging is not successful, then the MME sends IDA messages with last known location information with "Age-Of-Location-Information" AVP and without "Current-Location-Retrieved" AVP to the HSS.

Location Reporting Control

The Location Report Control messages allow the MME to request the eNB to report where the UE is currently located.

MME's IDR-initiated Paging Process

If the UE is in ECM-IDLE and the MME receives IDR with "EPS Location Information Request" and "Current Location Request" flags set in IDR-Flags AVP, then the MME starts the ISDA guard timer (configurable for 1-100 seconds**) and also triggers the paging procedure. If the MME receives a response from the eNB before the timer expires, then MME sends an IDA message with the UE's current location information in the "EPS-Location-Information" AVP. Otherwise the MME sends an IDA message with the last known location information in "EPS-Location-Information" AVP when the ISDA timer expires. (**Configuration as of Release 17.4.)

Paging initiation is similar to paging for signaling events. However, a separate event shall be used in this case and be processed. If the paging procedure is already running for that UE, then when IDR is received with both flags set the MME shall not trigger paging again. MME behavior depends on the precedence configuration under paging-map:

- If the paging procedure already running for the UE has a higher precedence than for IDR, then when IDR is received with both flags set and if the other paging is not successful, then the MME does not trigger IDR paging again.

- If the paging procedure already running for the UE has a lower precedence than for IDR, and if IDR is received with both flags set, then the MME stops the ongoing paging procedure and triggers an IDR paging procedure.

If the paging procedure completes before the ISDA guard timer expires and a paging response is not received from the eNB, then the MME sends an asynchronous IDA response immediately without waiting for ISDA timeout.

MME's Immediate Response Through IDA

In Release 21.0 the MME responds to the IDR messages immediately with the cached location information, if the request is received within a configured amount of time. Earlier, when the MME received an IDR request for the current location of the UE, it sends a query to the eNodeB to acquire the location information of the UE, though MME had the location information available in it's cache memory.

Now, based on a configurable timer under mme-service configuration, the location information, that is, ECGI and TAI of the UE, available in the MME cache memory, is sent immediately in the IDA message. This location information is sent only if the configured timer has not expired. The eNodeB is not queried with any messages if the location information is available in the MME.

If both flags 'EPS Location Information' and 'Current Location Request' are received in the IDR, the MME immediately sends the cached location information through the IDA, if the configured timer has not expired.

This specific functionality of MME to respond immediately to the incoming IDR is license controlled. Contact your Cisco Account or Support representative for information on how to obtain a license.

Standards Compliance

The MME's support of the State/Location Information Retrieval flag complies with the following standards:

- Feature-List AVP, IDR-Flags AVP,. and EPS-Location-Information AVP sections as specified in 3GPP TS 29.272 v11.9.0

Configuring Support for the State Location Information Retrieval Flag

There is no configuration to enable or disable the MME's support of the State/Location-Information-Retrieval Flag. But, we highly recommend that you set precedence for IDR paging appropriate to your network. The significance of precedence is explained above in the *MME's IDR-initiated Paging Process* section.

Important If precedence is not configured, then the lowest precedence is automatically assigned.

Configuring Precedence for IDR Paging

Precedence for IDR paging is set using the existing **precedence** command with a special **idr** added as a paging trigger option to the signaling filter of the **traffic-type** keyword. The **precedence** command enables the operator to apply a priority for different paging-profiles based on traffic type. When a defined MME service is associated with a configured paging map, the system checks the configured profile map to determine which paging-profile to adopt for a given paging trigger, such as an IDR.

configure
lte-policy
paging-map *paging_map_name*
precedence *precedence* **traffic-type signaling [idr] paging-profile** *paging_profile_name*
no precedence *precedence*
end

Notes:

- *paging_map_name* must be an alphanumeric string of up to 64 characters to identify a unique paging map associated with the LTE Policy.
- *precedence* must be an integer from 1 (lowest precedence) to 4 (highest precedence) to specify the handling precedence for this particular configuration definition.
- **idr** option selects IDR as the signaling traffic sub-type that triggers paging. (There are several other signaling traffic-type options.)
- *paging_profile_name* must be an alphanumeric string of up to 64 characters to identify a unique paging profile associated with the paging map and the LTE Policy.
- **no precedence** *precedence* removes the precedence configuration associated with the paging-map.

Verifying the Precedence Configuration

The **show lte-policy paging-map name** *map_name* command allows you to see the precedence information configured, for example:

```
asr5000# show lte-policy paging-map name pm1
=====================================================================
  Paging Map : pm1
=====================================================================
  Precedence 1 : Signaling-IDR  Paging is performed as per paging-profile pm1
---------------------------------------------------------------------
```

Configuring the ISDA Guard Timer

isda-guard-timeout

This new command in the MME Service configuration mode enables the operator to set the number of seconds the MME waits for current location information for the UE. If the current location is not learned before expiry, because there is no paging response or location reporting control from the eNB, then the MME sends the ISDA with the last-known location upon expiry of this timer.

configure
context *context_name*

```
mme-service service_name
    [ no ] isda-guard-timeout seconds
    end
```

Notes:

- **no** prepended to the command disables any configuration for this timer and resets the wait time to the default of 25 seconds.
- Only when the ISDR is received with both location flags (current and last-known locations) set is the ISDA guard timer started. Upon expiry of this wait timer, the MME sends the ISDA with the last-known location of the UE.
- In situations where the MME receives the ISDR with only the last-known location flag set, then the MME immediately sends the ISDA with location information - no delay and this timer is not started even if configured.
- When the ISDA guard timer expires, the paging procedure does not stop until the page timer expires but the MME ignores the paging timer and sends the ISDA with the last-known location ***if*** the ISDR was received with both location flags set and the UE is in EMM-idle mode.
- While the MME is serving the ISDR (where both location flags are set) from the HSS, if the HSS tries to send another similar request then the MME responds to the HSS with DIAMETER_UNABLE_TO_COMPLY.

Configuring Location Validation Timer for IDA

loc-validity-time

This command is used to configure a timer value, with which the location information of the UE is sent immediately through the IDA message. If the current location is not learned before expiry, because there is no paging response or location reporting control from the eNB, the MME sends the IDA with the last-known location upon expiry of this timer.

```
configure
  context context_name
    mme-service service_name
      [ no ] isda loc-validity-timeout timer_value
      end
```

Notes:

- **no** disables the location validity configuration.
- *timer_value* specifies the amount of time in seconds. The timer is an integer value that ranges from 1 to 1000 seconds.
- **isda** command specifies/selects the Insert Subscriber Data Answer sent to the HSS.
- **loc-validity-time** command specifies the expiry time for the age of the UE's location information. During this time, if the EPS Location Information with current location is requested in the ISDR, the MME does not process a location procedure with the eNodeB, but sends the location information from the cache.

Verifying the Precedence Configuration

The **show lte-policy paging-map name** *map_name* command allows you to see the precedence information configured, for example:

```
asr5000# show lte-policy paging-map name pm1
=====================================================================
  Paging Map : pm1
=====================================================================
  Precedence 2 : Signaling-IDR  Paging is performed as per paging-profile pm1
---------------------------------------------------------------------
```

Monitoring the MME's Support for the State - Location Information Retrieval Flag

show mme-service statistics

Counters have been added, to the output generated by this command, to display quantitative data for successes and failures of paging initiated in response to IDR:

```
Paging Initiation for SIGNALING IDR Events:
Attempted:                  0     Success:   0
Failures:                   0
Success at Last n eNB:      0     Success at Last TAI:       0
Success at TAI List:        0
```

show mme-service all

On execution of the above command, the following fields are displayed:

```
Service Name                    : mmesvc
---------------
ISDA Gaurd Timeout              : 10s
ISDA Location Availability      : 10s
Mobile Reachable Timeout        : 3480s
---------------
```

show hss-peer-service statistics service

On executing the above command, the following fields are displayed:

```
HSS statistics for Service: mme1
Location Message Stats:
  Asynchronous ISDR Req       0    Asynchronous ISDA           0
  Asynchronous ISDA Dropped   0
  ISDR with Current Location  0    ISDA with Cached Location   0
```

Notes:

- **ISDR with Current Location:** This statistics is updated when ISDR is received with the Current Location bit set in the IDR flags.
- **ISDA with Cached Location:** This statistics is updated when an ISDR is responded with the current location information immediately from the cache, before the location validity timer expires.

show hss-peer-service statistics

In support of the new "State/Location Information Retrieval" flag functionality, counters have been added to the output generated by the **show hss-peer-service statistics** command :

- Asynchronous Message Stats:
- Asynchronous ISDR Req
- Asynchronous ISDA
- Aynchronous ISDA Dropped

Bulk Statistics

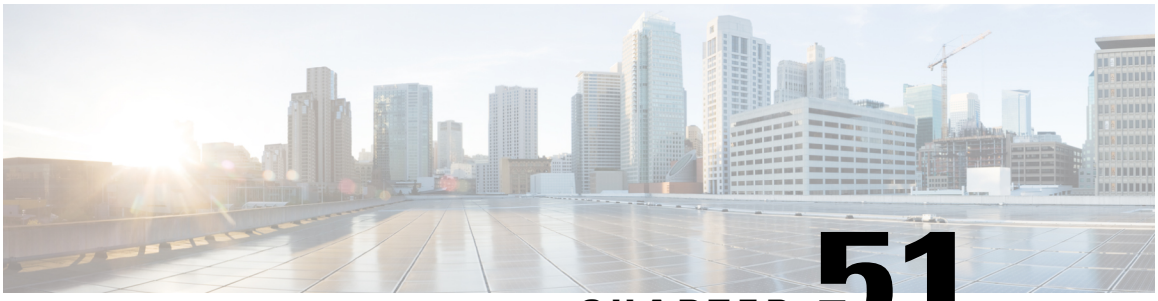
Functional descriptions, triggers and statistic type are defined for each of the bulk statistics listed below in the *Statistics and Counters Reference*.

The following bulk statistics have been added to the **MME schema** to track paging initiated in response to IDR:

- signaling-idr-paging-init-events-attempted
- signaling-idr-paging-init-events-success
- signaling-idr-paging-init-events-failures
- signaling-idr-paging-last-enb-success
- signaling-idr-paging-last-tai-success
- signaling-idr-paging-tai-list-success

The following bulk statistics have been added to the **HSS Schema** to track the location information response to the IDR:

- msg-isdr-curr-loc
- msg-isda-cached-location



CHAPTER 51

TAI-based Routing for 20-bit and 28-bit eNB ID

This feature enables MME to perform TAI-based routing for both 20-bit and 28-bit eNB IDs.

Feature Description

MME supports TAI-based routing of handover (HO) and configuration transfer messages towards Pico controller/HeNBGW when the target eNB ID is 28 bits, but it could not support TAI-based routing when the target Pico eNB ID is 20 bits.

Pico controller can transfer the target Pico eNB ID to 28 bits from 20 bits if the handover is Pico-to-Pico, but it could not handle Macro-to-Pico handover as there is no Pico Controller for Macro.

In releases 21.1 and beyond, the behavior of MME is modified so that it can perform TAI-based routing even if target home-eNB ID is 20 bits.

This feature provides a configurable option within MME service to configure target HeNB type (home or macro or both) behind HeNBGW. Based on this configuration, MME allows TAI-based lookup of target eNB, if target eNB ID is not found by MME during handover. By default, TAI-based lookup is performed only for home eNB ID (28-bits).

This feature is also introduced to support identification of target eNB using target TAI for target eNB type Macro or Pico nodes or both so that handover to such eNB can be supported if it is connected to MME through Pico controller/HeNBGW. From MME point of view, Pico controller is a Macro eNB which is using 20 bit eNB ID to support multi-cell.

Along with S1 based intra-MME HO, this feature can be applied to inter MME S1 HO procedures (inbound S10, S3 and Gn handovers). Please note that, in Gn case, MME converts target RNC ID to macro eNB ID so target TAI-based lookup for macro eNB works fine.

This feature allows operators to configure the global eNodeB IDs of HeNBGWs in the MME service. The MME uses this information to perform HeNBGW related functions. In case of S1-based handovers to home eNodeBs served by a HeNBGW, the lookup at MME for the target eNodeB based on global eNB ID will fail, as MME is aware of only the HeNBGW. In those cases, additional lookup needs to be done based on TAI to find the HeNBGW serving the home eNodeB.

Since TAI-based lookup for home or macro eNBs is supported for HeNBGWs, all such HeNBGWs should be defined in HeNBGW management database (HeNBGW-mgmt-db). The HeNBGW-mgmt-db should be associated within mme-service.

In this release, the number of HeNBGW entries in the HeNBGW-mgmt-db has been increased from 8 to 512.

Limitations

The following are the limitations of this feature:

- TAI-based lookup is performed only for home eNB.
- TAI should be unique and should not be shared across multiple HeNBGWs. If the TAIs are shared, then any one of the target eNBs sharing the TAC under consideration will be chosen during TAI-based target eNB selection and handover to the eNB might fail.

Configuring TAI-based Lookup of eNB

The following section provides the configuration commands to enable the TAI-based lookup of eNB.

Configuring Target eNB Type for TAI-based Lookup

Use the following configuration commands to configure the target eNB type or target henb-type as home or macro.

```
configure
  context context_name
    mme-service service_name
      henbgw henb-type { macro-enb | home-enb | all }
      end
```

Notes:

- The **henbgw henb-type { macro-enb | home-enb | all }** is a new CLI command introduced in 21.1 release to support TAI-based lookup functionality.
- **henbgw**: Configures Home eNodeB gateway options.
- **henbgw-type**: Configures HeNB type. TAI-based lookup depends on HeNB type.
  - **home-enb**: Configures HeNB type home-enb (28-bits)
  - **macro-enb**: Configures HeNB type macro-enb (20-bits)
  - **all**: Configures HeNB type both macro-enb (20-bits) and home-enb (28-bits)
- By default, when the **henbgw henb-type** command is not applied explicitly, target eNB type is set as home-enb.
- Use the **no henbgw henb-type** command to delete the existing configuration, if previously configured.
- The target eNB type configuration is effective only when the **henbgw henb-type** CLI command is configured within mme-service and the HeNBGW-mgmt-db is associated with HeNBGWs inside mme-service.

Verifying the Target eNB Type Configuration

Use the following commands to verify the configuration status of this feature.

show mme-service all
- or -

show mme-service name *service_name*
service_name must be the name of the MME service specified during the configuration.

This command displays all the configurations that are enabled within the specified MME service.

The following is a sample configuration of this feature.

```
configure
  lte policy
    mme henbgw mgmt-db db_name
      henbgw-global-enbid mcc 123 mnc 456 enbid 12345
      henbgw-global-enbid mcc 123 mnc 456 enbid 12543
      end
configure
  context context_name
    mme-service service_name
      henbgw henb-type macro-enb
      associate henbgw-mgmt-db henbdb
      end
```

Notes:

- By default, when the **henbgw henb-type** command is not configured, target eNB type is set as home-enb.

Monitoring and Troubleshooting the TAI-based Lookup

This section provides information regarding show commands and/or their outputs in support of this feature.

The following operations can be performed to troubleshoot any failure related to this feature:

- Verify if the feature is enabled using **show mme-service all** CLI command. If not enabled, configure the **henbgw henb-type** CLI command in MME service Configuration mode and check if it works.
- Collect and analyze the output of **show configuration**, **show support details**, **show mme-service name** *service_name* and **show mme-service statistics handover** commands. Also, check the reported logs, if any. For further analysis, contact Cisco account representative.
- Check and analyze the debug logs for mme-app, s1ap, mmemgr, and mmedemux facilities to determine if TAI-based lookup fails for a particular TAI.

show mme-service all

The following field is added to the output of the **show mme-service all** command in support of this feature.

```
HENBGW HeNodeB Type: macro-enb
```

Table 16: show mme-service all Command Output Descriptions

Field	Description
HENBGW HeNodeB Type	Displays the configured type for HeNodeB gateway. HENBGW HeNodeB Type can be one of the following: • macro-enb • home-enb • all

show mme-service name *service_name*

The following field is added to the output of the **show mme-service name** *service_name* command in support of this feature.

```
HENBGW HeNodeB Type: macro-enb
```

Table 17: show mme-service name service_name Command Output Descriptions

Field	Description
HENBGW HeNodeB Type	Displays the configured type for HeNodeB gateway. HENBGW HeNodeB Type can be one of the following: • macro-enb • home-enb • all

show mme-service statistics handover

The following fields are added to the output of the **show mme-service statistics handover** command in support of this feature.

```
Handover Statistics:
  Intra MME Handover
    .
    .
    Target TAI based S1 handover
      Attempted:       4
      Success:         3
      Failures:        1
.
.
  EUTRAN<-> EUTRAN using S10 Interface:
    .
```

```
    .
    Inbound relocation using Target TAI based S1 HO procedure:
      Attempted:       0
      Success:         0
      Failures:        0
```

Table 18: show mme-service statistics Command Output Descriptions

Field	Description
Target TAI based S1 handover	
Attempted	Displays the total number of attempted intra MME S1 handovers that used target TAI to identify the target HeNodeB, if target eNB ID is unknown.
Success	Displays the total number of successful intra MME S1 handovers that used target TAI to identify the target HeNodeB.
Failures	Displays the total number of failed intra MME S1 handovers that used target TAI to identify the target HeNodeB.
Inbound relocation using Target TAI based S1 HO procedure	
Attempted	Displays the total number of attempted inter MME S10 handovers where target MME used target TAI to identify the target HeNodeB, if target eNB ID is unknown.
Success	Displays the total number of successful inter MME S10 handovers where target MME used target TAI to identify the target HeNodeB.
Failures	Displays the total number of failed inter MME S10 handovers where target MME used target TAI to identify the target HeNodeB.

show mme-service statistics peer-id

The following fields are added to the output of the **show mme-service statistics peer-id** *peer_id* **handover** command in support of this feature.

```
Handover Statistics:
  Intra MME Handover
    .
    .
    Target TAI based S1 handover
      Attempted:       4
      Success:         3
      Failures:        1
.
.
```

```
EUTRAN<-> EUTRAN using S10 Interface:
  .
  .
  Inbound relocation using Target TAI based S1 HO procedure:
    Attempted:       0
    Success:         0
    Failures:        0
```

Table 19: show mme-service statistics Command Output Descriptions

Field	Description
Target TAI based S1 handover	
Attempted	Displays the total number of attempted intra MME S1 handovers that used target TAI to identify the target HeNodeB, if target eNB ID is unknown.
Success	Displays the total number of successful intra MME S1 handovers that used target TAI to identify the target HeNodeB.
Failures	Displays the total number of failed intra MME S1 handovers that used target TAI to identify the target HeNodeB.
Inbound relocation using Target TAI based S1 HO procedure	
Attempted	Displays the total number of attempted inter MME S10 handovers where target MME used target TAI to identify the target HeNodeB, if target eNB ID is unknown.
Success	Displays the total number of successful inter MME S10 handovers where target MME used target TAI to identify the target HeNodeB.
Failures	Displays the total number of failed inter MME S10 handovers where target MME used target TAI to identify the target HeNodeB.

Bulk Statistics

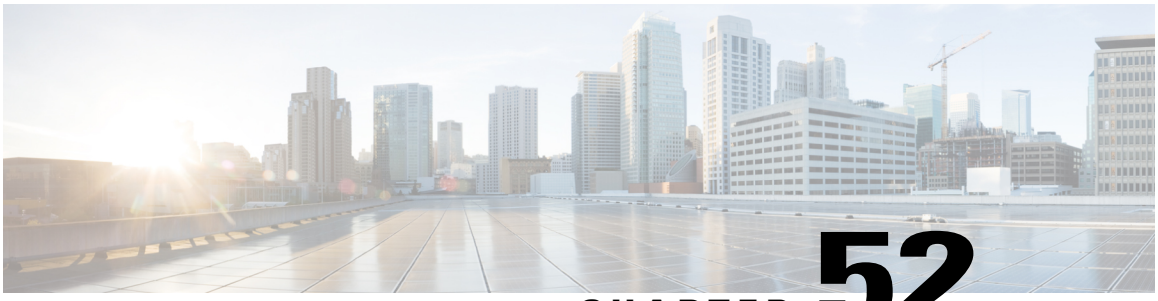
MME Schema

The following bulk statistics have been added to the MME schema to track the TAI-based lookup attempts, successes and failures during intra-MME S1 and inter-MME inbound S10 handovers:

- emmevent-s1ho-target-tai-attempt

- emmevent-s1ho-target-tai-success
- emmevent-s1ho-target-tai-failure
- in-s1-ho-4gto4g-s10-target-tai-attempted
- in-s1-ho-4gto4g-s10-target-tai-success
- in-s1-ho-4gto4g-s10-target-tai-failures

For detailed information on these bulk statistics, refer to the **BulkstatStatistics_documentation.xls** spreadsheet that is included as part of the software companion package for this release.



CHAPTER 52

Timer-based GBR Bearer Deactivation

Feature Description

The Timer-based GBR Bearer Deactivation, a proprietary feature of StarOS, allows MME to retain dedicated bearers of a User Equipment (UE) when eNodeB sends a S1-AP Context Release to enable the UE to resume a VoLTE call on receiving a new Service Request or RCC Connection. For example, if a subscriber is out of coverage for a short period of time during a VoLTE call, the GBR bearer would be retained and the session is not lost.

MME provides a configurable timer for which the GBR bearers are preserved when a UE Context Release Request message with "Radio Connection With UE Lost" cause code is received from the eNodeB. MME preserves the GBR bearers for the configured time.

A valid license key is required to enable this feature. Contact your Cisco Account or Support representative for information on how to obtain a license. This license was not enforced in earlier releases.

How It Works

When MME receives a UE Context Release Request with "Radio Connection With UE Lost" cause code from the eNodeB to initiate the S1 Release procedure for a UE, the MME is configurable to preserve GBR bearers of the UE for a time ranging from 1 - 600 seconds. The configurable range of time avoids time consumption during bearer reestablishment if the UE reconnects within the given time.

Based on operator policy, in case of eNodeB failure, the MME either preserves all the bearers or initiate the Dedicated Bearer Deactivation procedure for GBR bearers. This functionality is provisioned in the Call Control Profile.

Limitations

Negligible amount of memory is affected because the GBR bearers are preserved for the configured amount of time instead of being released.

Configuring Timer-based GBR Bearer Deactivation

This section documents configuration of Timer-based GBR Bearer Deactivation and its related functionality.

Configuring Timer-based GBR Bearer Deactivation

The Timer-based GBR Bearer Deactivation is configured in the Call Control Profile configuration mode.

The following CLI command allows the user to configure the timer, which defines the time allowed for the GBR bearers to be preserved when the UE Context Release Request message with the "Radio Connection With UE Lost" cause code is received from eNodeB.

gbr-bearer-preservation-timer

The Timer-based GBR Bearer Deactivation is configured in the Call Control Profile Configuration Mode. The **gbr-bearer-preservation-timer** command allows the user to configure the timer, which defines the time allowed for the GBR bearers to be preserved when the UE Context Release Request message with the "Radio Connection With UE Lost" cause code is received from eNodeB.

configure
call-control-profile *profile_name*
gbr-bearer-preservation-timer *timer_value*
[remove] gbr-bearer-preservation-timer
end

Notes:

- The **gbr-bearer-preservation-timer** command allows the operator to set the preservation time for the bearer on receiving the UE Context Release with the "Radio Connection With UE Lost" cause code.
- The *timer_value* specifies the duration for preserving the bearers in seconds. It is an integer value ranging from 1 to 600.
- **remove** disables the timer configuration.

Verifying the Timer-based GBR Bearer Deactivation Configuration

The following section describes command available to verify Timer-based GBR Bearer Deactivation configuration on the MME.

show call-control-profile full name *test*
On running the above show command the full configuration for the call control profile is displayed. The following fields relate to this feature:

```
GMM-T3346 Timer
Min Value : Not Configured
```

```
Max Value : Not Configured
TCP Maximim Segment Size : Not Configured
GBR Bearer Preservation Timer : 10s
```

Monitoring and Troubleshooting the Timer-based GBR Bearer Deactivation

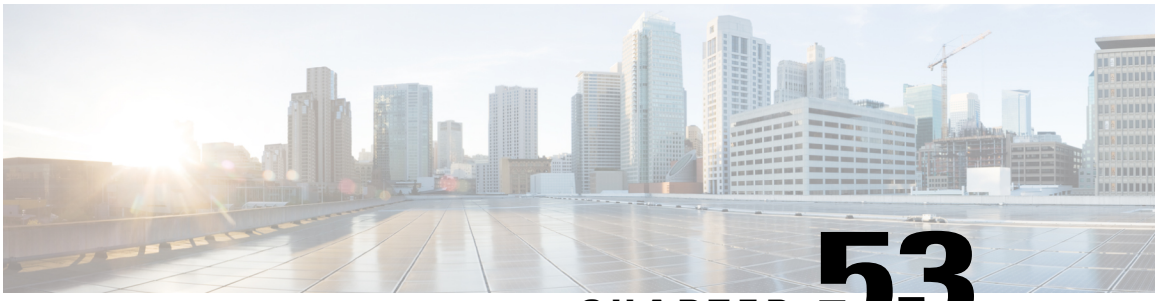
The following sections describe commands available to monitor or troubleshoot Timer-based GBR Bearer Deactivation on the MME.

Troubleshooting Timer-based GBR Bearer Deactivation

To troubleshoot the Timer-based GBR Bearer Deactivation feature, use the following instructions:

- Verify if the feature is enabled or not by executing the following command:
  show call-control-profile full name *test*
  If the **GBR Bearer Preservation Timer** field displays the configured timer value, then the feature is considered to be enabled, else disabled.
- To raise a trouble ticket, collect the output of the following show commands:
  show configuration

  show call-control-profile full all



CHAPTER 53

UDPC2 Support for MME/SGSN

This chapter includes the following topics:

Feature Description

The MME and SGSN now support the UDPC2 hardware. The maximum number of MME managers supported per chassis on ASR 5500 with DPC is 24, to support UDPC2 on ASR 5500 the maximum number of MME managers have been increased to 36.

The CLI command **task facility mmemgr per-sesscard-density { high | normal }** under the Global configuration mode is used to configure the density (number of MME managers) of MME managers per session card. The disadvantage of this command is it does not allow configuration of specific number of MME managers per card, but allows the operator to configure only high or normal density. This CLI is deprecated and new CLI commands are introduced to provide the operator with more flexibility to configure number of MME managers per active session cards (or per active session VM in case of VPC) and the total number of MME managers. The MME managers are now moved to Non-Demux card, therefore the number of managers depends on the number of session cards per chassis. The new CLI command enables the operator to spawn the maximum or desired number of MME managers even when the chassis is not fully loaded in the case of ASR 5K and ASR 5500 platforms. For VPC DI the operator can restrict max number of MME managers per chassis, if operator desires to scale with more session VMs without requiring additional MME managers.

In UDPC2, the number of Session Managers in ASR5500 is increased from 336 to 1008.

Note The StarOS does not support an ASR5500 deployment with mixed usage of DPC and DPC2 cards. All session cards in one ASR5500 have to be of the same type.

Note All product specific limits, capacity and performance, will remain same as compared to ASR5500 with DPC.

MME Scaling on DPC2 to 2xDPC

This feature enhancement provides improved CEPS (Call Events Per Second) and session capacity utilization for MME/SGSN on the ASR5500 DPC2 platform. It is observed that the current MME/SGSN deployments limit the maximum session/subscriber capacity utilization as the CPU reaches its maximum threshold for some proclets though sufficient memory is available in the system and in the proclet for additional sessions/subscribers. With this enhancement, the session utilization capacity is doubled (2X) on the ASR5500 DPC2 platform for a specific call model.

This feature has increased the limits for the following MME/SGSN specific proclets on ASR5500 DPC2 platform:

- The maximum number of MME managers per chassis has been increased to "48" on ASR5500 DPC2 platform.
- The maximum number of MME managers per Non-Demux card has been increased to "8" on ASR5500 DPC2 platform.
- The maximum number of IMSI managers per Demux card has been increased to "8" on ASR5500 DPC2 platform.

MMEMGR Scaling on DPC

In this feature enhancement, the load on the MME managers are distributed widely with the increase in the number of MME managers. This enhancement is most likely seen in a standalone MME deployment, where the difference in the usage of MME manager CPU and Session Manager CPU is apparent.

This feature has increased the limits of the following MME/SGSN proclets on the ASR5500 DPC Platform:

- The maximum number of MME managers per chassis has been increased to "36" on the ASR5500 DPC platform.

How It Works

In previous releases, the number of MME managers for a platform is pre-defined and not configurable. The operator can now configure the desired number of MME managers defined for each platform. A new CLI command **task facility mmemgrs max** *value* is introduced to configure the number of MME managers. If the operator does not configure the desired number of MME managers, a default number of pre-defined MME managers will be configured on the chassis. The table below depicts the default and maximum number of MME managers per chassis for each platform:

Platform	Default max. number of MME Managers per chassis	Maximum number of MME Managers per chassis.
ASR 5000	12	12

Platform	Default max. number of MME Managers per chassis	Maximum number of MME Managers per chassis.
ASR 5500 with DPC	24	36 **Note** Releases prior to 21.1, the maximum number of MME Managers per chassis supported was only "24".
ASR 5500 with DPC2	48 **Note** Releases prior to 21.0, the default number of MME Managers per chassis supported was only "36".	48 **Note** Releases prior to 21.0, the default number of MME Managers per chassis supported was only "36".
SSI MEDIUM/LARGE	2	2
SSI SMALL	1	1
SCALE MEDIUM/LARGE	24	48 **Note** : Releases prior to 20.0, the maximum number of MME Managers per chassis supported was only "24".

In previous releases the number of MME managers for a session card could be configured based only on the density per session card/VM. With the introduction of the CLI command **task facility mmemgr per-sesscard-count** *number* the operator can now configure the number of MME Managers per session card. If the operator does not configure the desired number of MME managers per session card, a default number of MME managers will be spawned on the session card. The table below depicts the default and maximum number of MME managers configurable per session card for different platforms/cards:

Platform	Default number of MME Managers per session card	Maximum number of MME Managers per session card
ASR 5000 PSC/PSC2/PSC3	1	2
ASR 5500 with DPC	4	6
ASR 5500 with DPC2	8 **Note** Releases prior to 21.0, the default number of MME managers per session card supported was only "6".	8 **Note** Releases prior to 21.0, the default number of MME managers per session card supported was only "6".
SSI MEDIUM/LARGE	2	2

Platform	Default number of MME Managers per session card	Maximum number of MME Managers per session card
SSI SMALL	1	1
SCALE MEDIUM/LARGE	1	2

Configuring the number of MME managers helps to scale the number of eNodeB connections.The maximum number of eNodeB connections supported by MME is 128K per ASR5500 chassis. Having more number of MME managers ensure better CPU utilization, load balancing across MME managers and improved message communication between Session managers and MME managers.

Configuring MME/SGSN Support on UDPC2

The following CLI command is deprecated from release 19.2 onwards. It was introduced in release 18.0 and is valid till release 19.0. When an operator using this configuration command upgrades to release 19.2, this CLI is mapped to a new CLI command **task facility mmemgr per-sesscard-count** *count*.

configure
task facility mmemgr per-sesscard-density { high | normal }
exit

This CLI command is deprecated as it does not allow the operator to configure the required number of MME managers per session card. This command only allows two predefined modes of either "high" or "normal" density.

New commands are introduced to provide more flexibility to the operator to configure required number of MME managers per session card and to configure the desired number of MME managers per chassis.

The following CLI command is introduced to configure the desired number of MME managers per session card:

configure
task facility mmemgr per-sesscard-count *count*
default task facility mmemgr per-sesscard-count
exit

Notes:

- The maximum number of MME managers that can be configured per session card varies based on the platform/VM and card type. However, the upper limit of MME managers that can be configured per session card is set to "6" for releases up to 20.0 and to “8” from release 21.0 onwards.
- This configuration change will be effective only after a chassis reload. The operator must save the configuration changes prior to a reload. The system issues appropriate warnings to the operator to indicate that configuration changes must be saved and the changes will be effective only after a chassis reload.
- This command is not specific to any platform or card type. It is applicable and available to all platforms and card types.
- The keyword **default** resets the number MME managers per session card to the default number of MME managers per session card/VM. By default this CLI is not configured. When this CLI is not configured default number of MME managers per session card will be selected based on platform and card type. Listed below are the default values:

Platform/VM and card type	Default number of MME managers per session card
ASR5000 PSC/PSC2/PSC3	1
ASR 5500 DPC	4
ASR 5500 DPC2	8 **Note** Releases prior to 21.0, the default number of MME managers per session card supported was only "6".
SSI MEDIUM/LARGE	2
SSI SMALL	1
SCALE LARGE/MEDIUM	1

- The keyword **per-sesscard-count** *count* is used to set the maximum number of MME managers per session card.
  - The value of *count* is an integer with range "1" up to "6" for releases up to 20.0 and to “8” from release 21.0 onwards.

Listed below is the maximum number of MME managers allowed per session card based on the platform/VM and card type:

Platform/VM and card type	Maximum number of MME managers per session card
ASR5000 PSC/PSC2/PSC3	2
ASR 5500 DPC	6
ASR 5500 DPC2	8 **Note** Releases prior to 21.0, the maximum number of MME managers per session card supported was only "6".
SSI MEDIUM/LARGE	2
SSI SMALL	1
SCALE LARGE/MEDIUM	2

Usage example:

Listed below is an example where 3 MME managers are configured per session card on an ASR5500 platform with DPC2 card:

task facility mmemgr per-sesscard-count 3

Listed below is an example where default number of MME managers configured per session card on an ASR5500 platform with DPC card:

default task facility mmemgr per-sesscard-count

The following CLI command is introduced configure desired number of MME managers per chassis:

configure
task facility mmemgr max *value*
default task facility mmemgr max
exit

Notes:

- This configuration change will be effective only after a chassis reload. The operator must save the configuration changes prior to a reload. The system issues appropriate warnings to the operator to indicate that configuration changes must be saved and the changes will be effective only after a chassis reload.
- The maximum number of MME managers that can be configured per chassis is varies based on the platform. However, the upper limit of MME managers per chassis is set to 48.

Note Note: For releases prior to 20.0 the upper limit of MME managers per chassis was set to "36".

- This CLI is not configured by default. The keyword default resets the number of MME managers per chassis to the default values. Listed below are the default values:

Platform/VM and card type	Default number of MME managers per chassis
ASR5000	12
ASR 5500 DPC	24
ASR 5500 DPC2	48 **Note** For releases prior to 21.0 the default number of MME managers per chassis was “36”.
SSI MEDIUM/LARGE	1
SSI SMALL	1
VPC-DI or SCALE LARGE/MEDIUM	24

- The keyword **max value** is used to set the maximum number of MME managers per chassis.
  - The maximum *value* is an integer with range 1 up to 48.

Note Note: For releases prior to 20.0 the upper limit of MME managers per chassis was set to "36".

Listed below is the maximum number of MME managers allowed per chassis based on the platform/VM and card type:

Platform/VM and card type	Maximum number of MME managers per chassis
ASR5000	12
ASR 5500 DPC	36 **Note** For releases prior to 21.1 the maximum number of MME managers per chassis was “24”.
ASR 5500 DPC2	48 **Note** For releases prior to 21.0 the default number of MME managers per chassis was “36”.
SSI MEDIUM/LARGE	2
SSI SMALL	1
VPC-DI or SCALE LARGE/MEDIUM	48 **Note** Releases prior to 20.0, the maximum number of MME Managers per chassis supported was only "24".

Usage example:

Listed below is an example where 5 MME managers are configured per chassis on an ASR5500 platform with DPC2 card:

task facility mmemgr max 5

Listed below is an example where default number of MME managers configured per chassis on an ASR5500 platform with DPC card:

default task facility mmemgr max

Verifying the Configuration

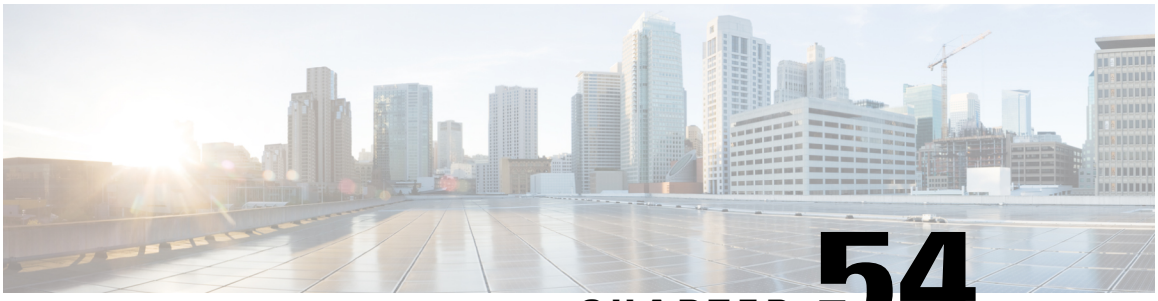
The **show configuration** command is used to verify the configuration of this feature. The output displays the configured values of number of MME managers per chassis or number of MME managers per session card.

If "5" MME managers are configured per chassis the following output is displayed on issuing the **show configuration** command:

task facility mmemgr max 5

If "2" MME managers are configured per session card the following output is displayed on issuing the show configuration command:

task facility mmemgr per-sesscard-count 2



CHAPTER 54

UE Relocation

This chapter describes how to relocate UEs to a specific MME in an MME pool.

Feature Description

This feature enables operators to move a UE between different MME nodes within a MME pool area. This functionality can be useful for maintenance of equipment, to allow testing on all components, verifying functionality on new nodes that are not in service yet (when expanding the pool), and for establishing a particular call scenario for troubleshooting.

How it Works

UE Relocation

Using this command, the MME can release a UE (based on the UE"s IMSI), and cause it to attach to another particular MME within an MME Pool Area.

The UE must be in the EMM-REGISTERED or ECM-CONNECTED state in order to be relocated. If the UE is not in either of these states, the command will be rejected.

If the UE is in ECM-CONNECTED state, the MME uses the GUTI relocation command with a GUTI constructed from the parameters of the **mme relocate-ue** command. Once confirmation is received from the UE, the UE is detached with detach type "re-attach required". If the GUTI relocation procedure fails, the UE is still detached from the network.

Relocating UE to Specific MME

Issuing the mme relocate-ue Command

Use this exec mode command to trigger the specified UE (IMSI) to detach from the current MME and to reattach to the target MME.

You must know the mme-group-id and mme-code of the target MME. You must also know the IMSI of the UE to be relocated and provide a new GUTI MME-TMSI for this UE.

This is a one-time executable command. The MME does not retain a record of UEs which have been targeted for relocation. There is no restriction on the number of UEs that can be relocated.

mme relocate-ue imsi *imsi* **new-guti mme-group-id** *grp_id* **mme-code** *mme_code* **m-tmsi** *mtmsi*
Notes:

- If the UE is not in EMM-REGISTERED or ECM-CONNECTED mode, the command is rejected.
- **new-guti mme-group-id** *grp_id* identifies the group to which the target MME belongs. Enter an integer from 0 through 65536. (Note that with StarOS Releases prior to 16.5, 17.4, and 18.2, the valid range for the MME Group ID was limited to 32768 through 65536.)
- **mme-code** *mme_code* identifies the target MME to which the UE should be attached. Enter an integer from 0 through 255.
- **m-tmsi** *mtmsi* identifies the new GUTI MME-TMSI for the UE. Enter an integer from 0 through 4294967295.
- If the UE is not in EMM-REGISTERED or ECM-CONNECTED mode, the command is rejected.
- If the mme-group-id and mme-code correspond to the MME where the UE is currently registered, the command is rejected.

Monitoring UE Relocation

This section lists the bulk statistics and show commands that display UE relocation statistics for a given MME.

UE Relocation Bulk Statistics

The following statistics are included in the **MME** Schema to track UE Relocations:

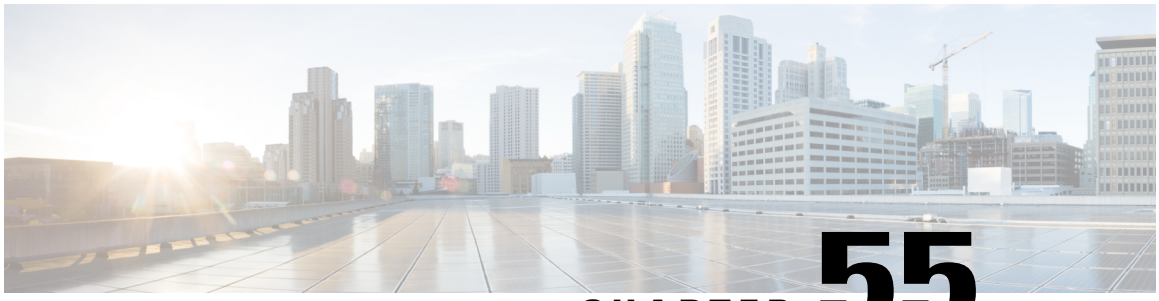
emm-msgtx-guti-reloc	The total number of EMM control messages sent - GUTI relocations. **Type:** Counter	Int32
emm-msgtx-guti-reloc-retx	The total number of EMM control messages sent - retransmitted GUTI relocations. **Type:** Counter	Int32

emm-msgrx-guti-reloc-complete	The total number of EMM control messages received - GUTI relocation complete. **Type:** Counter	Int32

UE Relocation Show Commands

The following counters are included in the **show mme-service statistics** output in support of the UE Relocation feature:

Total EMM Control Messages	
GUTI Relocation	The total number of EMM GUTI Relocation messages sent for a specific ECM event associated with all MME services on the system.
Retransmissions	The total number of retransmitted EMM GUTI Relocation messages sent for a specific ECM event associated with all MME services on the system.
GUTI Reloc Complete	The total number of EMM GUTI Reloc Complete messages received for a specific ECM event associated with all MME services on the system.
EMM (Evolved Mobility Management) Statistics	
GUTI Relocation	This sub-group displays all GUTI relocation event attempts/successes/failures associated with all MME services on the system.



CHAPTER 55

VLR Management

This chapter describes various MME features that provide additional resiliency of the Circuit Switched Fallback (CSFB) service, relating to the management of Visitor Location Registers (VLRs).

Feature Description

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

Passive VLR Offloading

The MME provides the ability for an operator to enable or disable "offload" mode for a specified VLR. This capability enables operators to preemptively move subscribers away from an SGs interface associated with a VLR which is planned for maintenance mode. When this offload command is set on the MME, all sessions matching this VLR are marked with a "VLR offload" flag. During the next UE activity, the MME requires each UE to perform a combined TAU/LAU. This feature is available to all VLRs, both non-pooled VLRs as well as those configured within an MME LAC pool area.

The VLR offload functionality and MME offload functionality cannot be performed at the same time; activation of one prevents activation of the other (and vice versa).

Active VLR Offloading

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. This feature is available to all VLRs, both non-pooled VLRs as well as those configured within an MME LAC pool area.

The VLR offload functionality and MME offload functionality cannot be performed at the same time; activation of one prevents activation of the other (and vice versa).

UE Detach on VLR Recovery

The MME supports the ability to perform a controlled release of UEs when a failed VLR becomes active again. This feature is available to all VLRs, both non-pooled VLRs as well as those configured within an MME LAC pool area.

This applies to UEs that are currently registered as EPS-Only. This enables the UE to return to a combined attached state to restore SMS services.

UE Detach on VLR Failure

The MME supports the ability to perform a controlled release of UEs when an active VLR connection fails. This applies to CSFB UEs that are currently registered to the VLR that failed. This feature is available to all VLRs, both non-pooled VLRs as well as those configured within an MME LAC pool area.

This enables the UE to return to a combined attached state on a different VLR.

Enabling VLR Offloading

Enabling Passive VLR Offloading

The following Exec mode command instructs the MME to mark UEs associated with the specified VLR with a "VLR offload" flag. This enables the MME to preemptively move subscribers away from an VLR which is scheduled to be put in maintenance mode.

sgs offload sgs-service *service-name* **vlr** *vlr-name* **start time-duration 0 [-noconfirm]**
The following command stops the marking of subscribers associated with the specified VLR to an offload state.

sgs offload sgs-service *service-name* **vlr** *vlr-name* **stop [-noconfirm]**
Notes:

- A **time-duration** value of 0 enables Passive VLR Offloading only.
- More than one VLR may be offloaded at the same time.
- VLR Offloading and MME offloading cannot be performed at the same time.

Enabling Active VLR Offloading

The following Exec mode command instructs the MME to mark UEs associated with the specified VLR with a "VLR offload" flag, and begin detaching these UEs according to the time-duration specified in the command. Affected UEs are detached and required to reattach to another VLR.

sgs offload sgs-service *service-name* **vlr** *vlr-name* **start time-duration** *duration* **[-noconfirm]**

The following command stops active VLR offloading for UEs associated with the specified VLR.

sgs offload sgs-service *service-name* **vlr** *vlr-name* **stop [-noconfirm]**
Notes:

- A **start time-duration** *duration* entry must be an integer from 1 through 3000 to enables Active VLR Offloading and Passive VLR Offloading. The MME splits this time duration into *n* intervals, 5 seconds apart. A maximum of 50 subscribers will be actively detached per interval. For example, a setting of 120 minutes with 60000 subscribers would process all subscribers in 100 minutes. Any subscribers remaining at the expiry of the time-duration will not be detached, but will be marked with the "VLR offload" flag.
- VLR Offloading and MME offloading cannot be performed at the same time.

Verifying VLR Offload Status and Configuration

The following command displays VLR offload statistics for the specified SGs service.

show sgs-service offload-status service-name *sgs_svc_name*
The following sample output shows VLR Offload related statistics.

```
[local]asr5x00# show sgs-service offload-status service-name sgssvc
VLR Name                  : vlr1
VLR Offload               : Yes
Offloaded Count           : 31678
Total Count               : 43051
VLR Name                  : vlr2
VLR Offload               : No
Offloaded Count           : 0
Total Count               : 45789
```

To clear the counters displayed by the previous command, issue the following command.

clear sgs-service offload-status service-name *sgs_svc_name*
When Passive or Active VLR Offload is enabled, the following command displays the "VLR Offload" flag for the specified VLR.

show mme-service session vlr-name *vlr_name*
The following output shows the VLR Offload flag enabled.

```
[local]asr5x00# show mme-service session vlr-name vlr1
   CSFB Information:
        SGS Assoc State:    SGs-ASSOCIATED
        SGS Service:        sgssvc
        VLR:                vlr1
        LAI:                123:456:200
        Pool Area:          pool1
        Non-Pool Area:      N/A
        P-TMSI:             0x1
        Flags:
   VLR Reliable Indicator
   VLR Offload
```

The following command shows the offload state of all VLRs on the system.

show sgs-service vlr-status full

```
[local]asr5x00#  show sgs-service vlr-status full
MMEMGR                        : Instance 6
MME Reset                     : Yes
Service ID                    : 2
Peer ID                       : 100794369
VLR Name                      : vlr1
SGS Service Name              : test
SGS Service Address           : 192.60.60.25
SGS Service Port              : 29118
VLR IP Address                : 192.60.60.6
```

```
VLR Psgsort                    : 29118
Assoc State                    : DOWN
Assoc State Up Count           : 2
VLR Offload                    : No
```

To clear the counters displayed by the previous command, issue either of the following commands. The first command clears statistics for all VLRs, while the second command clears statistics for the specified VLR only.

clear sgs-service vlr-status service-name *sgs_svc_name*
clear sgs-service vlr-status vlr-name *vlr_name*

Enabling UE Detach on VLR Failure or VLR Recover

UE Detach on VLR Recovery

The following Exec mode command instructs the MME to automatically perform active recovery of UEs when a failed VLR becomes responsive again.

sgs vlr-recover sgs-service *sgs_svc_name* **duration** *duration* **backoff-timer** *time* **[-noconfirm]**
Notes:

- When this command is issued, the MME monitors the availability of all VLRs. If a failed VLR become available again, the MME attempts to recover UEs that failed while the VLR was unavailable with an EPS Detach.
- When a VLR is down, and a UE needs to associate with the VLR that went down, the UE will be downgraded to EPS-Only-Attach when initially attaching. This command should be issued after the VLR recovers.
- UEs which required CSFB (voice) and were downgraded as a result of the VLR being down will not be affected by this command. This command remains active until it is disabled with the **no sgs vlr-recover** command.
- **duration** *duration* Specifies the number of minutes during which all qualifying UEs will be recovered.

  The MME splits this duration into *n* intervals, 5 seconds apart. A maximum of 50 subscribers are processed per interval. For example, a setting of 2 minutes with 100 subscribers would result in the MME processing all subscribers in the first 2 intervals (10) seconds. Any subscribers remaining at the expiry of the duration will not be processed.
- **backoff-timer** *time* Specifies the number of seconds that the MME will wait, following the detection of a recovered VLR, before starting the VLR recovery actions.
- Refer to the *sgs vlr-recover* command in the Exec Mode chapter of the *Command Line Interface Reference* for more information.

The command listed below disables the **sgs vlr-recover** functionality.

no sgs vlr-recover sgs-service *sgs_svc_name* **[-noconfirm]**

UE Detach on VLR Failure

This functionality can be enabled manually, on an as-needed basis, using an Exec mode command, or it can be made a persistent configuration via an SGs Service Configuration Mode command. The following two sections describe how to configure each method (automatic and manual).

Important The MME will report a command line interface error (Invalid operation: VLR already set for failure.) if an attempt is made to configure/enable both methods simultaneously.

Configuring Automatic UE Detach on VLR Failure

The following commands configure the MME to automatically detect a VLR failure and initiate the controlled release of CSFB UEs. The configuration of this feature also allows a UE detach rate (UEs per second) to be defined.

configure
context *context_name*
sgs-service *sgs_svc_name*
vlr-failure duration *minutes* **backoff-timer** *seconds* **detach-rate** *number* **[-noconfirm]**
end

The following commands disable this configuration:

configure
context *context_name*
sgs-service *sgs_svc_name*
no vlr-failure [-noconfirm]
end

Refer to the **vlr-failure** command in the *MME SGs Service Configuration Mode Commands* chapter of the *Command Line Interface Reference* for more information.

Manually Enabling UE Detach on VLR Failure

The following Exec mode command instructs the MME to perform controlled release of CSFB UEs connected to a VLR when a VLR becomes unavailable.

sgs vlr-failure sgs-service *sgs_svc_name* **duration** *duratioin* **backoff-timer** *time* **[-noconfirm]**
Notes:

- When enabled, the MME monitors the availability of all VLRs. If one or more VLRs become unavailable, the MME performs a controlled release (EPS IMSI detach) for all UEs associated with that VLR. If another VLR is available, the MME sends a combined TA/LA Update with IMSI attach.
- **duration** *duration* Specifies the number of minutes during which all qualifying UEs will be detached. Enter an integer from 1 to 3000.

  The MME splits this duration into *n* intervals, 5 seconds apart. A maximum of 50 subscribers are processed per interval. For example, a setting of 2 minutes with 100 subscribers would result in the MME processing all subscribers in the first 2 intervals (10) seconds. Any subscribers remaining at the expiry of the duration will not be processed.

- **backoff-timer** *time* Specifies the number of seconds the MME will wait following the detection of a VLR condition before starting the controlled release of affected UEs. Enter an integer from 1 through 3000.
- **detach-rate** This optional keyword specifies a maximum number of detaches to perform per 5 second cycle. **Note:** This keyword is available only for the **vlr-failure** command in the SGs Configuration Mode.

  For example, if 12,000 subscribers are to be detached during a 5 minute window (duration = 5 minutes), the MME calculates 60 cycles (5 minutes / 5-second cycles) which results in 200 UEs to detach per cycle.

  If the detach-rate is configured to 100, the MME will only detach 100 per 5 second cycle, resulting in a total of 6000 detaches. Any remaining UEs will remain attached until detached by other means (UE/network detach, etc).

The enabling command remains active until it is disabled with the following command:

no sgs vlr-failure sgs-service *sgs_svc_name* **[-noconfirm]**
Refer to the **sgs vlr-failure** command in the *Exec Mode (D-S)* chapter of the *Command Line Interface Reference* for more information.

Verifying UE Detach on VLR Failure/Recovery Status and Configuration

Use the following command to display the offload status of all VLRs on the system.

show sgs-service vlr-status full
This sample output shows the fields relating to UE Detach on VLR Failure and UE Detach on VLR Recover. Not all fields shown below may be displayed, based on your configuration:

```
[local]asr5x00# show sgs-service vlr-status full
Exec Configured VLR Failure Detach : No         Detached Count : 0        Total : 0
SGs Service Configured
   VLR Failure Detach : Yes       Detached Count : 10     Total : 800
  VLR Recover Detach : Yes       Detached Count : 11     Total : 102
```

To clear the counters displayed by the previous command, issue either of the following commands. The first command clears statistics for all VLRs for the specified SG, while the second command clears statistics for the specified VLR only.

clear sgs-service vlr-status service-name *sgs_svc_name*
clear sgs-service vlr-status vlr-name *vlr_name*

Monitoring and Troubleshooting VLR Offload

SNMP Traps

The following traps are generated to track conditions relating to VLR associations:

The VLR down trap is raised only after the VLR goes to the DOWN state after being UP. When all VLR's are down after at least one has been UP, the all VLR's DOWN trap is raised.

- **starVLRAssocDown** and **starVLRAssocUp** - indicates a condition when an association of a VLR is down (VLRAssocDown), and when a down association comes back up (VLRAssocUp).

- **starVLRDown** and **starVLRUp** - indicates a condition where **all** SCTP associations to a specific VLR are down (VLRDown), and when a down VLR comes back up (VLRUp).
- **starVLRAllAssocDown** and **starVLRAllAssocDownClear** - indicates a condition when **all** SCTP associations of **all** VLRs are down (VLRAllAssocDown), and when a down association comes back up (VLRAllAssocDownClear).

Bulk Statistics

This SGs schema provides operational statistics that can be used for monitoring and troubleshooting the SGs connections on a per-VLR basis.

Refer to the *SGs Schema Statistics* chapter of the *Statistics and Counters Reference* for detailed explanations of all bulk statistics provided in this schema.

Show Command(s) and/or Outputs

This section provides information regarding show commands and/or their outputs.

VLR Offload Status

The following command shows the status of the VLR offload process for the specified SGs service.

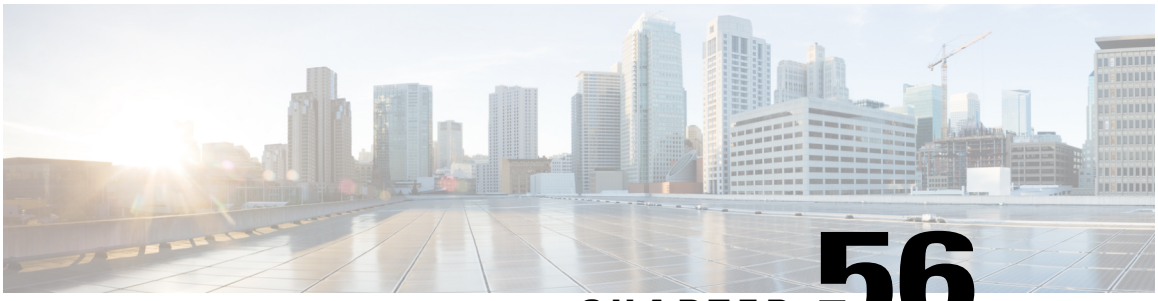
show sgs-service offload-status service-name *sgs_svc_name*
The following command shows the status and configuration information of all VLRs on the system.

show sgs-service vlr-status full

UE Detach on VLR Recovery and VLR Failure

The following command shows the statistics resulting from the **sgs vlr-recover** and **sgs vlr-failure** commands.

show sgs-service vlr-status full
Refer to the *show sgs-service* chapter of the *Statistics and Counters Reference* for detailed explanations of all information displayed by this command.



CHAPTER 56

Troubleshooting the MME Service

This chapter provides information and instructions for using the system command line interface (CLI) for troubleshooting issues that may arise during service operation.

Test Commands

In the event that an issue was discovered with an installed application or line card, depending on the severity, it may be necessary to take corrective action.

The system provides several redundancy and fail-over mechanisms to address issues with application and line cards in order to minimize system downtime and data loss. These mechanisms are described in the sections that follow.

Using the eGTPC Test Echo Command

This command tests the eGTP service's ability to exchange eGTPC packets with the specified peer which can be useful for troubleshooting and/or monitoring.

The test is performed by the system sending eGTP-C echo request messages to the specified peer(s) and waiting for a response.

Important This command must be executed from within the context in which at least one eGTP service is configured.

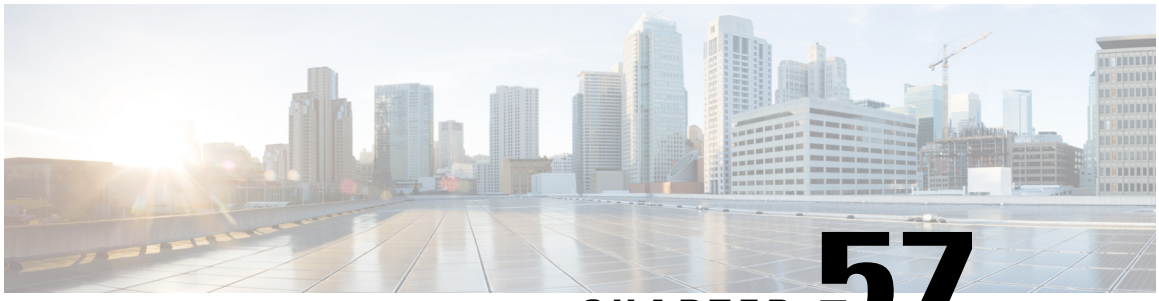
The command has the following syntax:
egtpc test echo peer-address *peer_ip_address* **src-address** *egtp_svc_ip_address*

Keyword/Variable	Description
peer-address *peer_ip_address*	Specifies that eGTP-C echo requests will be sent to a specific peer (HSS).*ip_address* is the address of the HSS receiving the requests.

Keyword/Variable	Description
src-address *egtp_svc_ip_address*	Specifies the IP address of a S6a interface configured on the system in eGTP service. **NOTE**: The IP address of the system's S6a interface must be bound to a configured eGTP service prior to executing this command.

The following example displays a sample of this command's output showing a successful eGTPC echo-test from an eGTP service bound to address 192.168.157.32 to an HSS with an address of 192.168.157.2.

```
EGTPC test echo
--------------
Peer: 172.10.10.2     Tx/Rx:  1/1  RTT(ms): 2    (COMPLETE) Recovery: 10 (0x0A)
```



CHAPTER 57

Monitor the MME Service

Overview

This chapter provides information for monitoring service status and performance using the **show** commands found in the Command Line Interface (CLI). These command have many related keywords that allow them to provide useful information on all aspects of the system ranging from current software configuration through call activity and status.

The selection of keywords described in this chapter is intended to provided the most useful and in-depth information for monitoring the system. For additional information on these and other **show** command keywords, refer to the Command Line Interface Reference.

In addition to the CLI, the system supports the sending of Simple Network Management Protocol (SNMP) traps that indicate status and alarm conditions. Refer to the SNMP MIB Reference Guide for a detailed listing of these traps.

Monitoring System Status and Performance

This section contains commands used to monitor the status of tasks, managers, applications and other software components in the system. Output descriptions for most of the commands are located in the Counters and Statistics Reference.

Table 20: System Status and Performance Monitoring Commands

To do this:	Enter this command:
View Session Statistics and Information	
Display Session Resource Status	
View session resource status	**show resources session**

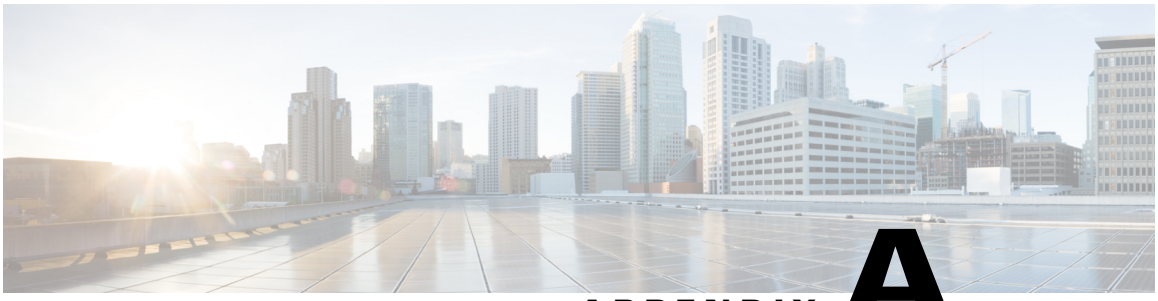
To do this:	Enter this command:
Display Historical Session Counter Information	
View all historical information for all sample intervals	**show session counters historical**
Display Session Duration Statistics	
View session duration statistics	**show session duration**
Display Session State Statistics	
View session state statistics	**show session progress**
Display Session Subsystem and Task Statistics Refer to the System Software Tasks appendix of the *System Administration Guide* for additional information on the Session subsystem and its various manager tasks.	
View AAA Manager statistics	**show session subsystem facility aaamgr all**
View MME Manager statistics	**show session subsystem facility mmemgr all**
View Session Manager statistics	**show session subsystem facility sessmgr all**
View MME Application statistics	**show logs facility mme-app**
View MME HSS Service facility statistics	**show logs facility mme-hss**
View MME miscellaneous logging facility statistics	**show logs facility mme-misc**
View MME Demux Manager logging facility statistics	**show logs facility mmedemux**
Display Session Disconnect Reasons	
View session disconnect reasons with verbose output	**show session disconnect-reasons**
View MME Service Statistics	
Display MME Service Session Statistics	
View MME service session state	**show mme-service session full**
View MME service session statistics	**show mme-service counters**
View MME database statistics for all instances of DB	**show mme-service db statistics**
View individual MME service statistics in concise mode	**show mme-service statistics mme-service** *mme_svc_name*
View HSS Statistics	
View HSS session summary	**show hss-peer-service session summary all**
View HSS session statistics	**show hss-peer-service statistics all**
View eGTPC Statistics	
View eGTPC peer information	**show egtpc peers interface sgw-egress address** *ip_address*

To do this:	Enter this command:
View eGTPC session information	**show egtpc sessions**
View eGTPC session statistics	**show egtpc statistics**
View Subscriber Session Trace Statistics	
View session trace statistics for subscriber with specific trace reference id on an MME	**show session trace subscriber reference-id** *trace_ref_id* **network-element mme**
View Trace Collection Entity connections and statistics for all network elements	**show session trace tce-summary**

Clearing Statistics and Counters

It may be necessary to periodically clear statistics and counters in order to gather new information. The system provides the ability to clear statistics and counters based on their grouping (MME, MME-HSS, MME DB, etc.).

Statistics and counters can be cleared using the CLI **clear** command. Refer to the *Command Line Reference* for detailed information on using this command.



APPENDIX A

Engineering Rules

This section provides engineering rules or guidelines that must be considered prior to configuring the system for your network deployment.

Service Engineering Rules

The engineering rules listed here apply to the services configurations for the MME system.

- A maximum combined total of 256 services (regardless of type) can be configured per system.

Important Maintaining a large number of services increases the complexity of management and may impact overall system performance (i.e., resulting from such things as system handoffs). Therefore, we recommend that you limit the number of services that you configure and that you talk to your Cisco Service Representative for optimization suggestions and additional information on service limits.

- The total number of entries per table and per chassis is limited to 256.
- Of the 256 possible services, the MME supports a maximum total combination of eight (8) MME-specific services, of the types MME + eMBMS + SGs+ SBc + SLs -service, be configured per chassis.
- The maximum number of HSS Peer Services that can be created and configured is 64 HSS Peer Services per MME chassis.

Important In some cases, two diameter endpoints (S6a and S13) can be configured for a single HSS Peer Service. To ensure peak system performance, we recommend that the total of all Diameter endpoints should be taken into consideration and limited to 64 endpoints.

- *We strongly recommend that service names be unique across the chassis/system configuration.* Even though service names can be identical to those configured in different contexts on the same system, this is not a good practice. Having services with the same name can lead to confusion, difficulty troubleshooting problems, and make it difficult to understand the outputs of show commands.

Node Engineering Rules

The following engineering rules apply regarding the number of nodes supported on the system.

eNodeBs:

- In Release 18 .0 and higher, the MME supports a maximum of 32,000 eNodeB connections on the ASR5000 platform and a maximum of 64,000 eNodeB connections on the ASR5500 DPC platform, with a fully loaded system (chassis).
- In Release 19.2, the MME supports a maximum of 64,000 eNodeB connections on the ASR5500 DPC2 platform with a fully loaded system (chassis).
- In Release 20.0, the MME supports a maximum of 128, 000 eNodeB connections on the ASR5500 DPC2 platform with a fully loaded system (chassis).

Release 17.0 and higher:

- The MME supports a maximum of 64,000 eNodeB connections on the ASR 5500 platform with a fully loaded system (chassis).

Previous Releases:

- On the ASR 5000, the MME supports a maximum of 32,000 eNodeB connections.
- On the ASR 5000, the MME supports a maximum of 8 MME Managers.

MME Managers

- In Release 17.0, The maximum number of MME Managers has been increased to 16 in order to support the increase in eNodeB connections.
- In Release 18.0, the maximum number of MME Managers is 12 on the ASR5000 platform and increased to 24 on the ASR5500 DPC platform, in order to support the increase in eNodeB connections.
- In Release 19.2, the maximum number of MME Managers is increased to 36 on the ASR5500 DPC2 platform, in order to support the increase in eNodeB connections.

MME Task Instance Limit

This section describes the task instance limit for MME managers and IMSI managers.

Table 21: Task Instance Limit for MME Managers

Platform	Default number of MME Managers per Chassis			Maximum number of MME Managers per Chassis		
StarOS Release	**v19.2**	**v20.0**	**v21.0**	**v19.2**	**v20.0**	**v21.0**
ASR5000	12	12	12	12	12	12
ASR5500 with DPC	24	24	24	24	24	24
ASR5500 with DPC2	36	36	48	36	36	48
VPC-SI MEDIUM/LARGE	2	2	2	2	2	2
VPC-SI SMALL, VPC-SI FORGE	1	1	1	1	1	1
VPC-DI MEDIUM/LARGE	24	48	48	24	48	48
ASR5700	24	24	24	24	24	24

Table 22: Task Instance Limit for IMSI Managers

Platform	Default number of IMSI Managers per Chassis			Maximum number of IMSI Managers per Chassis		
Release	**v19.2**	**v20.0**	**v21.0**	**v19.2**	**v20.0**	**v21.0**
ASR5000 PSC/PSC2/PSC3	1	1	1	1	1	1
ASR5500 with DPC	4	4	4	4	4	4
ASR5500 with DPC2	4	4	8	4	4	8
VPC-SI MEDIUM/LARGE	1	1	1	1	1	1
VPC-SI SMALL, VPC-SI FORGE	1	1	1	1	1	1
VPC-DI MEDIUM/LARGE	4	4	4	4	4	4
ASR5700	4	4	4	4	4	4

APN Engineering Rules

The following engineering rules apply to APN configuration on the MME:

- APNs must be configured within the context used for authentication.
- A maximum of 1,024 APNs can be configured per system.
- A maximum of 300 entries can be defined for an APN Remap Table.