Cisco ASR 5000 Series Mobility Management Entity Administration Guide

Version 12.0

Last Updated September 30, 2011

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

Text Part Number: OL-24873-02

Cisco ASR 5000 Series Mobility Management Entity Administration Guide

CONTENTS

About this Guide

This document pertains to the features and functionality that run on and/or that are related to the Cisco® ASR 5000 Chassis, formerly the Starent Networks ST40.

Conventions Used

The following tables describe the conventions used throughout this documentation.

Icon	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.
	Electro-Static Discharge (ESD)	Alerts you to take proper grounding precautions before handling a product.

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**

Command Syntax Conventions	Description
{ **`keyword`** or *`variable`* }	Required keywords and variables are surrounded by grouped brackets. Required keywords and variables are those components that are required to be entered as part of the command syntax.

Command Syntax Conventions	Description
[**keyword** or *variable*]	Optional keywords or variables, or those that a user may or may not choose to use, are surrounded by square brackets.
|	With some commands there may be a group of variables from which the user chooses one. These are called alternative variables and are documented by separating each variable with a vertical bar (also known as a pipe filter). Pipe filters can be used in conjunction with required or optional keywords or variables. For example: **{ nonce | timestamp }** OR [**count** *number_of_packets* | **size** *number_of_bytes*]

Contacting Customer Support

Use the information in this section to contact customer support.

For New Customers: 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 is required to this site. Please contact your local sales or service representative for additional information.

For Existing Customers with support contracts through Starent Networks: Refer to the support area of https://support.starentnetworks.com/ for up-to-date product documentation or to submit a service request. A valid username and password is required to this site. Please contact your local sales or service representative for additional information.

Important: For warranty and repair information, please be sure to include the Return Material Authorization (RMA) tracking number on the outside of the package.

Chapter 1
Mobility Management Entity Overview

The Cisco ASR 5000 chassis provides Long Term Evolution (LTE)/System Architecture Evolution (SAE) wireless carriers with a flexible solution that functions as a Mobility Management Entity (MME) in 3rd Generation Partnership Project (3GPP) LTE/SAE wireless data networks.

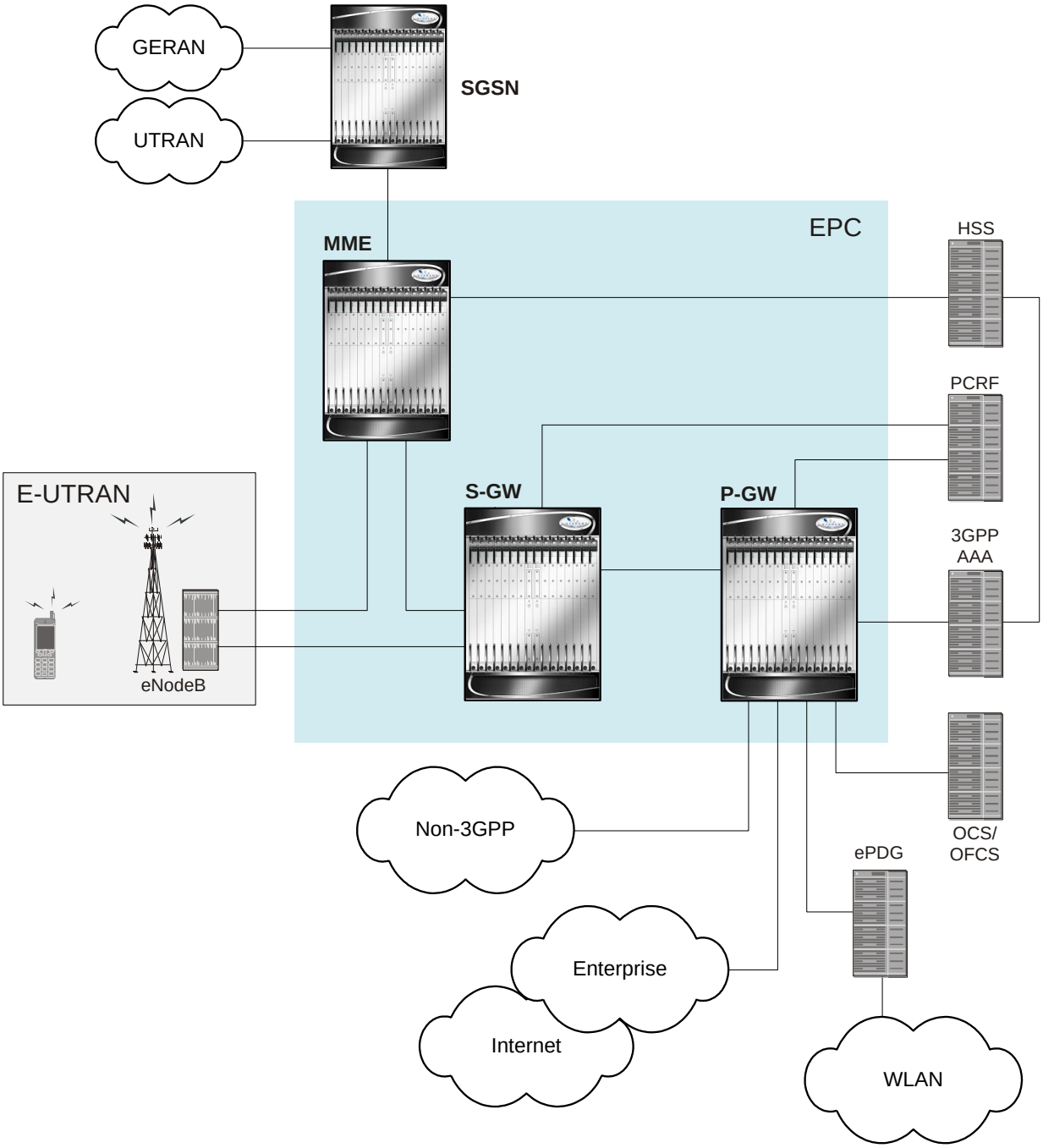
This overview provides general information about the MME including:

- SAE Network Summary
- Product Description
- Product Specification
- Network Deployment and Interfaces
- Features and Functionality - Base Software
- Features and Functionality - External Application Support
- Features and Functionality - Licensed Enhanced Feature Software
- How the MME Works
- Supported Standards

SAE Network Summary

The System Architecture Evolution was developed to provide a migration path for 3GPP systems and introduce higher data rates and lower latency for a variety of radio access technologies. SAE defines the packet network supporting the high-bandwidth radio network as the Evolved Packet Core (EPC). The EPC provides mobility between 3GPP (Global Systems for Mobile Communications (GSM), Universal Mobile Telecommunications System (UMTS), and LTE) and non-3GPP radio access technologies, including code division multiple access (CDMA), Worldwide Interoperability for Microwave Access (WiMAX), WiFi, High Rate Packet Data (HRPD), evolved HRPD, and European Telecommunications Standards Institute (ETSI)-defined Telecoms & Internet converged Services & Protocols for Advanced Networks (TISPAN) networks.

The following figure shows the interworking of the EPC with the different radio access technologies.



E-UTRAN / EPC Network Components

The Enhanced UTRAN (E-UTRAN) / EPC network is comprised of the following components:

eNodeB

The evolved NodeB (eNodeB), the E-UTRAN base station, is one of two nodes in the SAE Architecture user plane (the other is the Serving Gateway (S-GW)). The eNodeB communicates with other eNodeBs via the X2 interface. The eNodeB communicates with the EPC via the S1 interface. The user plane interface is the S1-U connection to S-GW. The signaling plane interface is the S1-MME connection to MME.

Basic functions supported include:

- Radio resource management, radio bearer control, and scheduling
- IP header compression and encryption of user data streams
- Selection of MME at UE attachment (if not determined by information sent from the UE)
- Scheduling and transmission of paging messages (originated from the MME)
- Scheduling and transmission of broadcast information (originated from the MME or OA&M)
- Measurement & measurement reporting configuration for mobility and scheduling

Mobility Management Entity (MME)

The MME is the key control-node for the LTE access-network. The MME provides the following basic functions:

- Network Access Signaling (NAS)
    - signalling
    - signalling security
- User Equipment (UE) access in ECM-IDLE state (including control and execution of paging retransmission)
- Tracking Area (TA) list management
- PDN Gateway (P-GW) and S-GW selection
- MME selection for handovers with MME change
- SGSN selection for handovers to 2G or 3G 3GPP access networks
- Terminates the interface from the Home Subscriber Service(HSS) over S6a
- Authentication
- Bearer management functions including dedicated bearer establishment
- Transparent transfer of HRPD signalling messages and transfer of status information between E-UTRAN and HRPD access, as specified in the pre-registration and handover flows

Serving Gateway (S-GW)

For each UE associated with the EPS, there is a single S-GW at any given time providing the following basic functions:

- Terminates the interface towards E-UTRAN (S1-U)

- Functions (for both the GPRS Tunneling Protocol (GTP)-based and the Proxy Mobile IP (PMIP)-based S5/S8) include:
    - local mobility anchor point for inter-eNodeB handover
    - mobility anchoring for inter-3GPP mobility (terminating S4 and relaying the traffic between 2G/3G system and P-GW)
    - EPS Connection Management (ECM)-IDLE mode downlink packet buffering and initiation of network triggered service request procedure
    - lawful intercept
    - packet routing and forwarding
    - transport level packet marking in the uplink and the downlink (e.g. setting the DiffServ Code Point)
    - Accounting
- Handling of Router Solicitation and Router Advertisement messages if PMIP based S5 and S8 are used
- Mobile Access Gateway (MAG) for PMIP based S5 and S8

PDN Gateway (P-GW)

For each UE associated with the Evolved Packet System (EPS), there is at least one P-GW providing access to the requested PDN. If a UE is accessing multiple PDNs, there may be more than one P-GW for that UE. The P-GW provides the following basic functions:

- Terminates the interface towards the PDN (SGi)
- P-GW functions (for both the GTP-based and the PMIP-based S5/S8) include:
    - per-user packet filtering (e.g. deep packet inspection)
    - lawful intercept
    - UE IP address allocation
    - Uplink (UL) and downlink (DL) service level charging, gating control, and service level rate enforcement
    - DL rate enforcement based on Aggregate Max Bit Rate (AMBR) and based on the accumulated MBRs of the aggregate of Service Data Flows (SDFs) with the same Guaranteed Bit Rate (GBR) QoS Class Index (QCI)
- Local Mobility Anchor (LMA) for PMIPv6

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:

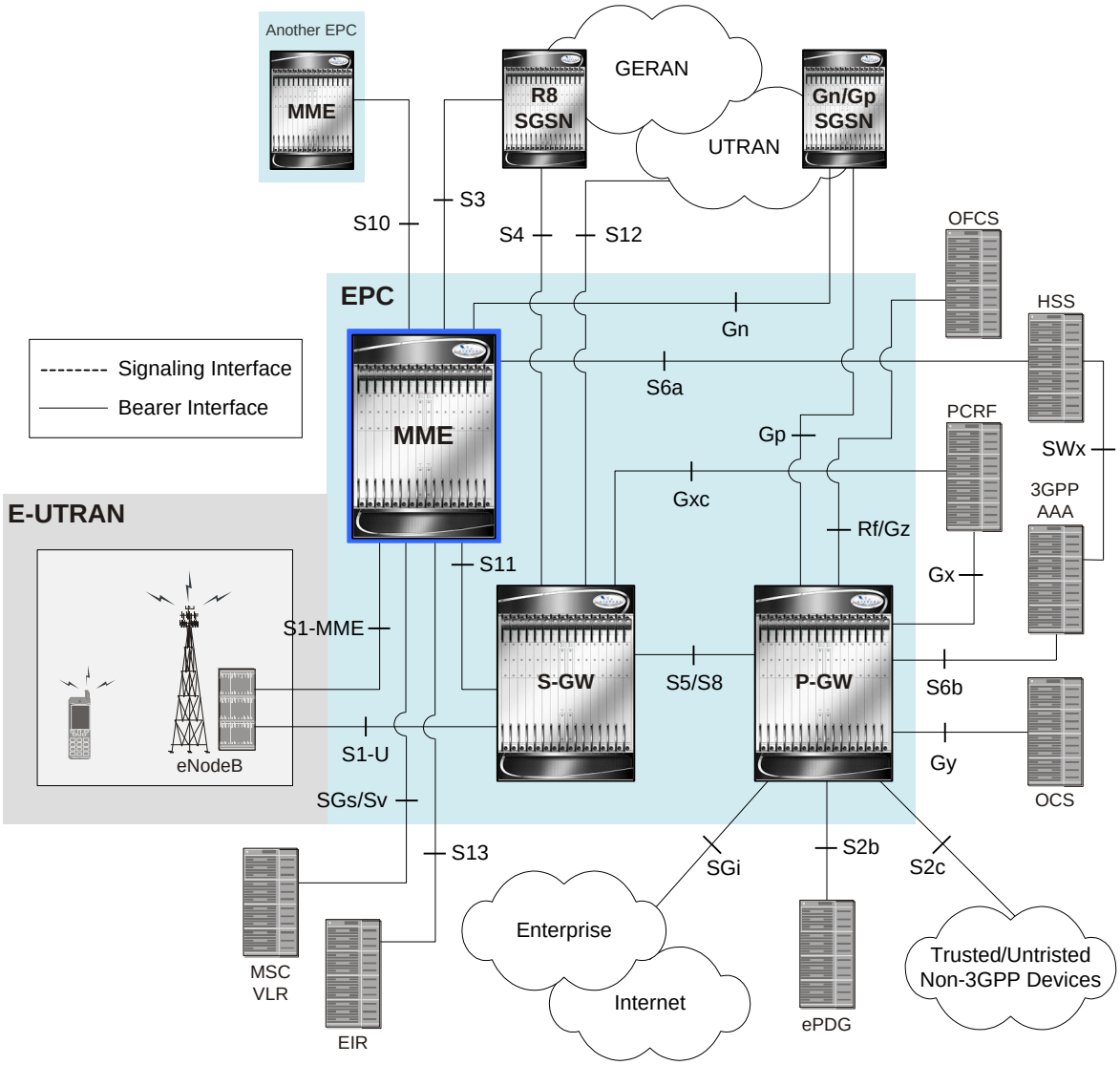
- Involved in the bearer activation/deactivation process and is also responsible for choosing the S-GW and for a UE at the initial attach and at the time of intra-LTE handover involving Core Network (CN) node relocation.
- Provides P-GW selection for subscriber to connect to PDN.
- Provides idle mode 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 Gn/Gp 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 Strutum (NAS) signalling
- NAS signalling security
- Inter CN node signalling 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 signalling traffic
- Warning message transfer function (including selection of appropriate eNodeB)
- UE Reachability procedures
- Interfaces with MSC for Voice paging
- Interfaces with Gn/Gp SGSN for interconnecting to legacy network
- MAP based Gr interface to legacy HLR

Product Specification

This section describes the hardware and software requirement for MME service.

The following information is located in this section:

- Licenses
- Hardware Requirements
- Operating System Requirements

Licenses

The MME is a licensed product. A session use license key must be acquired and installed to use the MME service.

For more information on supported features, refer to the *Features and Functionality* sections.

Hardware Requirements

Information in this section describes the hardware required to enable the MME service.

Platforms

The MME service operates on the following platform(s):

- ASR 5000

System Hardware Components

The following application and line cards are required to support MME services on the system:

- **System Management Cards (SMC)**: Provides full system control and management of all cards within the ASR 5000 platform. Up to two SMC can be installed; one active, one redundant.
- **Packet Services Cards (PSC/PSC2/PSC3)**: Within the ASR 5000 platform, PSCs/PSC2s/PSC3s provide high-speed, multi-threaded EPS Bearer context processing capabilities for MME services. Up to 14 PSCs/PSC2s/PSC3s can be installed, allowing for multiple active and/or redundant cards.

- **Switch Processor Input/Outputs (SPIOs)**: Installed in the upper-rear chassis slots directly behind the SPCs/SMCs, SPIOs provide connectivity for local and remote management, central office (CO) alarms. Up to two SPIOs can be installed; one active, one redundant.
- **Line Cards**: The following rear-loaded line cards are currently supported by the system:
  - **Ethernet 10/100 (FELC) and/or Ethernet 1000 Line Cards (GELC)**: Installed directly behind PSCs, these cards provide the physical interfaces to elements in the LTE/SAE network. Up to 26 line cards should be installed for a fully loaded system with 13 active PSCs/PSC2/PSC3, 13 in the upper-rear slots and 13 in the lower-rear slots for redundancy. Redundant PSCs/PSC2s/PSC3s do not require line cards.
  - **Quad Gig-E Line Cards (QGLCs)**: The 4-port Gigabit Ethernet line card is used in the ASR 5000 system only and is commonly referred to as the Quad-GigE Line Card or the QGLC. The QGLC is installed directly behind its associated PSC/PSC2 to provide network connectivity to the packet data network.
  - **10 Gig-E Line Cards (XGLCs)**: The 10 Gigabit Ethernet Line Card is used in the ASR 5000 system only and is commonly referred to as the XGLC. The XGLC supports higher speed connections to packet core equipment, increases effective throughput between the ASR 5000 and the packet core network, and reduces the number of physical ports needed on the ASR 5000.

    The one-port XGLC supports the IEEE 802.3-2005 revision which defines full duplex operation of 10 Gigabit Ethernet.

    The XGLC is configured and monitored via the System Management Card (SMC) over the system's control bus. Both SMCs must be active to maintain maximum forwarding rates.
- **Redundancy Crossbar Cards (RCCs):** Installed in the lower-rear chassis slots directly behind the SPCs/SMCs, RCCs utilize 5 Gbps serial links to ensure connectivity between Ethernet 10/100/Ethernet 1000/Quad Gig-E/10 Gig-E line cards and every PSC/PSC2 in the system for redundancy. Two RCCs can be installed to provide redundancy for all line cards and PSCs/PSC2a.

Important: Additional information pertaining to each of the application and line cards required to support LTE/SAE services is located in the *Hardware Platform Overview* chapter of the *Product Overview Guide*.

Operating System Requirements

The MME is available for ASR 5000 platforms running StarOS™ Release 9.0 or later.

Network Deployment and Interfaces

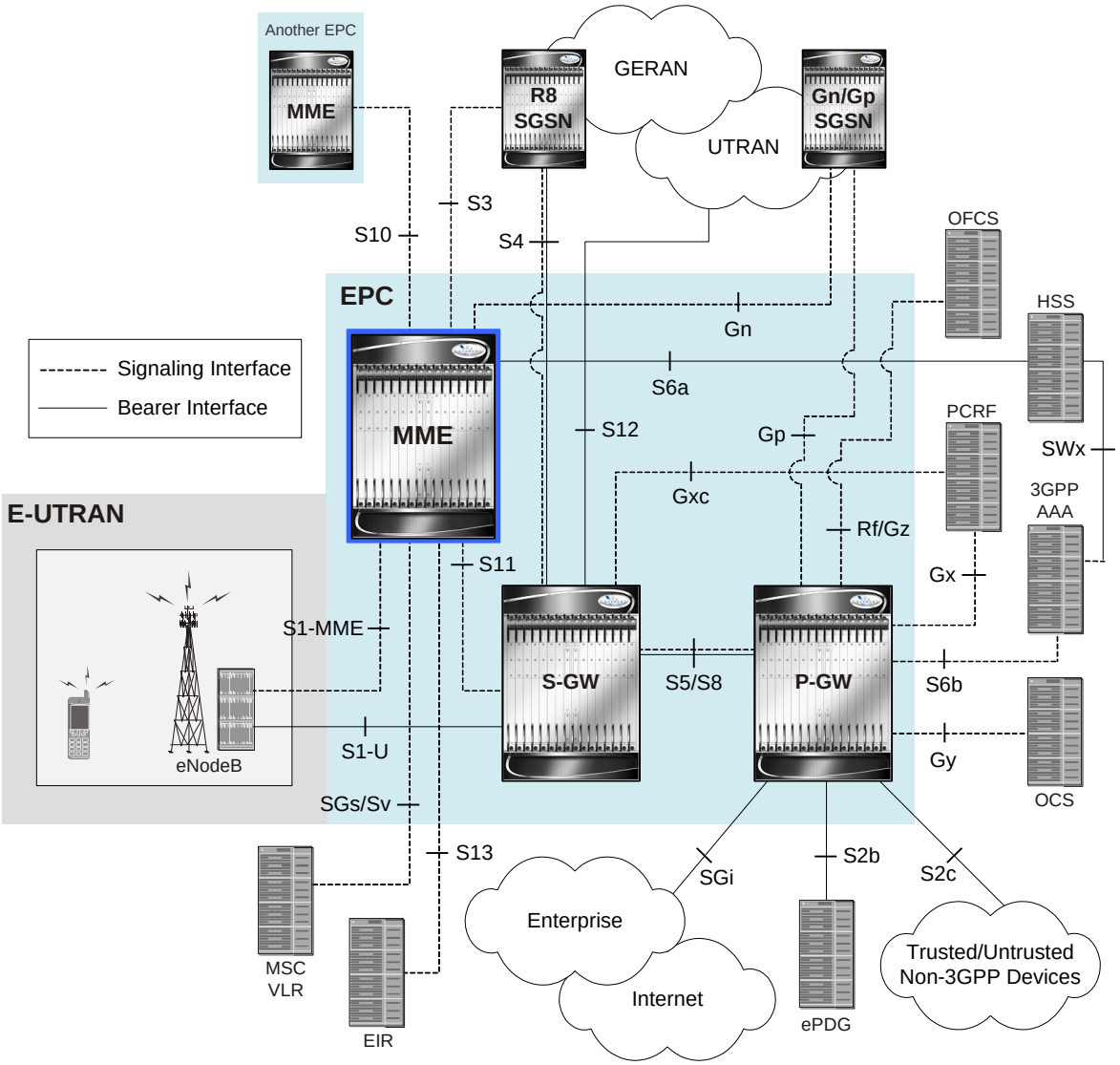
This section describes the supported interfaces and deployment scenario of MME in LTE/SAE network.

The following information is provided in this section:

MME in the LTE/SAE Network

The following figure displays a simplified network view of the MME and how it interconnects with other 3GPP Evolved-UTRAN/Evolved Packet Core network devices.

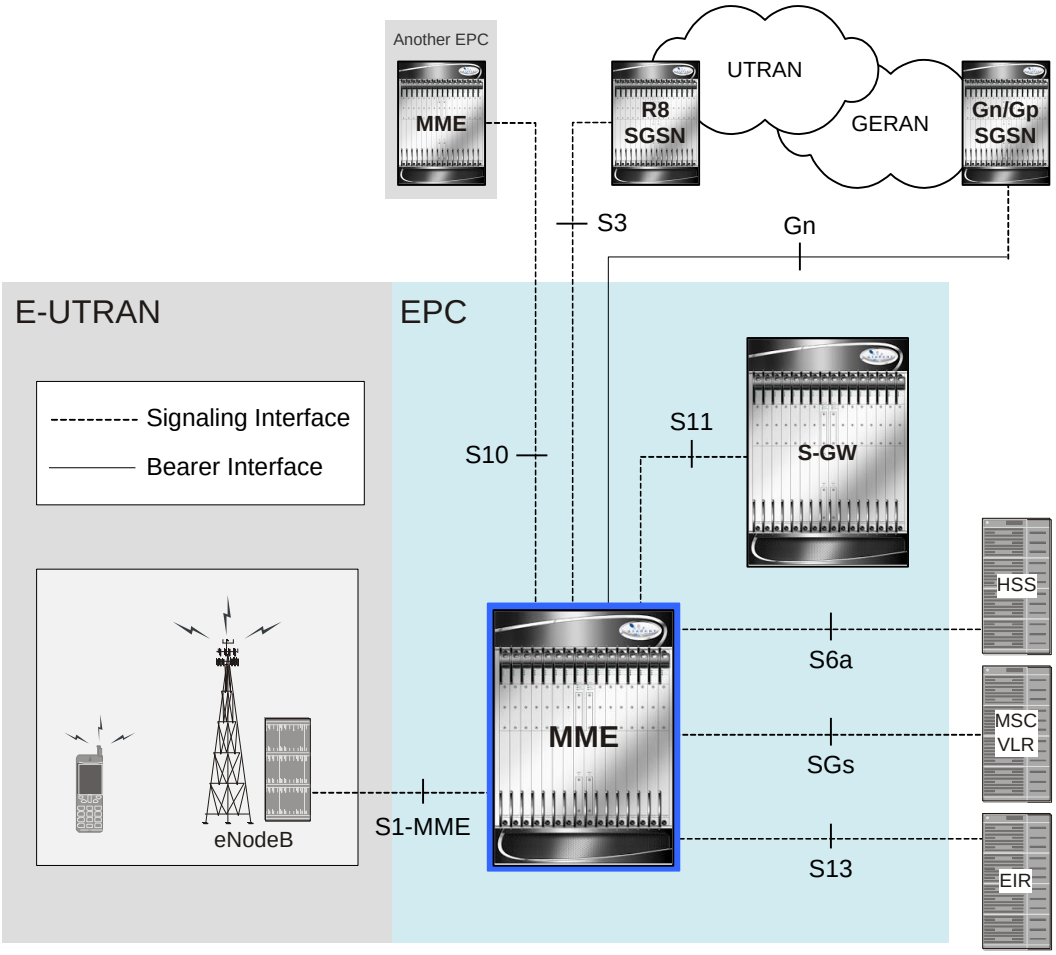
Figure 2. Interfaces in the E-UTRAN/EPC Network



Supported Interfaces

The following figure displays the specific network interfaces between a Mobility Management Entity and other network components.

Figure 3. Supported MME Interfaces in the E-UTRAN/EPC Network



The MME supports the following network interfaces/reference points:

- **S1-MME Interface**: This interface is the reference point for the control plane protocol between eNodeB and MME. S1-MME uses S1- Application Protocol (S1-AP) over 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.

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

- **S3 Interface**: This is the interface used by the MME to communicate with Release 8 SGSNs on the same Public PLMN for interworking between GPRS/UMTS and LTE network access technologies. This interface serves as the signalling path for establishing and maintaining subscriber UE contexts.

  The MME communicates with SGSNs on the PLMN using the GPRS Tunnelling Protocol (GTP). The signalling 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.

- **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.
- **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.

  One or more S10 interfaces can be configured per system context.
- **S11 Interface**: This interface provides communication between MME and Serving Gateways (S-GW) for information transfer using GTPv2 protocol.

  One or more S11 interfaces can be configured per system context.
- **S13 Interface**: This interface provides communication between MME and Equipment Identity Register (EIR).

  One or more S13 interfaces can be configured per system context.
- **SGs Interface**: The SGs interface connects the databases in the VLR and the MME to support circuit switch fallback scenarios.
- **DNS Interface**: MME supports the DNS interface for MME, S-GW, P-GW, and SGSN selection in the EPS core network. The MME uses the Tracking Area List as a fully qualified domain name (FQDN) to locate the address to establish the call with.

  One or more DNS interface can be configured per system context.
- **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 interoperation between EPS networks and 2G/3G 3GPP networks.

  Roaming and inter access mobility between Gn/Gp 2G and/or 3G SGSNs and an MME/S-GW are enabled by:
  - Gn functionality, as specified between two Gn/Gp SGSNs, which is provided by the MME, and
  - Gp functionality, as specified between Gn/Gp SGSN and Gn/Gp GGSN, that is provided by the P-GW.

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

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.

Important: To configure the basic service and functionality on the system for MME service, refer configuration examples provide in *MME Administration Guide*.

This section describes following features:

- 3GPP R8 Identity Support
- ANSI T1.276 Compliance
- APN Restriction Support
- Authentication and Key Agreement (AKA)
- Bulk Statistics Support
- Congestion Control
- EPS Bearer Context Support
- EPS GTPv2 Support on S11 Interface
- HSS Support Over S6a Interface
- Inter-MME Handover Support
- Interworking Support
- IPv6 Support
- Load Balancing
- Management System Overview
- MME Pooling
- MME Selection
- Mobile Equipment Identity Check
- Mobility Restriction
- Multiple PDN Support
- NAS Protocol Support
- NAS Signalling Security
- Operator Policy Support
- Overload Management in MME
- Packet Data Network Gateway (P-GW) Selection
- Radio Resource Management Functions
- Reachability Management
- SCTP Multi-homing Support

- Serving Gateway Pooling Support
- Serving Gateway Selection
- Subscriber Level Session Trace
- Threshold Crossing Alerts (TCA) Support
- Tracking Area List Management

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 ASR 5000 and the Web Element Manager 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 signalling data, and the confidentiality of the user data.

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 the Web 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:

- **System**: Provides system-level statistics
- **Card**: Provides card-level statistics
- **Port**: Provides port-level statistics
- **MME**: Provides MME service statistics
- **GTPC**: Provides GPRS Tunneling Protocol - Control message statistics

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 the Web 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 the Web 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 the Web Element Manager server.

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.

  - **Port Utilization Thresholds**: If you set a port utilization threshold, when the average utilization of all ports in the system reaches the specified threshold, congestion control is enabled.
    - **Port-specific Thresholds**: If you set port-specific thresholds, when any individual port-specific threshold is reached, congestion control is enabled system-wide.
  - **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 section in this chapter.

Important: For more information on congestion control, refer to the *Congestion Control* chapter in the *Cisco ASR 5000 Series System Administration Guide*.

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) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3 (Release 8)

The system supports the use of GTPv2 for EPS signalling 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.

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. The following interworking types are provided:

- Interworking with GnGp SGSNs
- Handover Support for Release 8 SGSNs

Interworking with Gn/Gp SGSNs

This feature enables an integrated EPC core network to anchor calls from multi-mode access terminals and support seamless mobility on call hand-offs between an LTE or GERAN/UTRAN access network. 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 Release 8 SGSNs

The S3 interface facilitates user mobility between an MME and a Release 8 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 (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 (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.

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
- SGs

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.

MME load balancing can be used in conjunction wit congestion control. For more information on congestion control, refere 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 MME should offload a cross-section of its subscribers with minimal impacts on the network and users (e.g. the MME should avoid offloading only the low activity users while retaining the high activity subscribers. Gradual rather than sudden off-loading should be performed as a sudden re-balance of large number of subscribers could overload other MMEs in the pool. With minimal impact on network and the user's experience, the subscribers should be off-loaded as soon as possible). The load re-balancing 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 entrant to the pool area into other MMEs).

Management System Overview

The system's management capabilities are designed around the Telecommunications Management Network (TMN) model for management - focusing on providing superior quality network element (NE) and element management system (Web Element Manager) functions. The system provides element management applications that can easily be integrated, using standards-based protocols (CORBA and SNMPv1, v2), into higher-level management systems - giving wireless operators the ability to integrate the system into their overall network, service, and business management systems. In addition, all management is performed out-of-band for security and to maintain system performance.

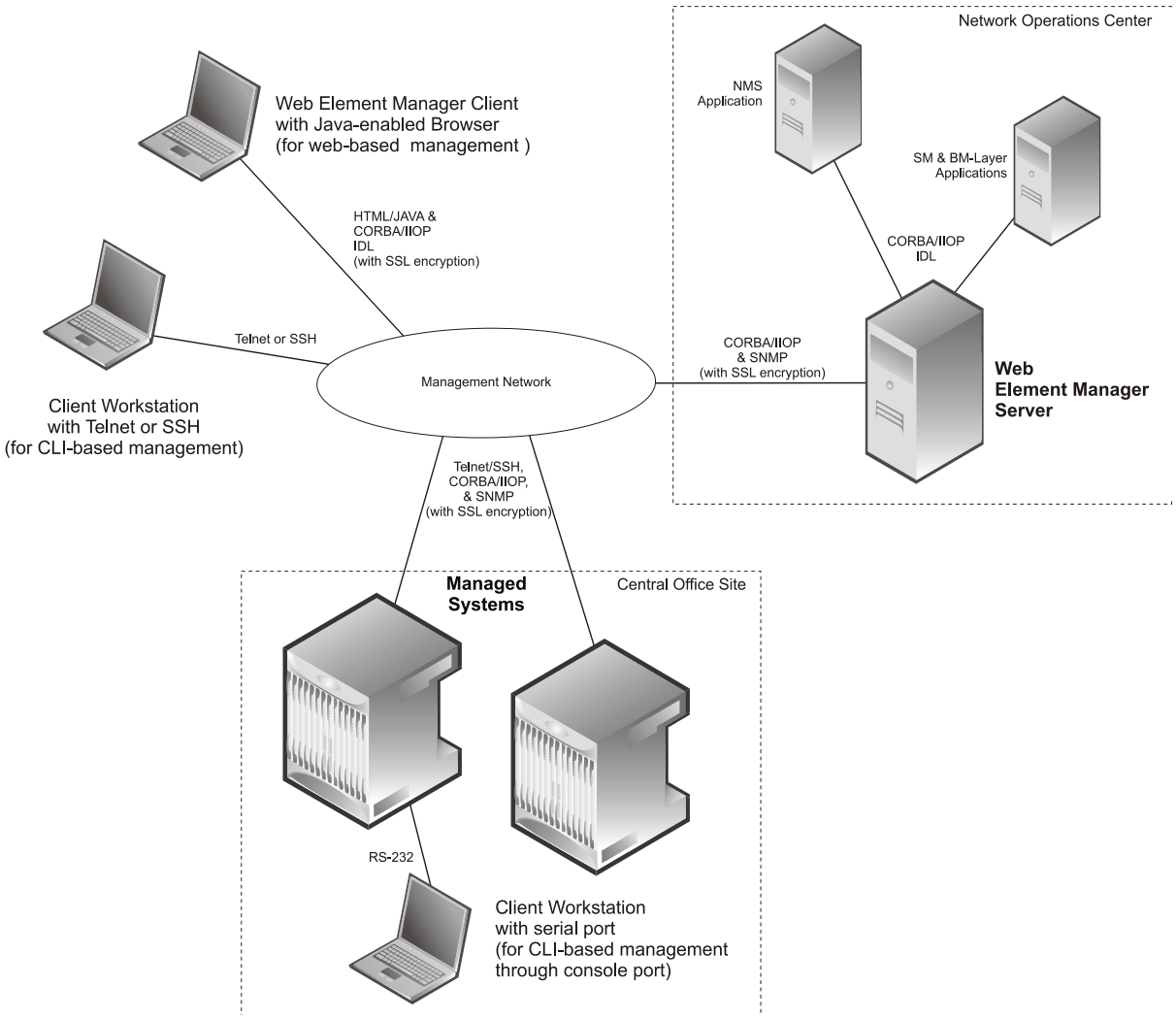
Operation and Maintenance module of ASR 5000 offers comprehensive management capabilities to the operators and enables them to operate the system more efficiently. There are multiple ways to manage the system either locally or remotely using its out-of-band management interfaces.

These include:

- Using the command line interface (CLI)
- Remote login using Telnet, and Secure Shell (SSH) access to CLI through SPIO card's Ethernet management interfaces
- Local login through the Console port on SPIO card using an RS-232 serial connection
- Using the Web Element Manager application
- Supports communications through 10 Base-T, 100 Base-TX, 1000 Base-TX, or 1000
- Base-SX (optical gigabit Ethernet) Ethernet management interfaces on the SPIO
- Client-Server model supports any browser (i.e. Microsoft Internet Explorer v5.0 and above or Netscape v4.7 or above, and others)
- Supports Common Object Request Broker Architecture (CORBA) protocol and Simple Network Management Protocol version 1 (SNMPv1) for fault management
- Provides complete Fault, Configuration, Accounting, Performance, and Security (FCAPS) capabilities
- Can be easily integrated with higher-level network, service, and business layer applications using the Object Management Group's (OMG’s) Interface Definition Language (IDL)

The following figure demonstrates these various element management options and how they can be utilized within the wireless carrier network.

Figure 4. Element Management Methods



Important: MME management functionality is enabled by default for console-based access. For GUI-based management support, refer *Web Element Management System*. For more information on command line interface based management, refer to the *Command Line Interface Reference*.

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

Handover Restriction Lists

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.

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.

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 signalling 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 Signalling Security

It provides integrity protection and encryption of NAS signalling. 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 signalling messages.

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

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

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.

Overload Management in MME

Provides mechanism to handle overload/congestion situation. It can use the NAS signalling to reject NAS requests from UEs on overload or congestion.

MME restricts the load that its eNodeBs are generating on it. This is achieved by the MME invoking the S1 interface overload procedure as per 3GPP TS 36.300 and 3GPP TS 36.413 to a proportion of the eNodeBs with which the MME has S1 interface connections.

Hardware and/or software failures within an MME may reduce the MME's load handling capability. Typically such failures result in alarms which alert the operator or Operation and Maintenance system.

For more information on congestion control management, refer to the *Configuring Congestion Control* chapter in the *System Administration Guide*.

Caution: Only if the operator or Operation and Maintenance system is sure that there is spare capacity in the rest of the pool, the operator or Operation and Maintenance system might use the load re-balancing procedure to move some load off an MME. However, extreme care is needed to ensure that this load re-balancing does not overload other MMEs within the pool area (or neighboring SGSNs) as this might lead to a much wider system failure.

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.

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.

SCTP Multi-homing for S6a

The Cisco MME service supports up to four SCTP bind end point IPv4 or IPv6 addresses for the S6a interface.

SCTP Multi-homing for S1-MME

The Cisco MME service supports up to two SCTP bind end point IPv4 or IPv6 addresses for the S1-MME interface.

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.

Subscriber Level Session Trace

The Subscriber Level Trace 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 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.

As a complement to Cisco's protocol monitoring function, the MME supports 3GPP standards based session level trace capabilities to monitor all call control events on the respective monitored interfaces including S6a, S1-MME and S11. 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

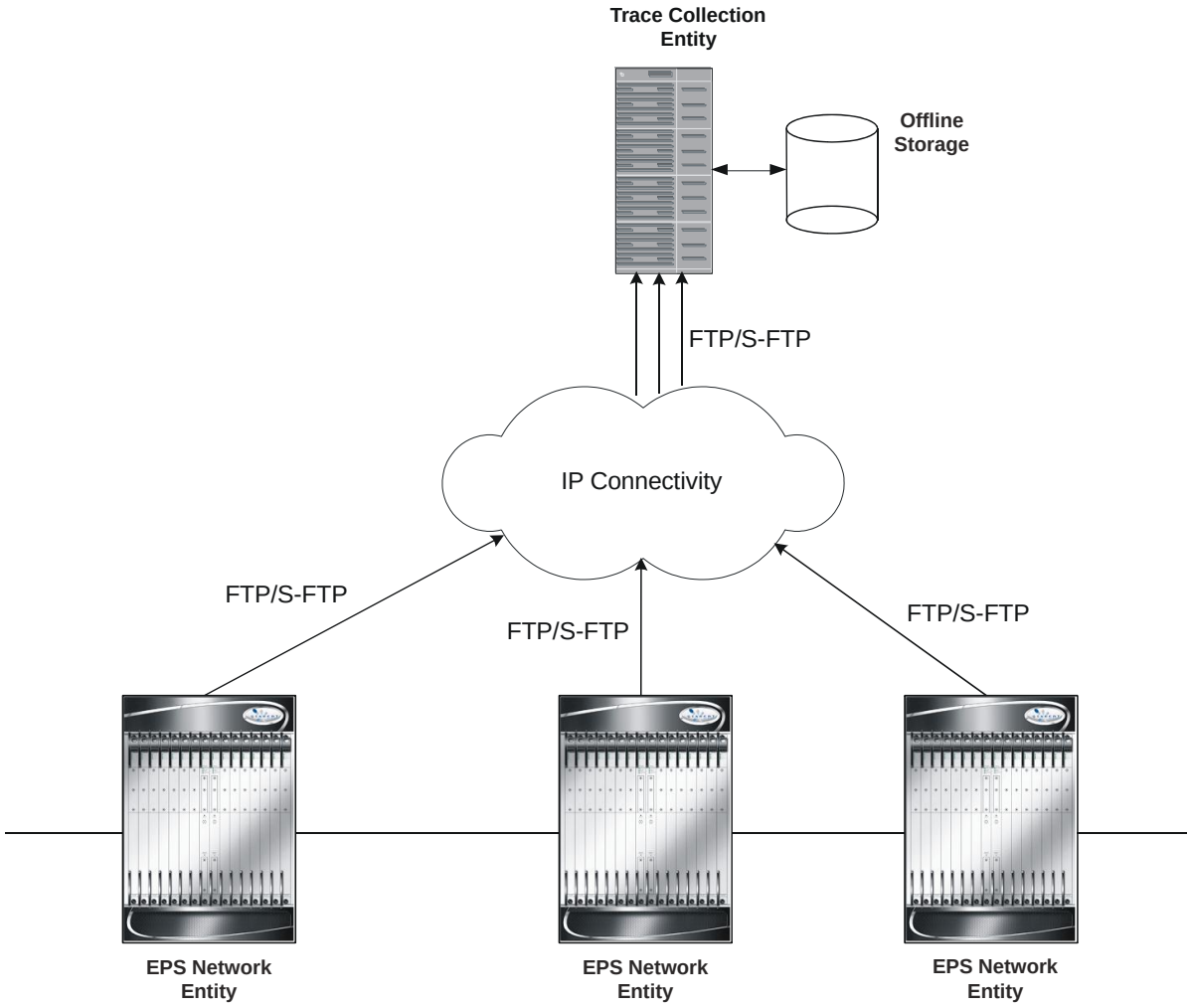
The session level trace function consists of trace activation followed by triggers. The EPC network element buffers the trace activation instructions for the provisioned subscriber in memory using camp-on monitoring. Trace files for active calls are buffered as XML files using non-volatile memory on the local dual redundant hard drives. 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.

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 and only *Maximum Trace Depth* is supported in this release.

The following figure shows a high-level overview of the session-trace functionality and deployment scenario:

Figure 5. Session Trace Function and Interfaces



For more information on this feature, refer to the *Configuring Subscriber Session Tracing* chapter in the *MME Service Administration Guide*.

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 menu in the Web 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.

To avoid a ping-pong effect, the MME includes the last visited TAI (provided that the tracking area is managed by the MME) in the TAI list assigned to the UE.

Tracking area lists assigned to different UEs moving in from the same tracking area should be different to avoid Tracking Area Update message overflow.

Features and Functionality - External Application Support

This section describes the features and functions of external applications supported on the S-GW. These services require additional licenses to implement the functionality.

This section describes following external applications:

- Web Element Management System

Web Element Management System

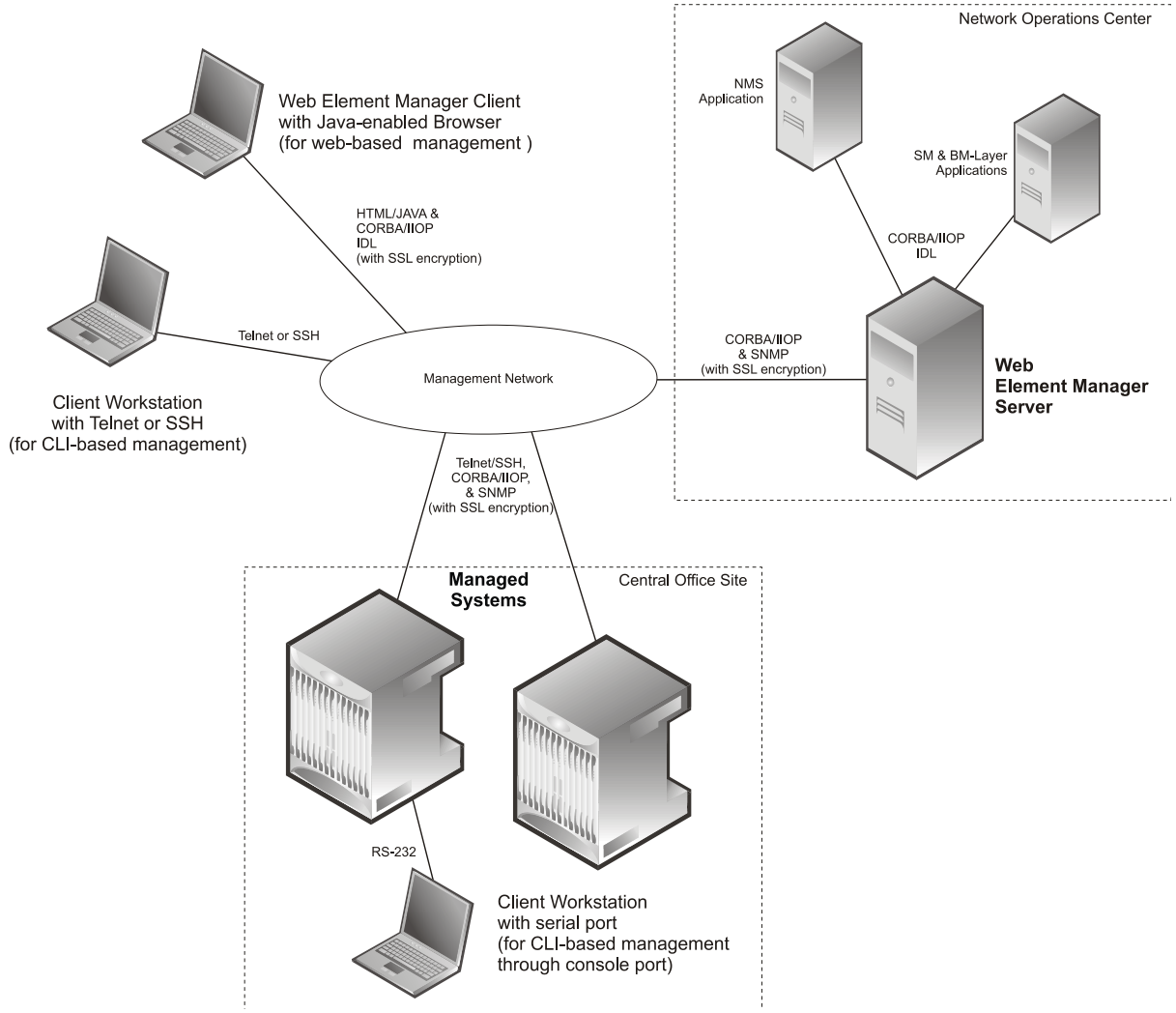
Provides a graphical user interface (GUI) for performing fault, configuration, accounting, performance, and security (FCAPS) management.

The Web Element Manager is a Common Object Request Broker Architecture (CORBA)-based application that provides complete fault, configuration, accounting, performance, and security (FCAPS) management capability for the system.

For maximum flexibility and scalability, the Web Element Manager application implements a client-server architecture. This architecture allows remote clients with Java-enabled web browsers to manage one or more systems via the server component which implements the CORBA interfaces. The server component is fully compatible with the fault-tolerant Sun® Solaris® operating system.

The following figure demonstrates these various element management options and how they can be utilized within the wireless carrier network.

Figure 6. Element Management Methods



Important: MME management functionality is enabled by default for console-based access. For GUI-based management support, refer *Web Element Management System*.

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.

This section describes following enhanced features:

- Circuit Switched Fall Back (CSFB) and SMS over SGs Interface
- IP Security (IPSec)
- Lawful Intercept
- Optimized Paging Support
- Session Recovery Support
- User Location Information Reporting

Circuit Switched Fall Back (CSFB) and SMS over SGs Interface

Circuit Switched Fall Back (CSFB) enables the UE to camp on an EUTRAN cell and originate or terminate voice calls through a forced switchover 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 EUTRAN network will be temporarily suspended (either the data transfer is suspended or the packet switched connection is handed over to the 2G/3G network).

Important: CSFB to CDMA 1x networks is not supported in this release.

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.

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 fall back to GSM/UMTS or CDMA1x access networks to receive incoming or place outgoing voice calls. Highlights of the CSFB procedure are as follows:

- **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 Call**:
  - 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.

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 amongst multiple MMEMGRs
- IMSI Paging Procedure
- SCTP Multi-homing
- IPv6 Transport for SGs
- SNMP Trap Support (Service/VLR association)
- Operator Policy Support
    - SMS-only
    - Disallow CSFB
- PS Suspend/Resume over S11 (Release 8)
- PS Suspend/Resume over S3/S11 (Release 9)

IP Security (IPSec)

IP Security provides a mechanism for establishing secure tunnels from mobile subscribers to pre-defined endpoints (i.e. enterprise or home networks) in accordance with the following standards:

- 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-3193, Securing L2TP using IPSEC, November 2001

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:

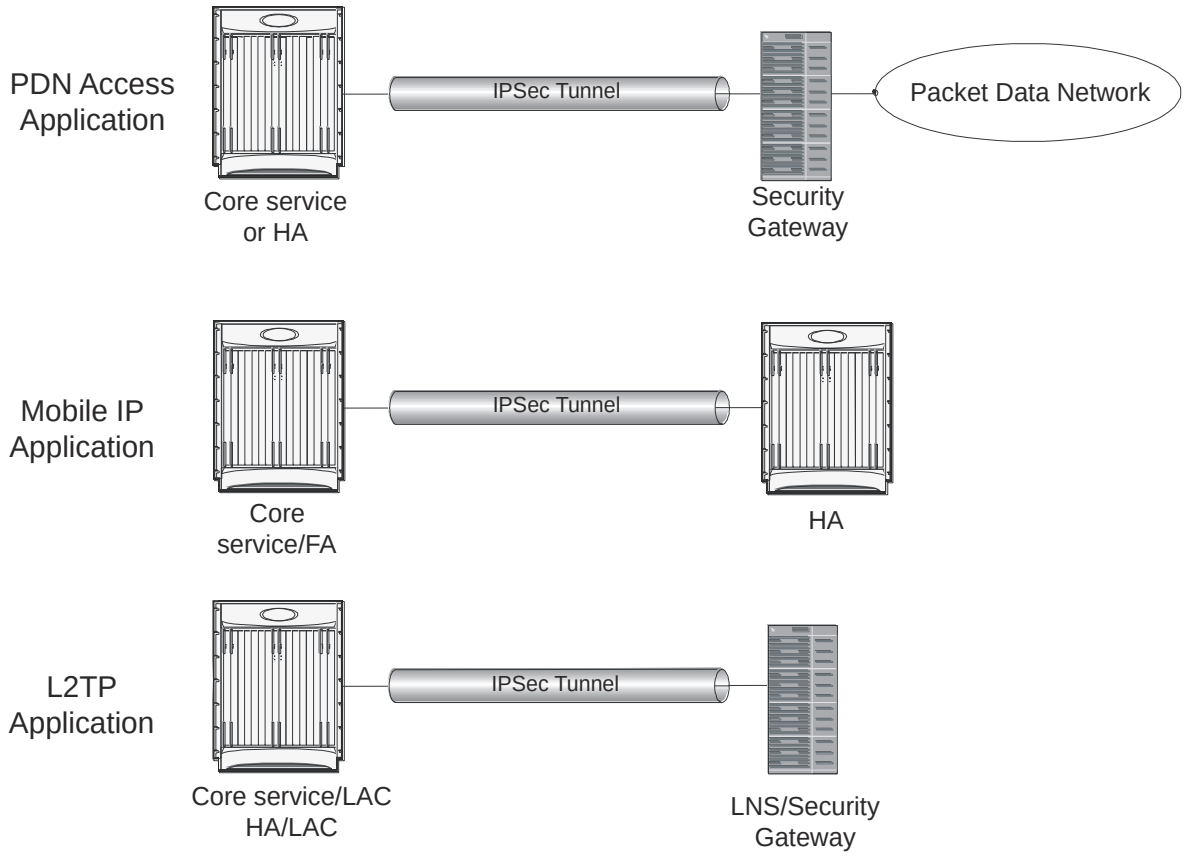
- **PDN Access**: Subscriber IP traffic is routed over an IPSec tunnel from the system to a secure gateway on the packet data network (PDN) as determined by access control list (ACL) criteria.
- **Mobile IP**: Mobile IP control signals and subscriber data is encapsulated in IPSec tunnels that are established 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 7. IPSec Applications



Important: For more information on IPSec support, refer to the *IP Security* appendix in the *MME Administration Guide*.

Lawful Intercept

The Cisco Lawful Intercept feature is supported on the MME. Lawful Intercept is a licensed 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 local Cisco sales representative.

Optimized Paging Support

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 acknowledgement 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.

Session Recovery Support

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.

This feature is also useful for Software Patch Upgrade activities. If session recovery feature is enabled during the software patch upgrading, it helps to permit preservation of existing sessions on the active PSC during the upgrade process.

Session recovery is performed by mirroring key software processes (e.g. session manager and AAA manager) within the system. These mirrored processes remain in an idle state (in standby-mode), wherein they perform no processing, until they may be needed in the case of a software failure (e.g. a session manager task aborts). The system spawns new instances of “standby mode” session and AAA managers for each active control processor (CP) being used.

Additionally, other key system-level software tasks, such as VPN manager, are performed on a physically separate packet processing card to ensure that a double software fault (e.g. session manager and VPN manager fails at same time on same card) cannot occur. The packet processing card used to host the VPN manager process is in active mode and is reserved by the operating system for this sole use when session recovery is enabled.

The additional hardware resources required for session recovery include a standby system processor card (SPC) and a standby packet processing card.

There are two modes for Session Recovery.

- **Task recovery mode**: Wherein one or more session manager failures occur and are recovered without the need to use resources on a standby packet processing card. In this mode, recovery is performed by using the mirrored “standby-mode” session manager task(s) running on active packet processing cards. The “standby-mode” task is renamed, made active, and is then populated using information from other tasks such as AAA manager.
- **Full packet processing card recovery mode**: Used when a PSC or PSC2 hardware failure occurs, or when a packet processing card migration failure happens. In this mode, the standby packet processing card is made active and the “standby-mode” session manager and AAA manager tasks on the newly activated packet processing card perform session recovery.

Session/Call state information is saved in the peer AAA manager task because each AAA manager and session manager task is paired together. These pairs are started on physically different packet processing cards to ensure task recovery.

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

User Location Information Reporting

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

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 Sess req
    - 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.

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.

The following procedures are supported in this release:

- EPS Bearer Context Processing
- Purge Procedure
- Paging Procedure
- Subscriber Session Processing
- Subscriber-initiated Initial Attach Procedure
- Subscriber-initiated Detach Procedure
- Service Request Procedures
    - UE-initiated Service Request Procedure
    - Network-initiated Service Request Procedure

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 Session Processing

This section provides information on how LTE/SAE subscriber data sessions are processed by the system MME. The following procedures are provided:

- **User-initiated Transparent IP:** An IP EPS Bearer context request is received by the MME from the UE for a PDN. The subscriber is provided basic access to a PDN without the MME authenticating the subscriber. Either a static or dynamic IP address can be assigned to the MS in this scenario.
- **User-initiated Non-transparent IP:** An IP EPS Bearer context request is received by the MME from the UE for a PDN. The MME provides subscriber authentication services for the data session. Either a static or dynamic IP address can be assigned to the MS in this scenario.
- **Network-initiated:** An IP EPS Bearer context request is received by the MME from the PDN for a specific subscriber. If configured to support network-initiated sessions, the MME, will initiate the process of paging the MS and establishing a EPS Bearer context.

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 8. Subscriber-initiated Attach (initial) Call Flow

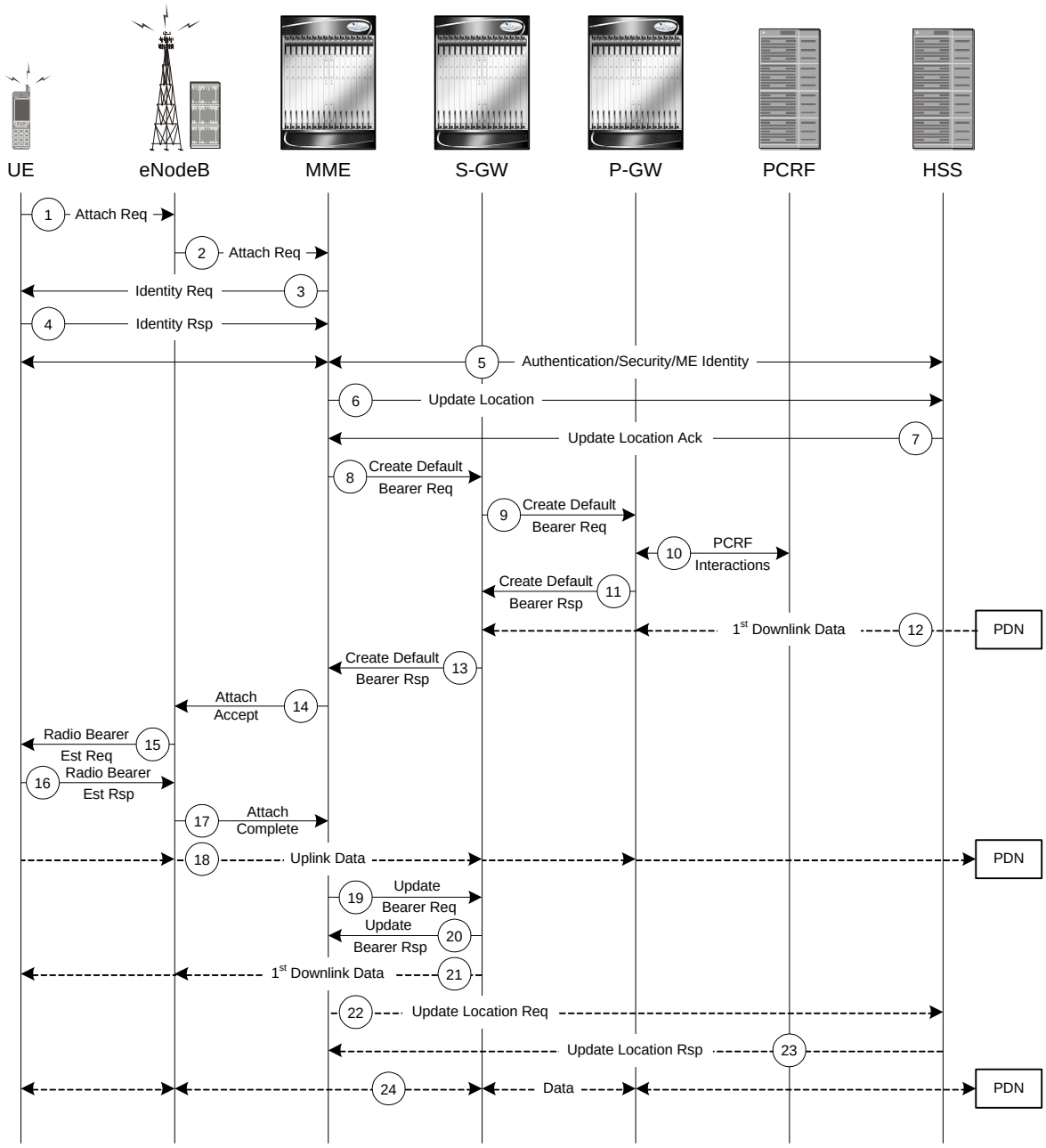


Table 1. Subscriber-initiated Attach (initial) Call Flow Description

Step	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.
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.

Step	Description
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 tunnelled 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.

Figure 9. Subscriber-initiated Detach Call Flow

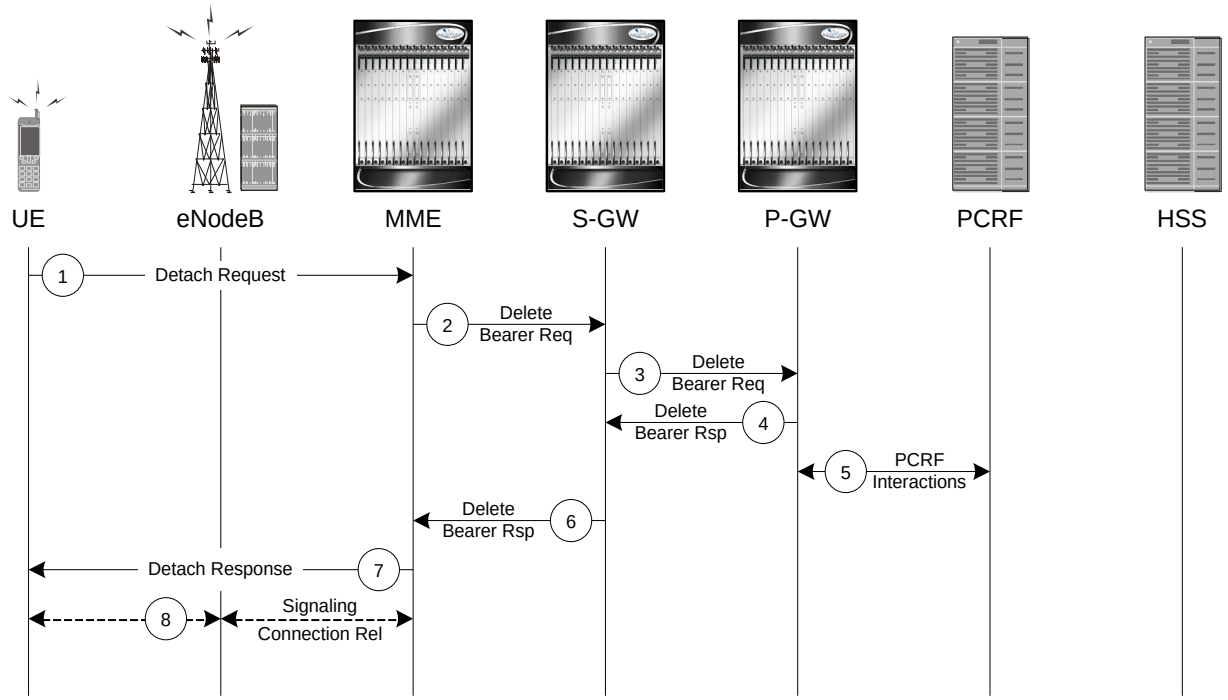


Table 2. Subscriber-initiated Detach Call Flow Description

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 signalling 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

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 10. UE-initiated Service Request Message Flow

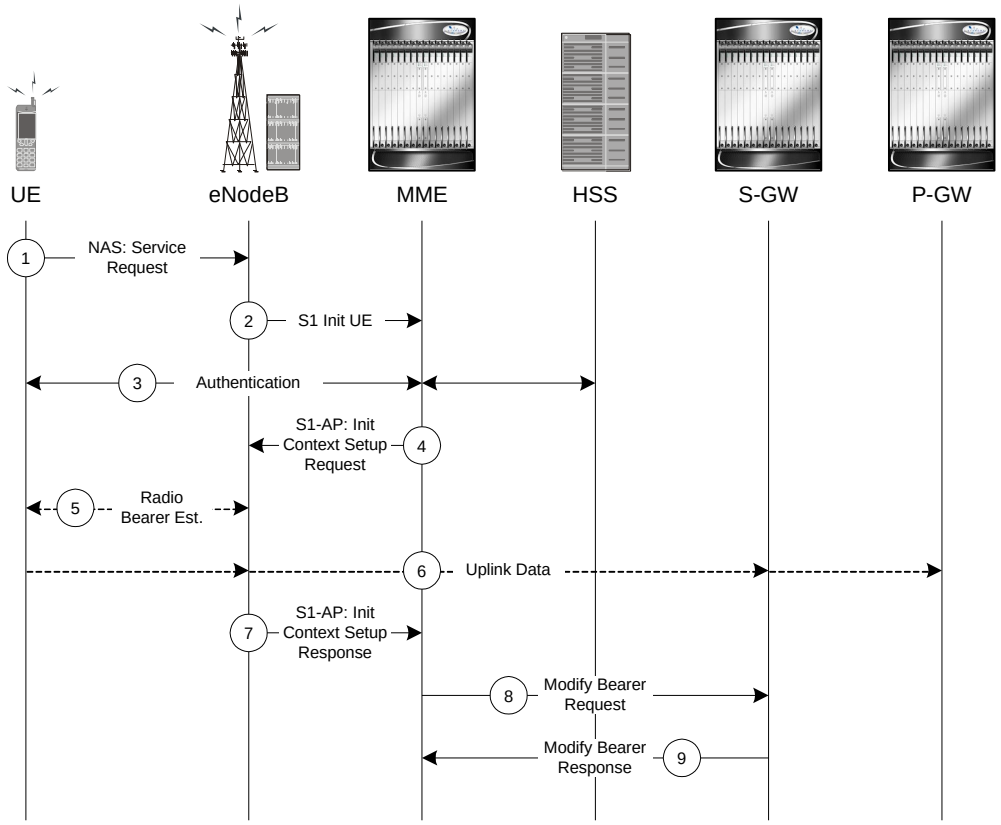


Table 3. UE-initiated Service Request Message Flow Description

Step	Description
1	(NAS) The UE sends a Network Access Signaling (NAS) message Service Request (S-TMSI) towards the MME encapsulated in an RRC message to the eNodeB.
2	The eNodeB forwards NAS message to the MME. The NAS message is encapsulated in an S1-AP: Initial UE message (NAS message, TAI+ECGI of the serving cell).
3	NAS authentication procedures may be performed.
4	The MME sends an S1-AP Initial Context Setup Request (S-GW address, S1-TEID(s) (UL), EPS Bearer QoS(s), Security Context, MME Signalling 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 Signalling 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 11. Network-initiated Service Request Message Flow

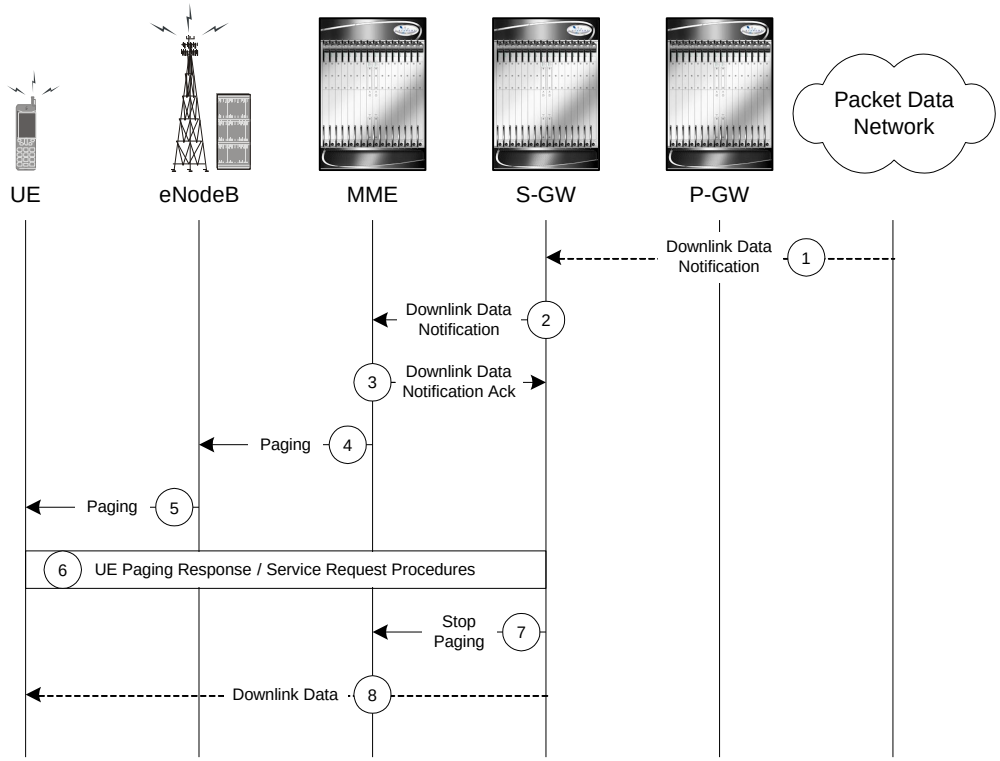


Table 4. Network-initiated Service Request Message Flow Description

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 Acknowledgement 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. **Important:** Steps 4 and 5 are skipped if the MME has a signalling 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
- IETF References
- Object Management Group (OMG) Standards

3GPP References

Release 8 Supported Standards

- 3GPP TS 23.122 V8.4.0 (2008-12): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Non-Access-Stratum (NAS) functions related to Mobile Station (MS) in idle mode (Release 8)
- 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 24.301 V8.4.0 (2009-12): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3 (Release 8)
- 3GPP TR 24.801 V8.0.1 (2008-10): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; 3GPP System Architecture Evolution; CT WG1 Aspects (Release 8)
- 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) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3 (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)
- 3GPP TS 36.401 V8.4.0 (2008-12): 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Architecture description (Release 8)
- 3GPP TS 36.410 V8.1.0 (2008-12): 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Access Network (E-UTRAN); S1 General aspects and principles (Release 8)
- 3GPP TS 36.411 V8.1.0 (2008-12): 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Access Network (E-UTRAN); S1 layer 1 (Release 8)

- 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 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*.

The following procedures are located in this chapter:

- Configuring the System as a Standalone MME (base configuration)
- Configuring Optional Features on the MME

Important: At least one Packet Services Card (PSC/PSC2) must be made active prior to service configuration. Information and instructions for configuring PSCs/PSC2s to be active can be found in the *Configuring System Settings* chapter of the *System Administration Guide*.

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. For a more robust configuration example, refer to the *Sample Configuration Files* appendix.

The configuration in this section assumes the following:

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

Information provided in this section includes the following:

- Information Required
- MME 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)	

Required Information	Description
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.
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.
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.

Required Information	Description
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.
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.

Required Information	Description
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	
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

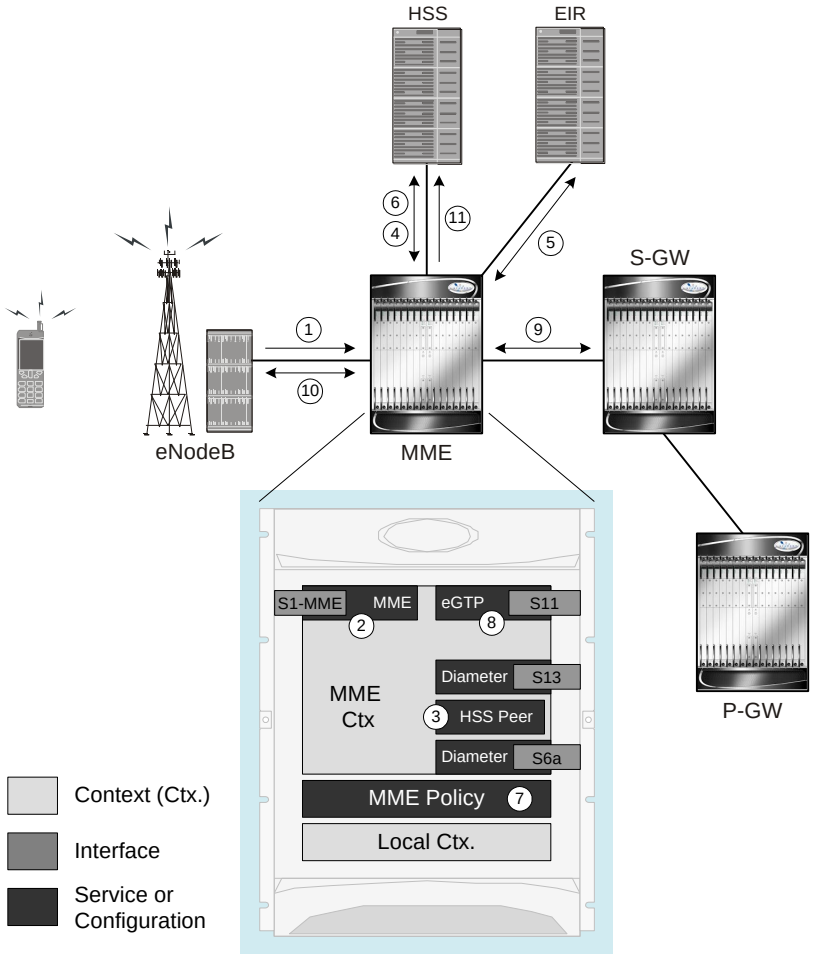
The following table lists the information that is required to configure the MME Policy on an MME.

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.

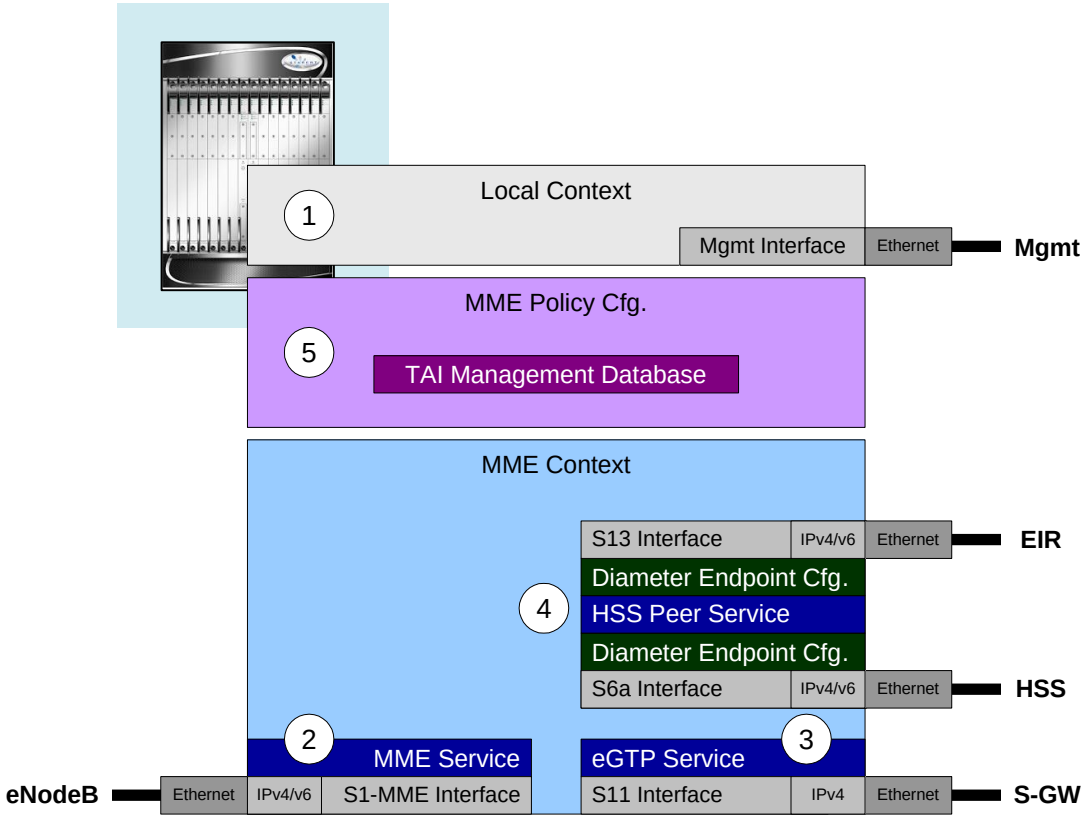


1. The eNodeB forwards an Attach Request message from the UE to the MME containing the IMSI, last visited TAI (if available), the UE's core network capability, the PDN Type, and the Attach Type.
2. The MME service receives the Attach Request message and references the HSS peer service for authentication 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 acknowledgement 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 Creating and Configuring the MME Context and Service section.

Step 3 Create the eGTP service and associate it with the S11 interface by applying the example configuration in the Creating and Configuring the eGTP Service and Interface Association 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 Creating and Configuring the HSS Peer Service and Interface Associations section.

Step 5 Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

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>
         mme-id group-id <grp_id> mme-code <mme_code>
         plmn-id mcc <mcc_value> mnc <mnc_value>
         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.
- Muli-homing is supported on the S1-MME and S6a interfaces. Refer to the Configuring SCTP Multi-homing Support section in this chapter for more information on configuring multi-homing for the S1-MME and/or S6a interface(s).
- 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 eGTP service is configured in the following section.
- The HSS peer service is configured in the Creating and Configuring the HSS Peer Service and Interface Associations section.
- 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. Refer to the Configuring SCTP Multi-homing Support section for information on configuring SCTP multi-homing for the S6a interface.

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.

The following optional configurations are provided in this section:

- Configuring Circuit Switched Falllback
- Configuring Dual Address Bearers
- Configuring Dynamic Peer Selection
- Configuring Gn/Gp Handover Capability
- Configuring Inter-MME Handover Support
- Configuring IP Security on the S1-MME Interface
- Configuring Load Balancing on the MME
- Configuring Mobility Restriction Support
- Configuring Optimized Paging
- Configuring Release 8 SGSN Handover Capability
- Configuring SCTP Multi-homing Support
- Configuring Static S-GW Pools
- Configuring User Location Information Reporting Support

Configuring Circuit Switched Falllback

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 Fall-back capability.

Important: Circuit Switched Fallback 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 circuit switched fall-back 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>
```

```
            exit
         exit
      exit
   context <mme_context_name> -noconfirm
      interface <sgs_intf_name>
         ip address <ipv4_address>
         exit
      sgs-service <name>
         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 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.
- Multiple TAC-to LAC values can be entered in the same configuration line.
- Multiple LAC values can be entered in the same configuration line.
- The VLR interface (**`vlr`** command) also supports IPv6 addressing and SCTP multi-homing.

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 **contex** <*ctx_name*> command/variable must be added to the command(s).

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 signalling 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
         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 section in this chapter.
- If dynamic peer-SGSN selection is configured, an additional gtpc command must be added to the SGTP service: **gtpc dns-sgsn contex** <*cntxt_name*>

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 **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 section in this chapter.
- The peer MME IP address can also be specified as an IPv6 address.

Configuring IP Security on the S1-MME Interface

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

Important: IP Security is a licensed feature and requires the purchase of the IP Security feature license to enable it.

The following configuration examples are included in this section:

- Creating and Configuring an IPSec Transform Set
- Creating and Configuring an IKEv2 Transform Set
- Creating and Configuring a Crypto Template
- Binding the S1-MME IP Address to the Crypto Template

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 IKEvs 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 securty key is allowed to exist, in seconds.
- The prf command configures the IKE Psuedo-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.
- The **bind** command also allows the interface(s) to be associated with a crypto map supporting IP Security. This support applies to both IPv4 and IPv6 addresses.

Configuring Load Balancing on the MME

In networks that contain multiple MMEs configured as a pool, load balancing is a necessary feature allowing UE attachments to be spread accross the pool instead of a small number of MMEs.

The following example configures load balancing on an MME:

```
configure
   context <mme_context_name>
      mme-service <mme_svc_name>
         relative-capacity <number>
         end
```

Notes:

- The **relative-capacity** command specifies a weight factor used in comparing the capacity of the MME to other MMEs in a pool.

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> <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 Optimized Paging

The example configuration in this section allows the MME to perform optimized, idle-mode paging, reducing the number of messages carried over the E-UTRAN access network.

Important: Optimized Paging is a licensed feature and requires the purchase of the Optimized Paging feature license to enable it.

The following configuration example enables optimized paging on the MME:

```
configure
   context <mme_context_name>
      mme-service <mme_svc_name>
         heuristic-paging
         end
```

Configuring Release 8 SGSN Handover Capability

This configuration example configures an S3 interface supporting inter-RAT handovers between the MME and a Release 8 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
```

```
            exit
         exit
      port ethernet <slot_number/port_number>
         no shutdown
         bind interface <s3_interface_name> <mme_context_name>
         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 section in this chapter.

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 Creating and Configuring the MME Context and Service section. 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
```

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 the Creating and Configuring the MME Context and Service section and the Diameter configuration for the S6a interface located in the Creating and Configuring the HSS Peer Service and Interface Associations section. Use the following example to configure S6a multi-homing between the MME and theHLR/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 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.
- 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.

Configuring User Location Information Reporting Support

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

Important: 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
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 5000. 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)
- 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 SGSN

The following is only a sampling of what working operator policies can control on an SGSN:

- APN information included in call activation messages are sometimes damaged, misspelled, missing. In such cases, the calls are rejected. The operator can ensure calls aren't rejected and configure a range of methods for handling APNs, including converting incoming APNs to preferred APNs and this control can be used in a focused fashion or defined to cover ranges of subscribers.
- In another example, it is not unusual for a blanket configuration to be implemented for all subscriber profiles stored in the HLR. This results in a waste of resources, such as the allocation of the default highest QoS setting for all subscribers. An operator policy provides the opportunity to address such issues by allowing fine-tuning of certain aspects of profiles fetched from HLRs and, if desired, overwrite QoS settings received from HLR.

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 (PSCs), 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.
- 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 PSCs 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 PSCs, 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 (SGSN only).
- 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 PSCs, 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 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 PSCs, 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.
- 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.

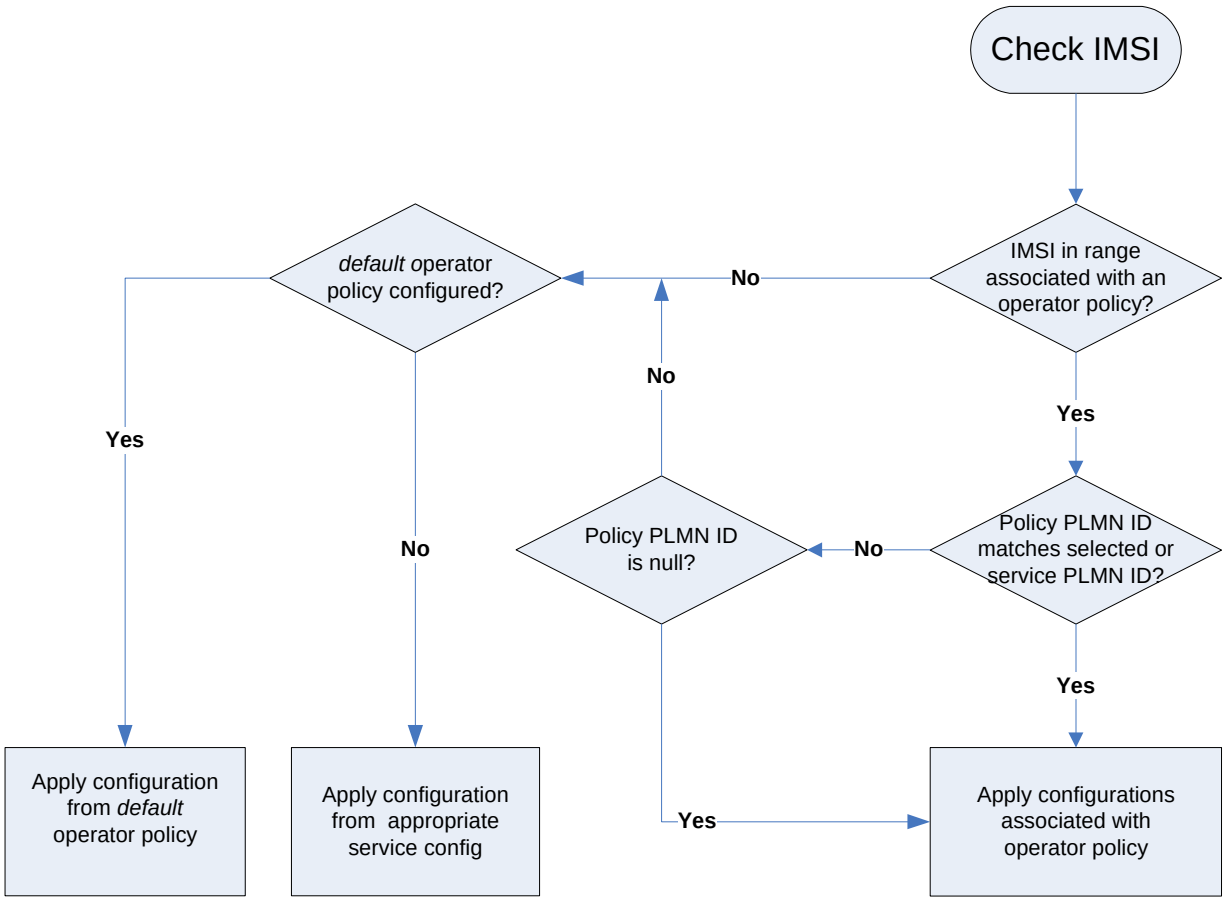
IMSI ranges are defined differently for each product supporting the operator policy feature.

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 12. 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: 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.

> ***Important:*** 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.

Step 3 Create and configure an IMEI profile by applying the example configuration presented in the *IMEI Profile Configuration* section.

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 the changes to a configuration.cfg file by applying the example configuration found in the *Saving the Configuration* section of the *Verifying and Saving Your Configuration* chapter in this book.

Step 9 Verify the configuration for each component separately by following the instructions provided the *Verifying the Feature Configuration* section.

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
```

Note:

- Refer to the *Call-Control Profile Configuration Mode* chapter in the *Cisco ASR 5000 Series 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
```

Note:

- 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
```

Note:

- 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
```

Note:

- 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 (MME-only)
      wildcard-apn pdp-type ipv4 network-identifier <apn_net_id>
      blank-apn network-identifier <apn_net_id> (SGSN only)
      end
```

Note:

- 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.

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
```

Note:

- 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>
      precedence <number> match-criteria imsi mcc <mcc_number> mnc <mnc_number>
msin first <start_range> last <end_range> operator-policy-name <policy_name>
```

```
end
```

Note:

- 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.

Configuring IMSI Ranges on the SGSN

The example below is specific to the SGSN and includes sample variables that you will replace with your own values.

```
configure
   sgsn-global
      imsi-range mcc 311 mnc 411 operator-policy oppolicy1
      imsi-range mcc 312 mnc 412 operator-policy oppolicy2
      imsi-range mcc 313 mnc 413 operator-policy oppolicy3
      imsi-range mcc 314 mnc 414 operator-policy oppolicy4
      imsi-range mcc 315 mnc 415 operator-policy oppolicy5
      end
```

Note:

- Operator policies are not valid until IMSI ranges are associated with them.

Operator Policy Component Associations - 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.

Associating Operator Policy Components on the MME

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.

Verifying the Feature Configuration

This section explains how to display the configurations after saving them in a .cfg file as described in the *Verifying and Saving Your Configuration* chapter elsewhere in this guide.

Important: All commands listed here are under Exec mode. Not all commands are available on all platforms.

Step 1 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]asr5000# 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
```

Note:

- 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 4
Verifying and Saving Your Configuration

This chapter describes how to save your system configuration.

Verifying the Configuration

You can use a number of commands to verify the configuration of your feature, service, or system. Many are hierarchical in their implementation and some are specific to portions of, or specific lines in, the configuration file.

Feature Configuration

In many configurations, you have to set and verify specific features. An example includes IP address pool configuration. Using this example, enter the following commands to verify proper feature configuration:

Enter the following command to display the IP address pool configuration:

show ip pool

The output from this command should look similar to the sample shown below. In this example, all IP pools were configured in the *isp1* context.

```
context : isp1:

+-----Type: (P) - Public (R) - Private

 | (S) - Static (E) - Resource

 |

 |+----State: (G) - Good (D) - Pending Delete (R)-Resizing

 ||

 ||++--Priority: 0..10 (Highest (0) .. Lowest (10))

 ||||

 ||||+-Busyout: (B) - Busyout configured

 |||| |||||| vvvvv Pool Name Start Address Mask/End Address Used Avail

 ----- --------- --------------- --------------- -------- --------

PG00 ipsec 12.12.12.0 255.255.255.0 0 254 PG00

pool1 10.10.0.0 255.255.0.0 0 65534 SG00

vpnpool 192.168.1.250 192.168.1.254 0 5 Total Pool Count: 5
```

Important: To configure features on the system, use the *show* commands specifically for these features. Refer to the *Cisco Systems ASR 5000 Command Line Interface Reference* for more information.

Service Configuration

Verify that your service was created and configured properly by entering the following command:

show <*service_type*> <*service_name*>

The output is a concise listing of the service parameter settings similar to the sample displayed below. In this example, a P-GW service called *pgw* is configured.

```
Service name : pgw1

Service-Id : 1

Context : test1

Status : STARTED

Restart Counter : 8

EGTP Service : egtp1

LMA Service : Not defined

Session-Delete-Delay Timer : Enabled

Session-Delete-Delay timeout : 10000(msecs)

PLMN ID List : MCC: 100, MNC: 99

Newcall Policy : None
```

Context Configuration

Verify that your context was created and configured properly by entering the following command:

show context name <*name*>

The output shows the active context. Its ID is similar to the sample displayed below. In this example, a context named *test1* is configured.

```
Context Name     ContextID     State

------------     ---------     -----

test1            2          Active
```

System Configuration

Verify that your entire configuration file was created and configured properly by entering the following command:

show configuration

This command displays the entire configuration including the context and service configurations defined above.

Finding Configuration Errors

Identify errors in your configuration file by entering the following command:

show configuration errors

This command displays errors it finds within the configuration. For example, if you have created a service named "service1", but entered it as "srv1" in another part of the configuration, the system displays this error.

You must refine this command to specify particular sections of the configuration. Add the **section** keyword and choose a section from the help menu:

show configuration errors section ggsn-service

or

show configuration errors section aaa-config

If the configuration contains no errors, an output similar to the following is displayed:

```
##############################################################################

Displaying Global
AAA-configuration errors
##############################################################################

Total 0 error(s) in this section !
```

Saving the Configuration

Save system configuration information to a file locally or to a remote node on the network. You can use this configuration file on any other systems that require the same configuration.

Files saved locally can be stored in the CompactFlash or a PCMCIA memory card on the SMC. Files that are saved to a remote network node can be transmitted through FTP or TFTP.

Saving the Configuration on the Chassis

These instructions assume that you are at the root prompt for the Exec mode:

[local]*host_name#*

To save your current configuration, enter the following command:

save configuration *url* **[-redundant] [-noconfirm] [showsecrets] [verbose]**

Table 7. Command Syntax for Saving the Configuration

Keyword/Variable	Description
url	Specifies the path and name to which the configuration file is to be stored. *url* may refer to a local or a remote file. *url* must be entered using one of the following formats: • **{ /flash | /pcmcia1 | /pcmcia2 }** *[/dir] /file_name* • **file:/{ /flash | /pcmcia1 | /pcmcia2 }** *[/dir] /file_name* • **tftp://**{ *ipaddress* | *host_name* [*:port#*] } [*/directory*] */file_name* • **ftp://**[*username* [*:pwd*] *@*] { *ipaddress* | *host_name* } [*:port#*] [*/directory*] */file_name* • **sftp://**[*username* [*:pwd*] *@*] { *ipaddress* | *host_name* } [*:port#*] [*/directory*] */file_name* **/flash** corresponds to the CompactFlash on the SMC. **/pcmcia1** corresponds to PCMCIA slot 1. **/pcmcia2** corresponds to PCMCIA slot 2. *ipaddress* is the IP address of the network server. *host_name* is the network server's *hostname*. *port#* is the network server's logical port number. Defaults are: • tftp: 69 - data • ftp: 20 - data, 21 - control • sftp: 115 - data Note: *host_name* can only be used if the **networkconfig** parameter is configured for DHCP and the DHCP server returns a valid nameserv er.dx *username* is the username required to gain access to the server if necessary. *password* is the password for the specified username if required. */directory* specifies the directory where the file is located if one exists. */file_name* specifies the name of the configuration file to be saved. Note: Configuration files should be named with a .cfg extension.
-redundant	Optional: This keyword directs the system to save the CLI configuration file to the local device, defined by the url variable, and then automatically copy that same file to the like device on the Standby SMC, if available. Note: This keyword will only work for like local devices that are located on both the active and standby SMCs. For example, if you save the file to the /pcmcia1 device on the active SMC, that same type of device (a PC-Card in Slot 1 of the standby SMC) must be available. Otherwise, a failure message is displayed. Note: When saving the file to an external network (non-local) device, the system disregards this keyword.

Keyword/Variable	Description
-noconfirm	Optional: Indicates that no confirmation is to be given prior to saving the configuration information to the specified filename (if one was specified) or to the currently active configuration file (if none was specified).
showsecrets	Optional: This keyword saves the CLI configuration file with all passwords in plain text, rather than their default encrypted format.
verbose	Optional: Specifies to display every parameter that is being saved to the new configuration file.

Important: The **`-redundant`** keyword is only applicable when saving a configuration file to local devices. This command does not synchronize the local file system. If you have added, modified, or deleted other files or directories to or from a local device for the active SMC, you must synchronize the local file system on both SMCs.

To save a configuration file called *system.cfg* to a directory that was previously created called cfgfiles on the CompactFlash in the SMC, enter the following command:

```
save configuration /flash/cfgfiles/system.cfg
```

To save a configuration file called *simple_ip.cfg* to a directory called *host_name_configs*, using an FTP server with an IP address of *192.168.34.156*, on which you have an account with a username of *administrator* and a password of *secure*, use the following command:

```
save configuration
ftp://administrator:secure@192.168.34.156/host_name_configs/
simple_ip.cfg
```

To save a configuration file called *init_config.cfg* to the root directory of a TFTP server with a hostname of *config_server*, enter the following command:

`save configuration` *`tftp://config_server/init_config.cfg`*

Chapter 5
Monitoring the Service

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 8. 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**
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 StatisticsRefer to the System Software Task and Subsystem Descriptions 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 couners**
View MME database statistics for all instances of DB	**show mme-service db statistics**

To do this:	Enter this command:
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*
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.

Chapter 6
Configuring Subscriber Session Tracing

This chapter provides information on subscriber session trace functionality to allow an operator to trace subscriber activity at various points in the network and at various level of details in EPS network. The product Administration Guides provide examples and procedures for configuration of basic services on the system. It is recommended that you select the configuration example that best meets your service model, and configure the required elements for that model, as described in the respective product Administration Guide, before using the procedures in this chapter.

Important: The features described in this chapter is an enhanced feature and need enhanced feature license. This support is only available if you have purchased and installed particular feature support license on your chassis.

This chapter discusses following topics for feature support of Subscriber Session Tracing in LTE service:

- Introduction
- Supported Standards
- Supported Networks and Platforms
- Licenses
- Subscriber Session Tracing Functional Description
- Subscriber Session Trace Configuration
- Verifying Your Configuration

Introduction

The Subscriber Level Trace 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 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

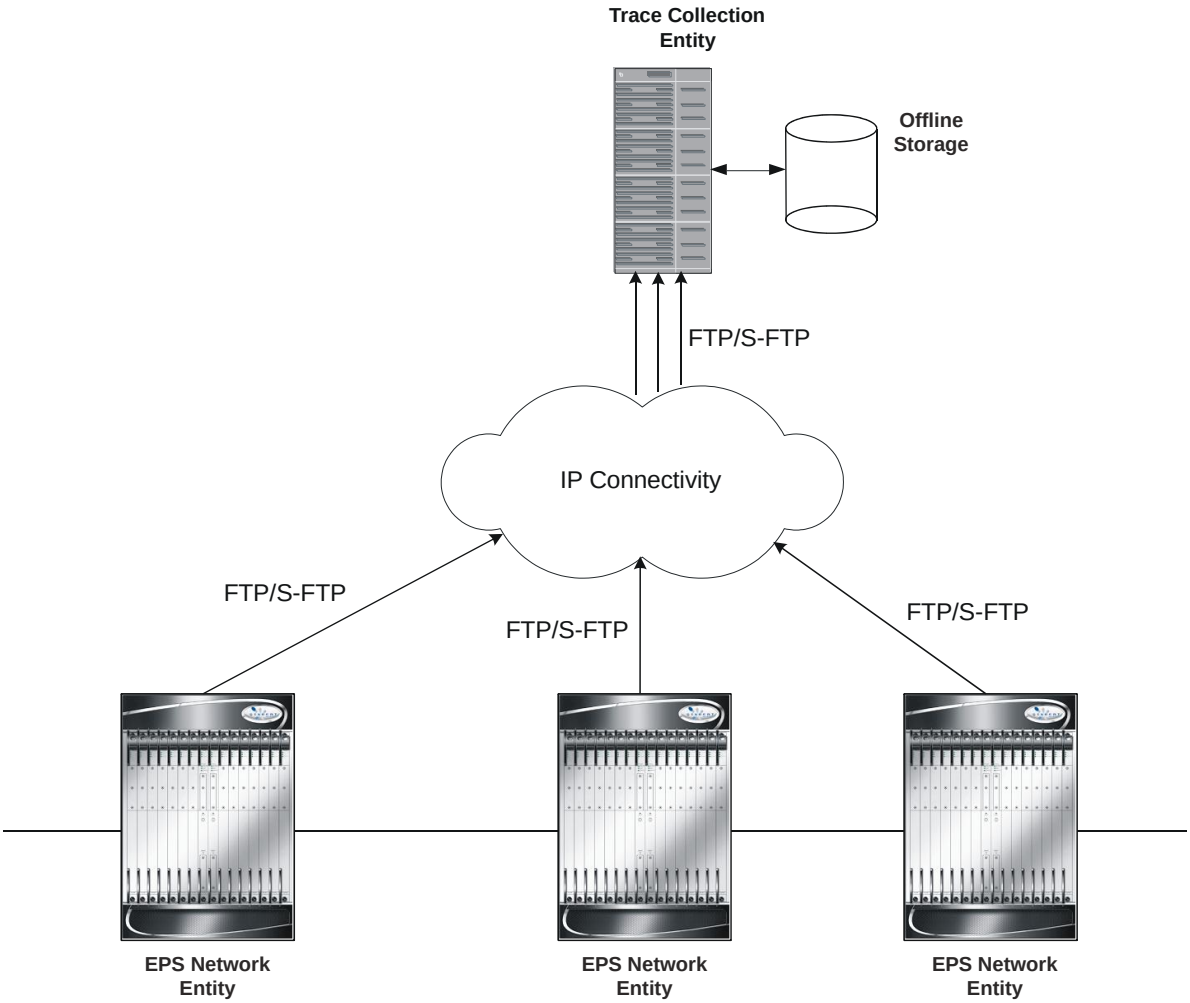
Important: Once the trace is provisioned it can be provisioned through the access cloud via various signaling interfaces.

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 ASR 5000 platforms. 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 13. 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 NE
    - Capacity to activate/deactivate TBD trace sessions per second
    - Each NE can buffer TBD bytes of trace data locally
- Statistics and State Support
- Session Trace Details
- Management and Signaling-based activation models
- Trace Parameter Propagation
- Trace Scope (EPS Only)
    - MME: S1, S3, S6a, S10, S11
    - 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

Supported Standards

Support for the following standards and requests for comments (RFCs) have been added with this interface support:

- 3GPP TS 32.421 V8.5.0 (2009-06): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Subscriber and equipment trace: Trace concepts and requirements (Release 8)
- 3GPP TS 32.422 V8.6.0 (2009-09): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Subscriber and equipment trace; Trace control and configuration management (Release 8)
- 3GPP TS 32.423 V8.2.0 (2009-09): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Subscriber and equipment trace: Trace data definition and management (Release 8)

Supported Networks and Platforms

This feature supports all ASR 5000 Series Platforms with StarOS Release 9.0 or later running MME/S-GW/P-GW service(s) for the core LTE network functions.

Licenses

This is a base feature and available for configuration with default LTE component license(s) on the system.

Subscriber Session Trace Functional Description

This section describes the various functionality involved in tracing of subscriber session 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).

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 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.

Management Activation

With a management-initiated activation, the WEM sends an activation request directly to the NE where the trace is to be initiated. 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 supprots data collection and reporting system to provide historical usage adn 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 support 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

Interface Name	Remote Device	Trace Signaling (De)Activation RX	Trace Signaling (De)Activation TX
S3	SGSN	Y	Y
S6a	HSS	Y	N
S10	MME	Y	Y
S11	S-GW	N	Y

S-GW

The S-GW support 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 PDN-GW support 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

Subscriber 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 the changes to system configuration by applying the example configuration found in *Verifying and Saving Your Configuration* chapter.

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 at the Exec mode:

```
session trace subscriber network-element { ggsn | mme | pgw | sgw } {
imei <imei_id> } { imsi <imsi_id> } { interface { all | <interface> } }
trace-ref <trace_ref_id> collection-entity <ip_address>
```

Notes:

- <*interface*> is the name of the interfaces applicable for specific NE on which subscriber session traces have to be collected. For more information, refer to the **session trace subscriber** command in the *Command Line Interface Reference*.
- <*trace_ref_id*> is the configured Trace Id to be used for this trace collection instance. It is composed of MCC (3 digit)+MNC (3 digit)+Trace Id (3 byte octet string).
- <*ip_address*> is the IP address of Trace collection Entity in IPv4 notation.

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 Saving Your Configuration chapter of this 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
```

Chapter 7
Troubleshooting the 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 PPP Echo-Test Command

The system provides a mechanism to verify the Point-to-Point Protocol session of a particular subscriber by sending Link Control Protocol (LCP) packets to the mobile node. This functionality can be extremely useful in determining the quality of the air link and delays that may occur.

The command has the following syntax:

```
ppp echo-test { callid call_id | ipaddr ip_address | msid ms_id |
username subscriber_name }
```

Keyword/Variable	Description
callid *call_id*	Specifies that the test is executed for a subscriber with a specific call identification number (callid). *call_id* is the specific call identification number that you wish to test.
ipaddr *ip_address*	Specifies that the test is executed for a subscriber with a specific IP address. ip_address is the specific IP address that you wish to test.
msid *ms_id*	Specifies that the test is executed for a subscriber with a specific mobile station identification (MSID) number. *ms_id* is the specific mobile station identification number that you wish to test.
username *subscriber_name*	Specifies that the test is executed for a subscriber with a specific username. *subscriber_name* is the specific username that you wish to test.

The following figure displays a sample of this command's output showing a successful PPP echo-test to a subscriber named user2@aaa.

```
USERNAME: user2@aaa MSID: 0000012345 CALLID: 001e8481

 Tx/Rx 1/0 RTT(min/max/avg) 0/0/0

USERNAME: user2@aaa MSID: 0000012345 CALLID: 001e8481

 Tx/Rx 1/1 RTT(min/max/avg) 77/77/77 (COMPLETE)
```

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.
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)
```

Using the DHCP Test Command

This command tests the system's ability to communicate with a Dynamic Host Control Protocol (DHCP) server. Testing is performed on a per-DHCP service basis for either a specific server or all servers the DHCP service is configured to communicate with. This functionality is useful for troubleshooting and/or monitoring.

Once executed, the test attempts to obtain an IP address from the DHCP server(s) and immediately release it.

Important: This command must be executed from within the context in which at least one MME service is configured.

The command has the following syntax:

dhcp test dhcp-service *svc_name* [**all** | **server** *ip_address*]

Keyword/Variable	Description
dhcp-service *svc_name*	The name of the DHCP service. *svc_name* can be from 1 to 63 alpha and/or numeric characters in length and is case sensitive.
all	Tests DHCP functionality for all servers.
server *ip_address*	Tests DHCP functionality for the server.

The following figure displays a sample of this command's output showing a successful DHCP test for a DHCP service called DHCP-Gi to a server with an IP address of 192.168.16.2. The IP address provided during the test was 192.168.16.144.

```
DHCP test status for service <DHCP-Gi>:

 Server address: 192.168.16.2 Status: Tested

 Lease address: 192.168.16.144 Lease Duration: 600 secs.
```

Appendix A
Engineering Rules

This section provides engineering rules or guidelines that must be considered prior to configuring the system for your network deployment.

This appendix describes following engineering rules for MME services:

- APN Engineering Rules
- DHCP Service Engineering Rules
- Service Engineering Rules

APN Engineering Rules

The following engineering rules apply to APNs:

- APNs must be configured within the context used for authentication.
- A maximum of 1,024 APNs per system can be configured.

DHCP Service Engineering Rules

The following engineering rule applies to the DHCP Service:

- Up to 8 DHCP servers may be configured per DHCP service.
- A maximum of 3 DHCP server can be tried for a call.

Service Engineering Rules

The following engineering rules apply to services configured within the system:

- A maximum of 256 services (regardless of type) can be configured per system.

> **Caution:** Large numbers of services greatly increase the complexity of management and may impact overall system performance (i.e. resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

- The total number of entries per table and per chassis is limited to 256.
- 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 difficulty understanding outputs of show commands.