Cisco ASR 5000 Series Mobility Management Entity Administration Guide

Version 11.0

Last Updated January 14, 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-24222-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

Reorient or relocate the receiving antenna.

Increase the separation between the equipment and receiver.

Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB’s public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco ASR 5000 Series Mobility Management Entity Administration Guide

© 2011 Cisco Systems, Inc. and/or its affiliated entities. All rights reserved.

CONTENTS

About this Guide vii
Conventions Used viii
Contacting Customer Support x
Mobility Management Entity Overview 11
SAE Network Summary 12
E-UTRAN / EPC Network Components 13
eNodeB 14
Mobility Management Entity (MME) 14
Serving Gateway (S-GW) 14
PDN Gateway (P-GW) 15
Product Description 16
Product Specification 19
Licenses 19
Hardware Requirements 19
Platforms 19
System Hardware Components 19
Operating System Requirements 20
Network Deployment and Interfaces 21
MME in the LTE/SAE Network 21
Supported Interfaces 22
Features and Functionality - Base Software 25
Network Access Control Functions 25
Authentication and Key Agreement (AKA) 25
HSS Support Over S6a Interface 26
Network Entity Management 27
3GPP R8 Identity Support 27
Interworking with Pre-Release 8 SGSNs on Gn Interface 28
MME Selection 28
Packet Data Network Gateway (P-GW) Selection 29
Reachability Management 29
Serving Gateway (S-GW) Pooling Support 29
Serving Gateway (S-GW) Selection 30
Tracking Area List Management 30
Network Operation Management Functions 30
IPv6 Transport for S1-MME 31
MME Load Balancing 31
MME Mobility Restriction 31
MME Pooling 31
Mobile Equipment Identity Check 32
Multiple PDN Support 32
Overload Management in MME 32
Radio Resource Management Functions 32
SCTP Multi-homing for S1-MME 33
Session and Quality of Service Management 33
Subscriber Session Management Features 33
EPS Bearer Context Support 34

EPS GTPv2 Support on S11 Interface 34
Heuristic Paging Support 35
MME APN Restriction 35
NAS Protocol Support 36
Operator Policy Support 36
Subscriber Level Session Trace 37
System Management Features 38
Bulk Statistics Support 39
Management System Overview 39
NAS Signalling Security 41
Threshold Crossing Alerts (TCA) Support 42
Features and Functionality - Licensed Enhanced Feature Software 44
Circuit Switched Fall Back (CSFB) and SMS over SGs Interface 44
IPv6 Support 45
Lawful Intercept 46
Session Recovery Support 47
Web Element Management System 47
How MME Works 49
EPS Bearer Context Processing 49
Purge Procedure 49
Paging Procedure 50
Subscriber Session Processing 50
Subscriber Registration Setup Procedure 50
User-initiated Subscriber De-registration Setup Procedure 52
Service Request Procedure 53
User-initiated Service Request Procedure 53
Network-initiated Service Request Procedure 55
Supported Standards 56
3GPP References 56
IETF References 57
Object Management Group (OMG) Standards 59
Mobility Management Entity Configuration 61
Configuring the System as a Standalone MME (base configuration) 62
Information Required 62
Required MME Context Configuration Information 62
Required MME Policy Configuration Information 64
MME Configuration 65
Creating and Configuring the MME Context and Service 66
Creating and Configuring the eGTP Service and Interface Association 67
Creating and Configuring the HSS Peer Service and Interface Association 68
Configuring the MME Policy 68
Configuring Optional Features on the MME 70
Configuring Dynamic S-GW/P-GW Selection 70
Configuring Gn/Gp Handover Capability 71
Configuring Support for Dual Address Bearers 71
Verifying and Saving Your Configuration 73
Verifying the Configuration 74
Feature Configuration 74
Service Configuration 75
Context Configuration 76
System Configuration 76
Finding Configuration Errors 76
Saving the Configuration 78
Saving the Configuration on the Chassis 79

Monitoring the Service 81
Monitoring System Status and Performance 82
Clearing Statistics and Counters 85
Configuring Subscriber Session Tracing 87
Introduction 88
Supported Functions 89
Supported Standards 91
Supported Networks and Platforms 92
Licenses 93
Subscriber Session Trace Functional Description 94
Operation 94
Trace Session 94
Trace Recording Session 94
Network Element (NE) 94
Activation 94
Management Activation 95
Signaling Activation 95
Start Trigger 95
Deactivation 95
Stop Trigger 95
Data Collection and Reporting 96
Trace Depth 96
Trace Scope 96
Network Element Details 96
MME 96
S-GW 97
P-GW 97
Subscriber Session Trace Configuration 98
Enabling Subscriber Session Trace on EPC Network Element 98
Trace File Collection Configuration 99
Verifying Your Configuration 100
Troubleshooting the Service 103
Test Commands 104
Using the PPP Echo-Test Command 104
Using the eGTPC Test Echo Command 105
Using the DHCP Test Command 105
Engineering Rules 107
APN Engineering Rules 108
DHCP Service Engineering Rules 109
Lawful Intercept Engineering Rules 110
Service Engineering Rules 111

About this Guide

This document pertains to 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 LTE/SAE wireless carriers with a flexible solution that functions as a Mobility Management Entity (MME) in 3GPP Long-Term Evolution/System Architecture Evolution wireless data networks.

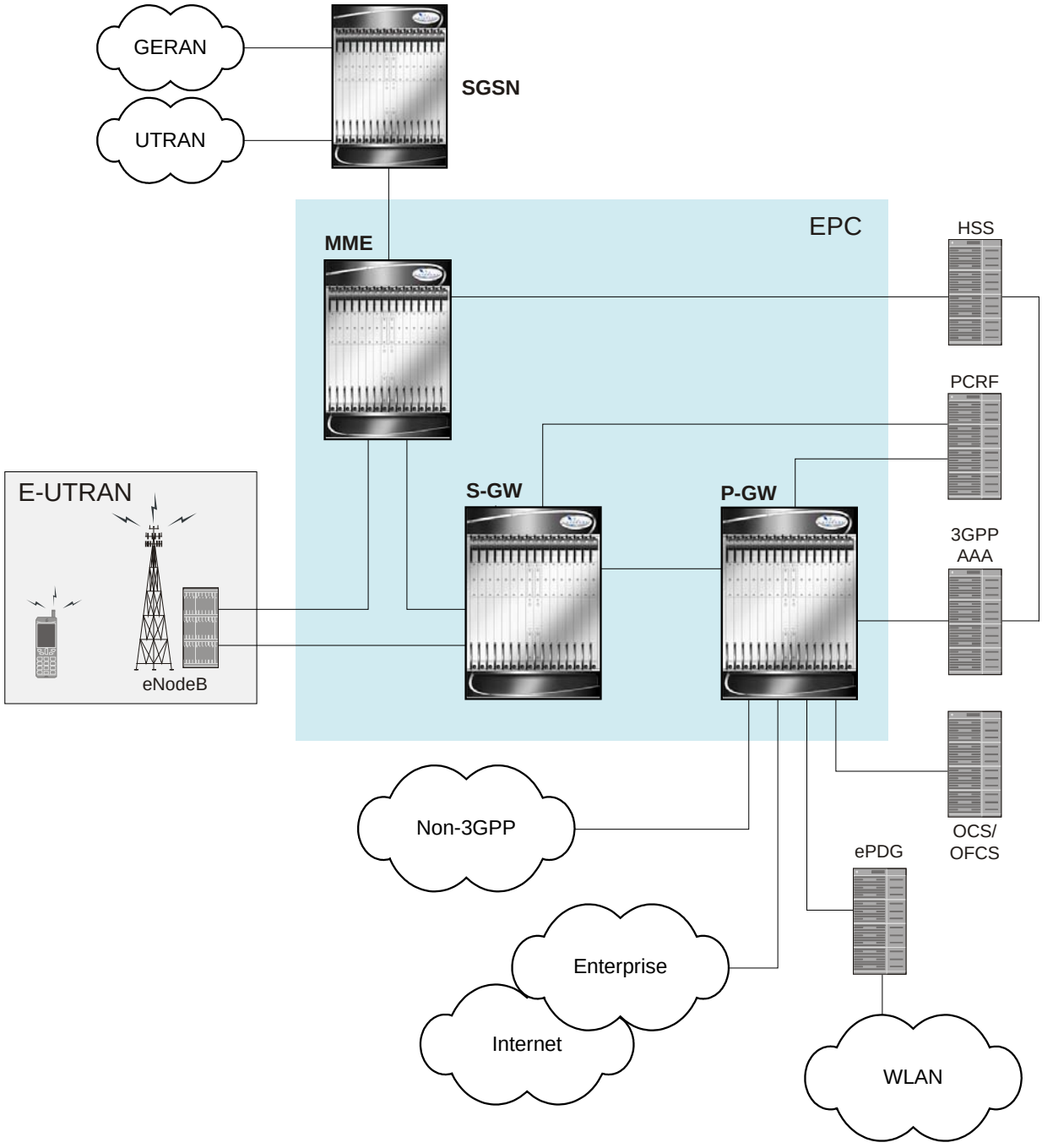
This overview provides general information about the MME including:

- SAE Network Summary
- Product Description
- Product Specification
- Network Deployment and Interfaces
- Features and Functionality - Base Software
- Features and Functionality - Licensed Enhanced Feature Software
- How 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 (GSM, UMTS, and LTE) and non-3GPP radio access technologies, including CDMA, WiMAX, WiFi, High Rate Packet Data (HRPD), evolved HRPD, and ETSI defined TISPAN networks.

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



E-UTRAN / EPC Network Components

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

eNodeB

The eNodeB is the E-UTRAN base station and is one of two nodes in the SAE Architecture user plane (the other is the 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:

- NAS
    - signalling
    - signalling security
- UE access in ECM-IDLE state (including control and execution of paging retransmission)
- Tracking Area (TA) list management
- 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 interface to HSS (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 GTP-based and the 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 PDN GW)
    - 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
- MAG for PMIP based S5 and S8

PDN Gateway (P-GW)

For each UE associated with the 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
    - UL and DL service level charging, gating control, and service level rate enforcement
    - DL rate enforcement based on AMBR (Aggregate Max Bit Rate) and based on the accumulated MBRs of the aggregate of SDFs with the same GBR QCI
- 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 Evolved NodeB (eNodeB), Serving Gateway (S-GW) within the Evolved Packet Core (EPC), or LTE/SAE core network to perform the following functions:

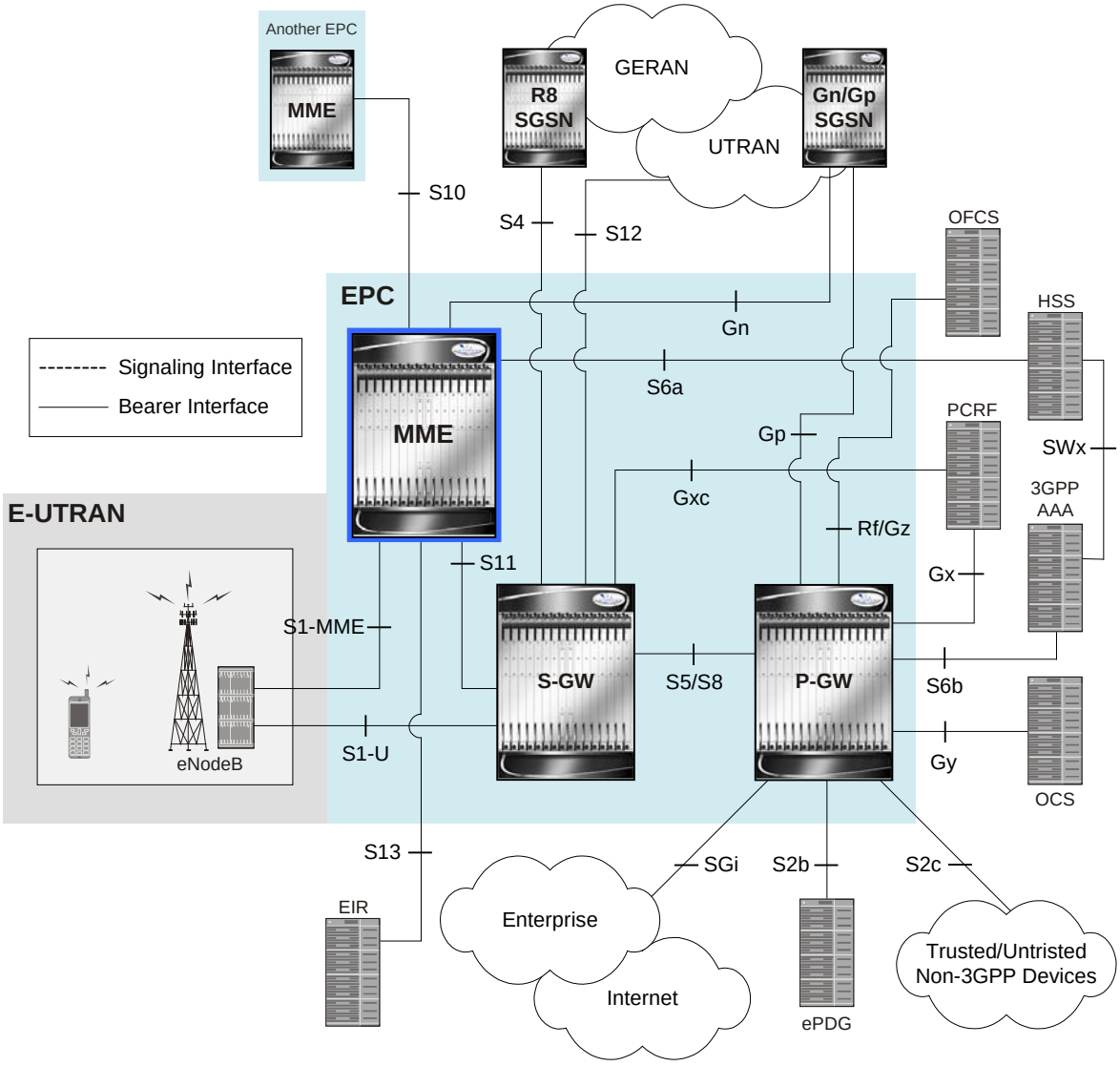
- Involved in the bearer activation/deactivation process and is also responsible for choosing the S-GW and for a UE at the initial attach and at time of intra-LTE handover involving Core Network (CN) node relocation.
- Provides PDN Gateway (P-GW) selection for subscriber to connect to PDN.
- Provides idle mode UE tracking and paging procedure, including retransmissions.
- 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 MME in same PLMN or on different PLMNs. The S10 interface is used for MME relocation and MME to MME information transfer or handoff.

Besides 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)**: Within the ASR 5000 platform, PSCs/PSC2s provide high-speed, multi-threaded EPS Bearer context processing capabilities for MME services. Up to 14 PSCs/PSC2s 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 and/or Ethernet 1000 Line Cards**: 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, 13 in the upper-rear slots and 13 in the lower-rear slots for redundancy. Redundant PSCs/PSC2s 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.

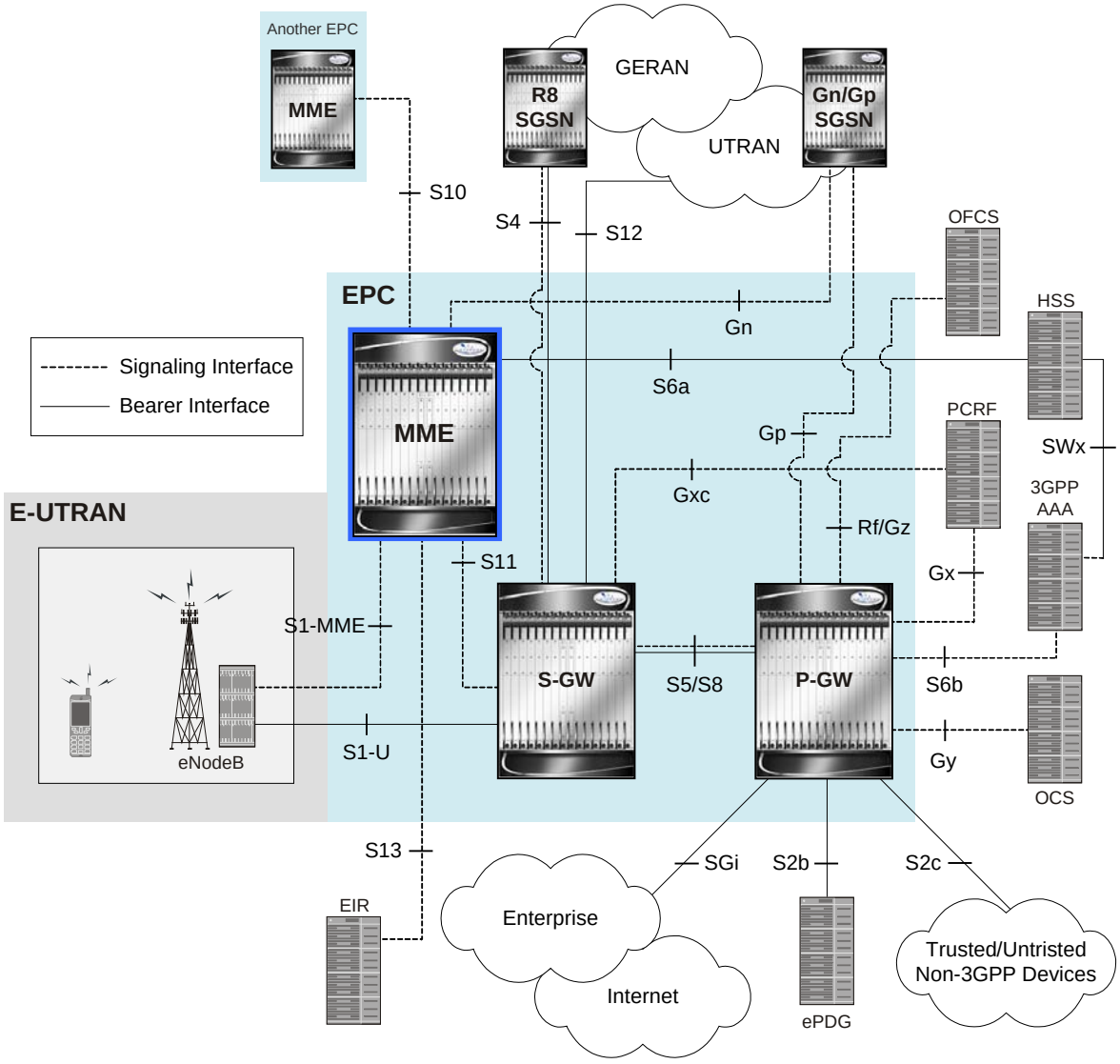
The following information is provided in this section:

- MME in the LTE/SAE Network
- Supported Interfaces

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.

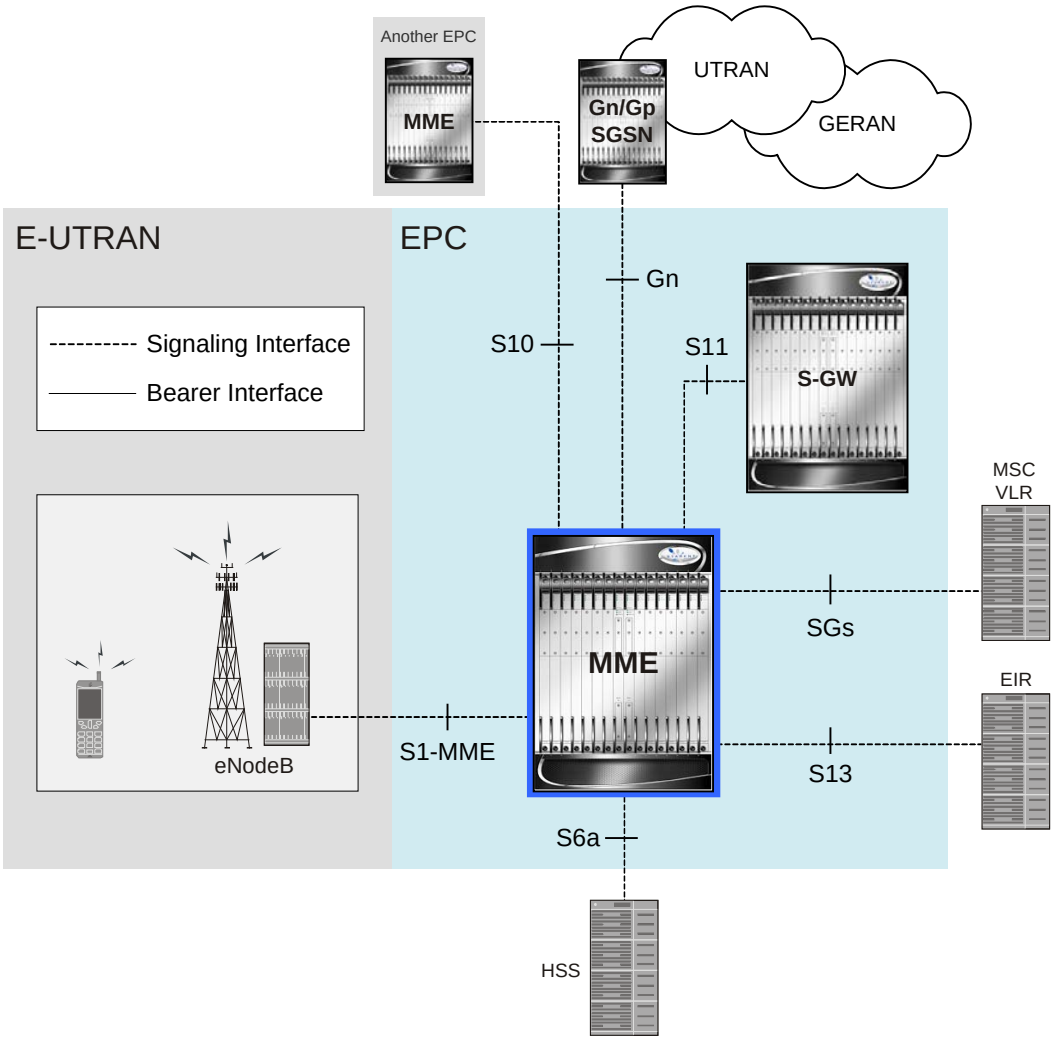
Figure 2. Interfaces in the E-UTRAN/EPC Network



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.

- **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 MME in 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/Gp Interface**: Gn/Gp interfaces facilitate user mobility between 2G/3G 3GPP networks. The Gn interface is used for intra-PLMN, and the Gp interface is used for inter-PLMN handovers. MME supports pre-Release-8 Gn/Gp 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 base software on MME service and do not require any additional license to implement the functionality with the MME service.

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

Following features and supports are discussed in this section:

- Network Access Control Functions
- Network Entity Management
- Network Operation Management Functions
- Session and Quality of Service Management
- Subscriber Session Management Features
- System Management Features

Network Access Control Functions

These functions enable secure user and device level authentication between the authenticator component of the MME and a 3GPP HSS / AuC and Diameter-based S6a interface support.

This section describes following features:

- Authentication and Key Agreement (AKA)
- HSS Support Over S6a Interface

Authentication and Key Agreement (AKA)

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.

The 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; confidentiality of signalling data; and confidentiality of user data

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.

Network Entity Management

This section describes following features:

- 3GPP R8 Identity Support
- Interworking with Pre-Release 8 SGSNs on Gn Interface
- MME Selection
- Packet Data Network Gateway (P-GW) Selection
- Reachability Management
- Serving Gateway (S-GW) Pooling Support
- Serving Gateway (S-GW) Selection
- 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.

Interworking with Pre-Release 8 SGSNs on Gn Interface

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.

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.

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.

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.

Serving Gateway (S-GW) 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 GWs. Each cell is associated to a pool of MMEs and a pool of S-GWs. Once a cell selects an MME, that MME is able to select an S-GW which is in a S-GW pool supported by the cell.

Static S-GW pools are configurable on the MME. Each pool is organized as a set of S-GWs and the TAIs supported by those S-GWs, known as a service area (SA). The incoming TAI is used to select an SA. Then, based on protocol and statistical weight factor, an S-GW is selected from the pool of S-GWs 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.

Serving Gateway (S-GW) Selection

The Serving GW (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.

S-GW selection chooses an available S-GW to serve a UE. 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.

Tracking Area List Management

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

The MME assigns the TAI list to a UE so as to minimize the TA updates that would be sent by the UE. The TAI list should not be very long as this would mean that the paging load would be high. There is a trade-off between paging load and Tracking Area Update procedures number.

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

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

Network Operation Management Functions

This section describes following features:

- IPv6 Transport for S1-MME
- MME Load Balancing
- MME Mobility Restriction
- MME Pooling
- Mobile Equipment Identity Check
- Multiple PDN Support
- Overload Management in MME
- Radio Resource Management Functions
- SCTP Multi-homing for S1-MME

IPv6 Transport for S1-MME

The S1-MME interface service is supported on native IPv6. The Cisco MME service can run S1-AP/SCTP over IPv6 and support IPv6 addresses for S1-U endpoints.

MME Load Balancing

The MME load balancing functionality permits UEs that are entering into an MME pool area to be directed to an appropriate MME in a manner that achieves load balancing between 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 Mobility Restriction

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

The Handover Restriction List is used by the MME operator policy and specifies roaming, service area, and access restrictions. Mobility restrictions at the MME are defined in 3GPP TS 23.401.

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.
- 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.

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 ME Identity is checked by the MME passing it to an Equipment Identity Register (EIR) and then the MME analyzes the response from the EIR in order to determine its subsequent actions; like rejecting/attaching a UE.

Multiple PDN Support

It provides multiple PDN connectivity support for UE initiated service request.

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

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 eNodeB's 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 *Enhanced Feature Configuration 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.

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.

SCTP Multi-homing for S1-MME

The Cisco MME service supports up to two SCTP bind end point IPv4 or IPv6 addresses.

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 Session Management Features

This section describes following features:

- EPS Bearer Context Support
- EPS GTPv2 Support on S11 Interface
- Heuristic Paging Support
- MME APN Restriction

- NAS Protocol Support
- Operator Policy Support
- Subscriber Level Session Trace

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*.

Heuristic Paging Support

Reduced 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 acutely felt 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 3M 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.

MME APN Restriction

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.

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.

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.

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

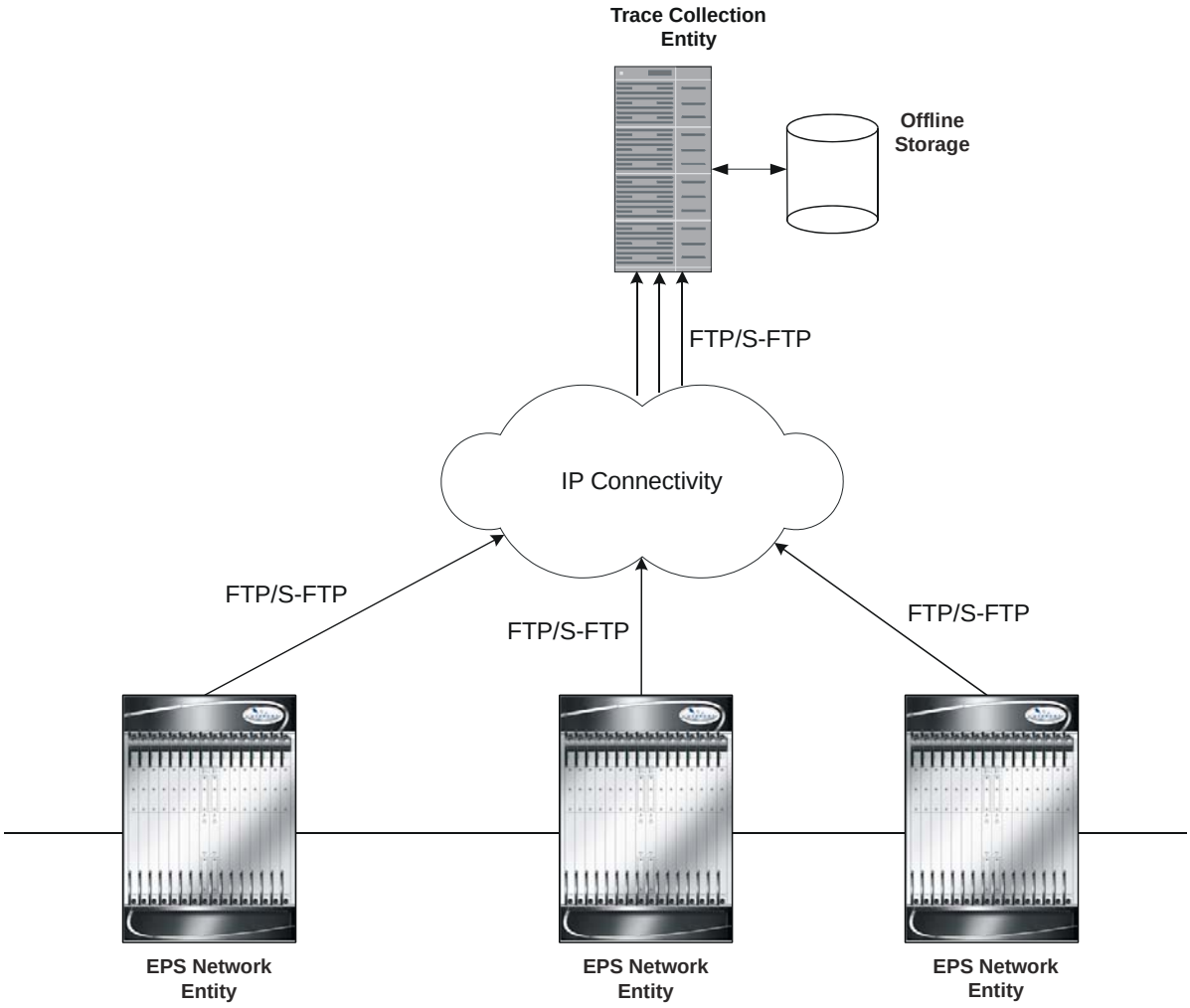
The session level trace function consists of trace activation followed by triggers. The time between the two events is treated much like Lawful Intercept where the EPC network element buffers the trace activation instructions for the provisioned subscriber in memory using camp-on monitoring. Trace files for active calls are buffered as XML files using non-volatile memory on the local dual redundant hard drives. 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 4. 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*.

System Management Features

This section describes following features:

- Bulk Statistics Support
- Management System Overview
- NAS Signalling Security
- Threshold Crossing Alerts (TCA) Support

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.

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.

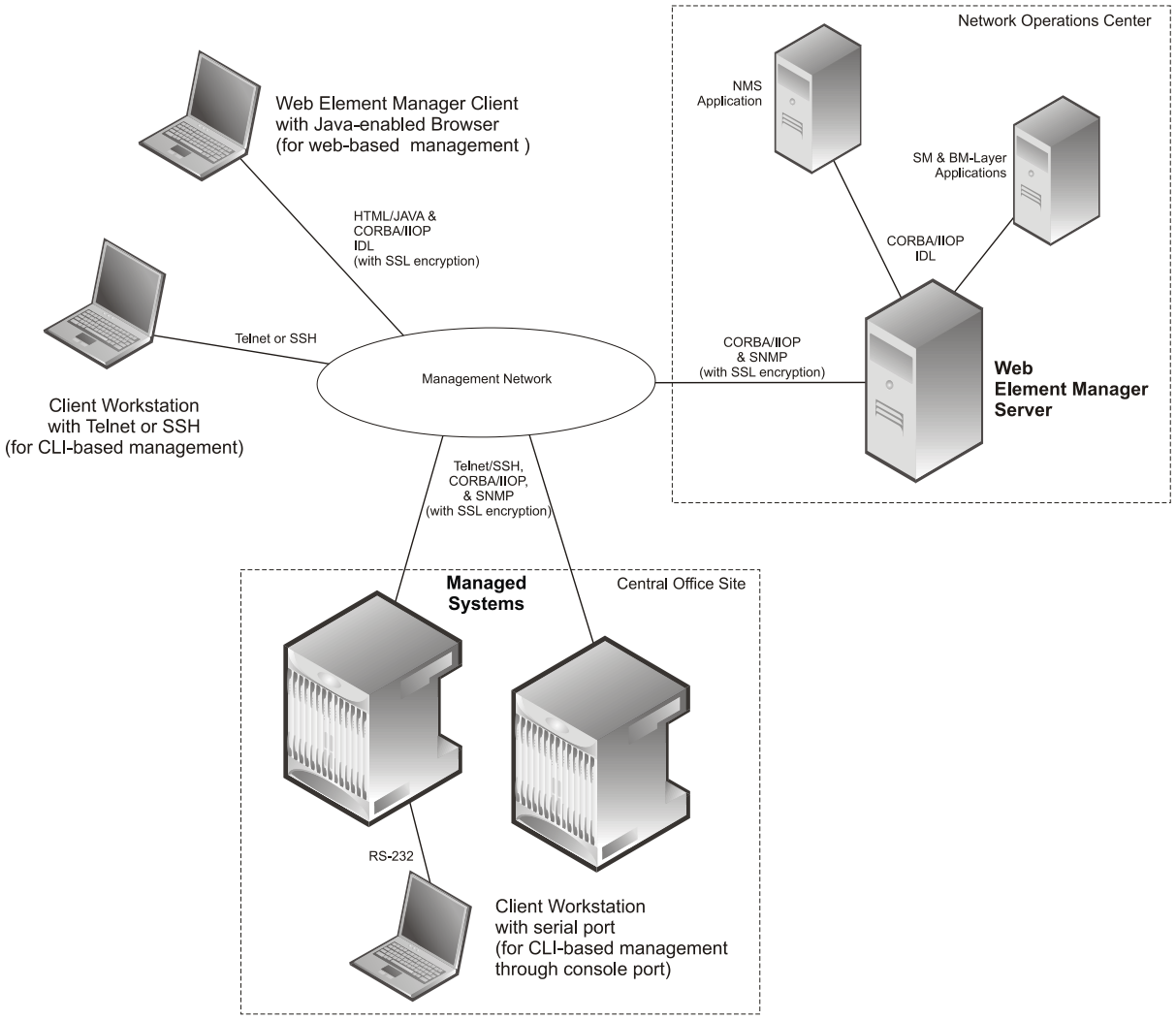
Operation and Maintenance module of ASR 5000 offers comprehensive management capabilities to the operators and enables them to operate the system more efficiently. There are multiple ways to manage the system either locally or remotely using its out-of-band management interfaces.

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 5. 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*.

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

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*.

Features and Functionality - Licensed Enhanced Feature Software

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

Important: Some of the following features require the purchase of an additional 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
- IPv6 Support
- Lawful Intercept
- Session Recovery Support
- Web Element Management System

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 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: Only SMS over SGs is supported at this time. CSFB to CDMA 1x networks is not supported in this release. Telephony services (voice applications) will be supported in a future 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.

IPv6 Support

This feature allows IPv6 subscribers to connect via the GPRS/UMTS 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 23.060: General Packet Radio Service (GPRS) Service description
- 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.

Lawful Intercept

Provides a standards-based architecture for lawful monitoring and interception of subscriber call control events as mandated by a warrant from a law enforcement agency.

In accordance with 3GPP TS 33.108 Release 8 requirements the Cisco MME supports the Lawful Intercept Access Function for intercepting control plane traffic pursuant to a court ordered subpoena. Lawful Intercept involves the process of mirroring subscriber call control or call content based on a request from a law enforcement agency to a telecom service provider.

In this release the MME support the X1 provisioning interface and X2 interface for mirroring Intercept Related Information (IRI) to an upstream Delivery Function/Mediation server. Intercept targets can be provisioned using subscriber information including MSISDN, IMSI and MEI. The Cisco MME supports secure provisioning via remote CLI over SSH connections from a DF mediation server. Our solution is currently interoperable with leading third party solutions.

The intercepted call control data is encoded in a Cisco proprietary message header format using an optional TLV field to pack the IRI information. The message header includes other identifying information including sequence numbers, timestamps and session & correlation numbers to correlate session and bearer related information with interception on other EPC elements. The MME can intercept any of the following IRI information:

- Subscriber attachments
- Subscriber detachments
- Tracking Area Updates
- UE requested PDN connectivity
- UE requested PDN disconnection

Important: For more information on Lawful Intercept support, refer to the *Lawful Intercept Configuration Guide*.

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* chapter in *System Enhanced Feature Configuration Guide*.

Web Element Management System

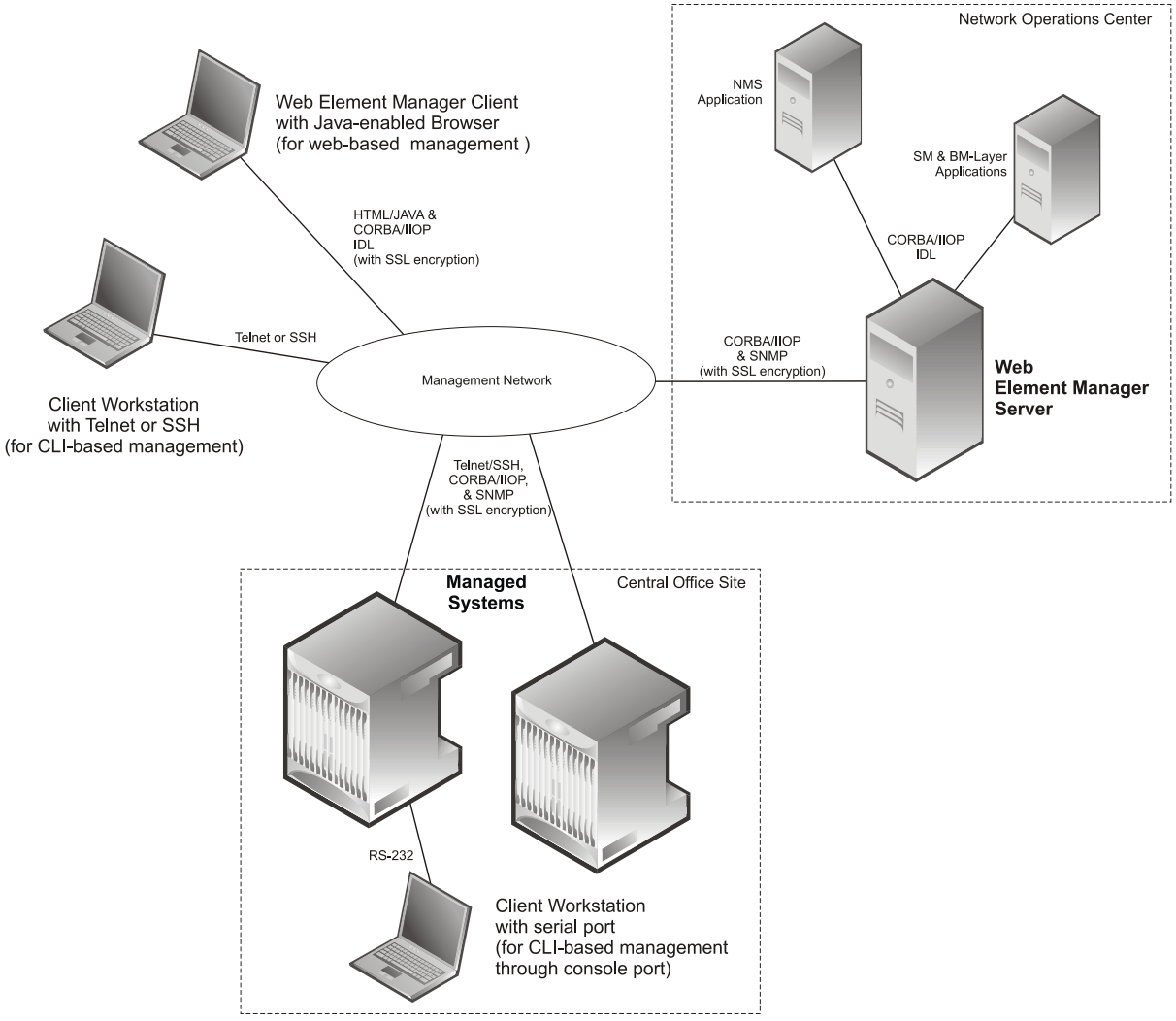
Provides a graphical user interface (GUI) for performing fault, configuration, accounting, performance, and security (FCAPS) management.

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*.

How 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
- Connection Setup and Registration Procedures
    - Subscriber Registration Setup Procedure
- UE De-registration Procedures
    - User-initiated Subscriber De-registration Setup Procedure
- Service Request Procedure
    - User-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

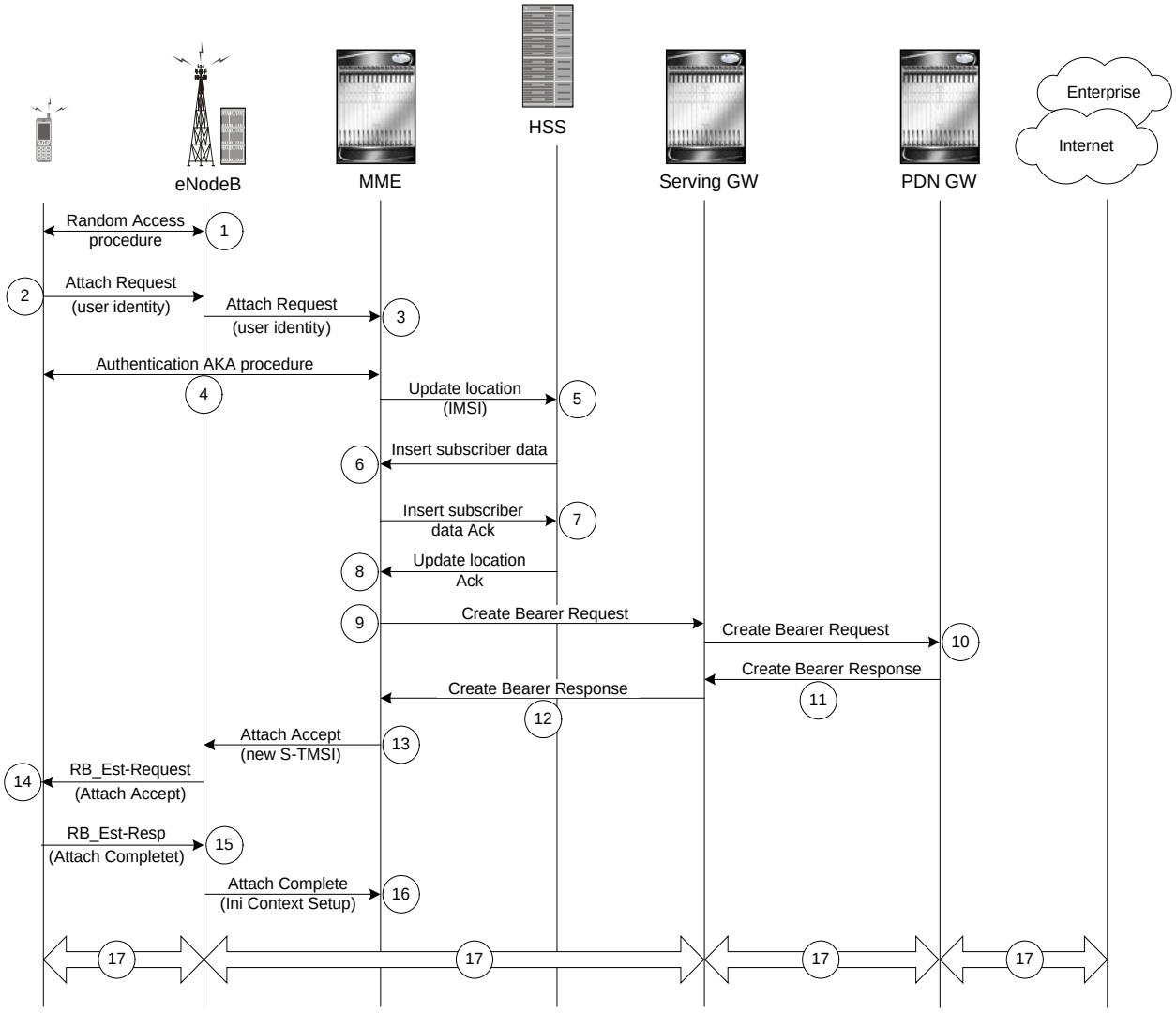
This section provides information on how LTE/SAE subscriber data sessions are processed by the system MME. The following procedures are provided:

- **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 Registration Setup Procedure

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

Figure 7. Subscriber Registration Setup Message Flow



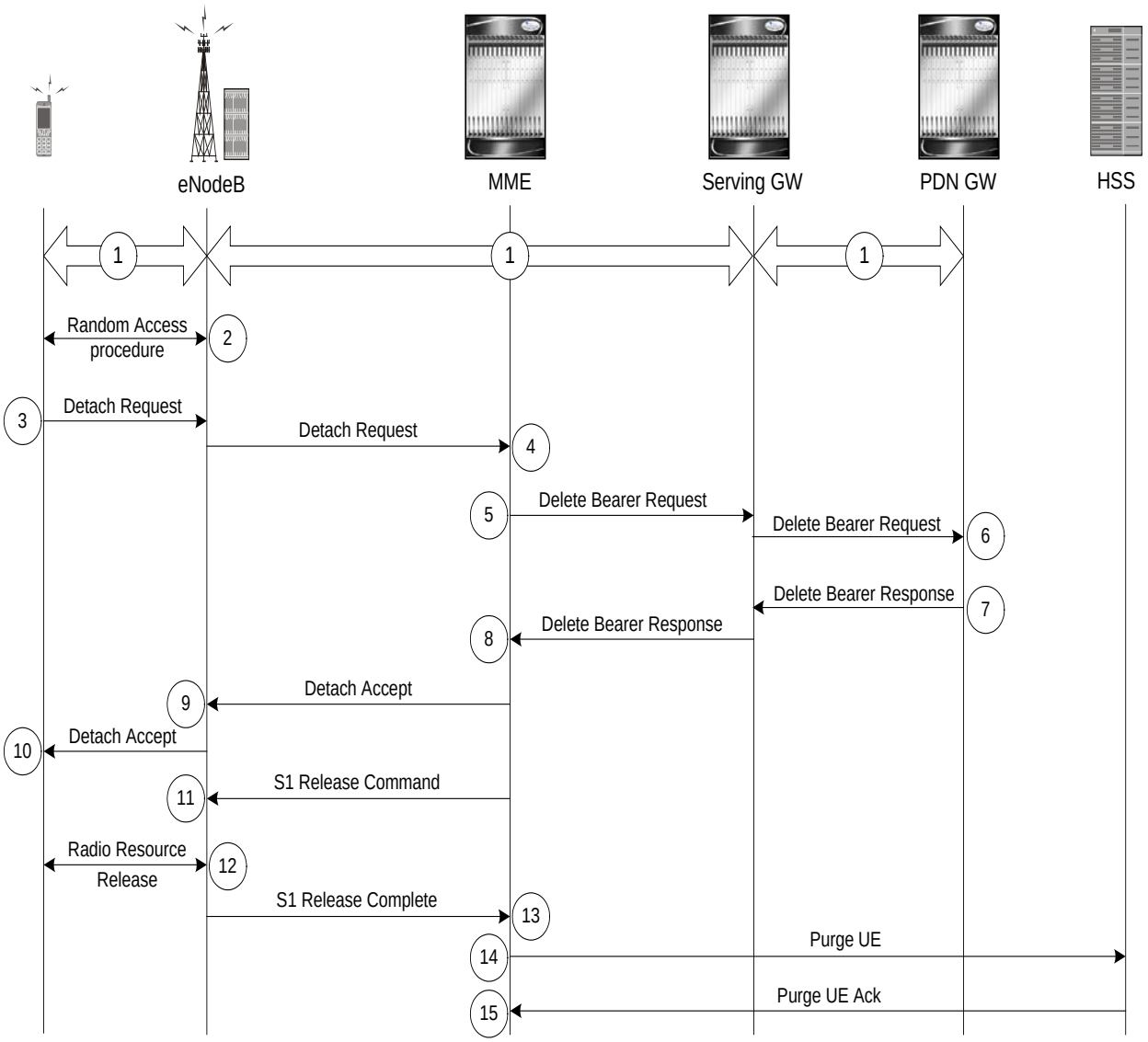
1. UE and eNodeB performs Random Access procedure.
2. After Random Access procedure completion, UE sends Attach Request with user identity to eNodeB.
3. The eNodeB forwards the Attach Request to MME
4. MME starts Authentication procedure with eNodeB and UE.
5. Once UE get authenticated MS sends Update Location Request to HSS with user IMSI derived during Authentication procedure.
6. Once user get validated at HSS with IMSI, HSS sends Insert Subscriber Data Request to MME providing subscriber profile and service subscription information to MME.
7. MME sends Create Bearer Request to Serving Gateway.
8. The S-GW forwards the request to P-GW.
9. P-GW reserves the EPS bearer and sends Create Bearer Response to the S-GW and establishes the EPS bearer with S-GW for this user.
10. Once S-GW receives the Create Bearer Response from P-GW it reserves the EPS bearer and sends Create Bearer Response to the MME and establishes the EPS bearer with MME for this user.

11. MME sends Attache Accept Response to eNodeB with new S-TMSI for this user.
12. The eNodeB sends Radio Bearer Establish Request as Attach Accept Response to UE to establish Radio bearer with UE.
13. UE sends Radio Bearer Establish Response as Attach Complete Response to eNodeB.
14. The eNodeB sends Attach Complete Response to MME with Initial EPS Bearer Context Setup procedure.
15. EPS Bearer established between UE and PDN through eNodeB, S-GW, and P-GW and subscriber session starts.

User-initiated Subscriber De-registration Setup Procedure

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

Figure 8. Subscriber De-registration Setup Message Flow



1. Subscriber session established between UE, eNodeB, S-GW, and P-GW.
2. *Optional*. If UE in idle or dormant mode it will initiate Random Access procedure.
3. UE initiates detach procedure and sends Detach Request to eNodeB.
4. eNodeB forwards the UE Detach Request to MME.
5. MME sends the Delete Session Request to S-GW for this subscriber.
6. S-GW forwards the Delete Session Request to P-GW for this subscriber.
7. P-GW deletes the EPS bearer for this subscriber and sends the Delete Session Response to S-GW.
8. S-GW deletes the UE context for this subscriber and sends the Delete Session Response to MME.
9. MME removes the subscriber context and sends the Detach Response to eNodeB.
10. MME sends S1 Release Command to eNodeB.
11. eNodeB forwards the Detach Accept to UE.
12. eNodeB starts Radio Release procedure with UE.
13. Once Radio Release procedure completed with UE, eNodeB sends S1 Release Complete response to MME and S1 link released for this UE.
14. Once S1 link released for subscriber, MME sends the Purge UE Request to HSS.
15. HSS clears all UE data and sends the Purge UE Ack to MME and subscriber de-registered.

Service Request Procedure

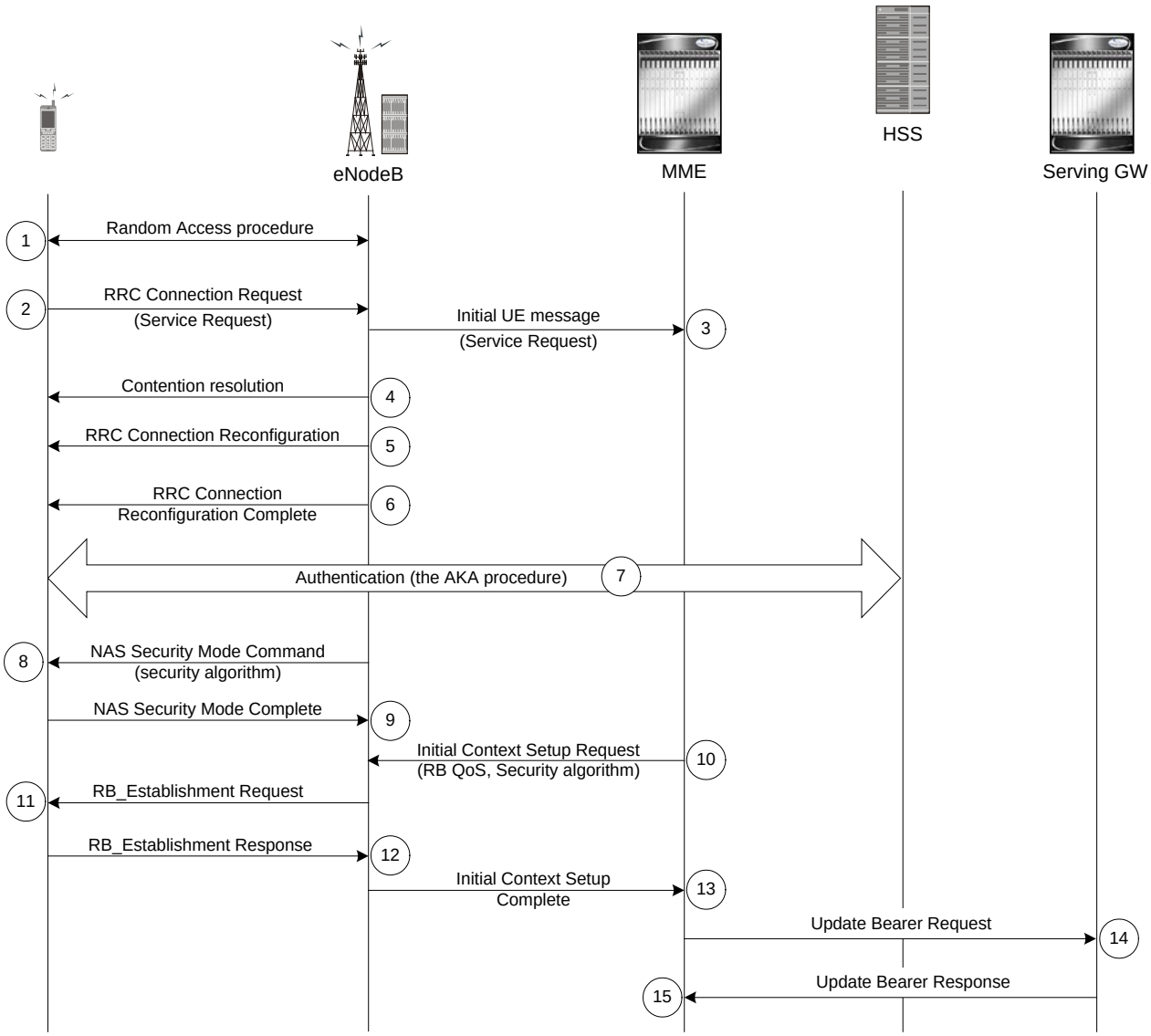
The Service Request procedure is used by the UE in the ECM Idle state to establish a secure connection to the MME as well as request resource reservation for active contexts. The MME allows configuration of the following service request procedures:

- Prohibition of services
- Enforce identity check

User-initiated Service Request Procedure

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

Figure 9. User-initiated Service Request Message Flow



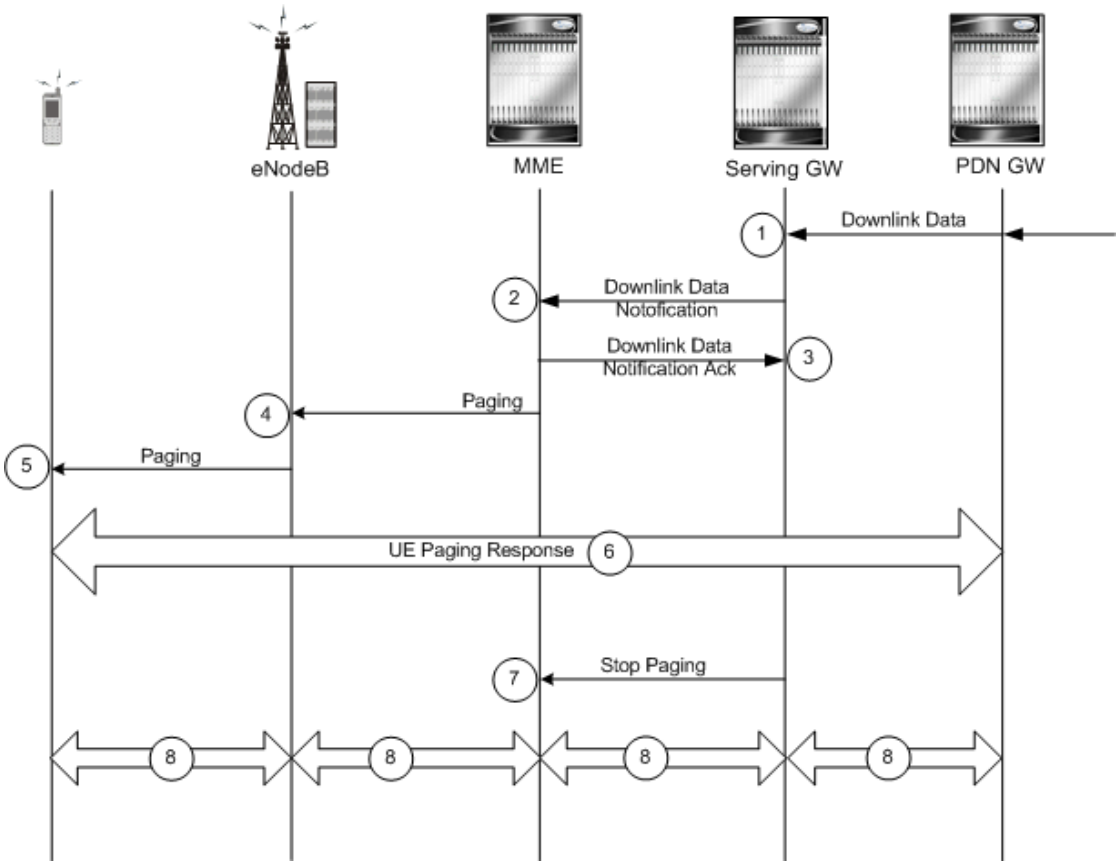
1. UE and eNodeB performs Random Access procedure.
2. UE sends service request (RRC Connection Request) to eNodeB.
3. eNodeB forwards Service request in Initial UE message to MME.
4. eNodeB preforms contention resolution with UE
5. eNodeB starts RRC connection reconfiguration.
6. eNodeB sends RRC Connection Request Complete and Reconfiguration Complete message to UE.
7. Authentication procedure starts between UE, MME and HSS.
8. eNodeB sends NAS Security Mode Command to UE with selected algorithm.
9. UE sends NAS Security Mode Complete Command to eNodeB.
10. MME sends initial Context Setup Request to eNodeB with radio bearer QoS, security algorithm etc.
11. eNodeB sends RB_Establishment Request to UE.
12. UE sends RB_Establishment Response to eNodeB and radio bearer established.
13. eNodeB sends initial Context Setup Request Response to MME.
14. MME sends Modify Bearer Request to S-GW.

15.S-GW modify the session for this UE and sends Modify Bearer Request response to MME.

Network-initiated Service Request Procedure

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

Figure 10. Network-initiated Service Request Message Flow



1. Downlink data received on S-GW from PDN for targeted UE.
2. S-GW sends Downlink Data notification to MME for a targeted UE.
3. MME sends Downlink Data notification acknowledgement to S-GW.
4. MME send Paging request to eNodeB for targeted UE.
5. eNodeB broadcasts Paging request in its coverage area for UE.
6. Once identified UE located S-GW and eNodeB starts messaging through UE Paging response.
7. S-GW sends Stop Paging message to MME.
8. Data downlink starts between identified UE and PDN.

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

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

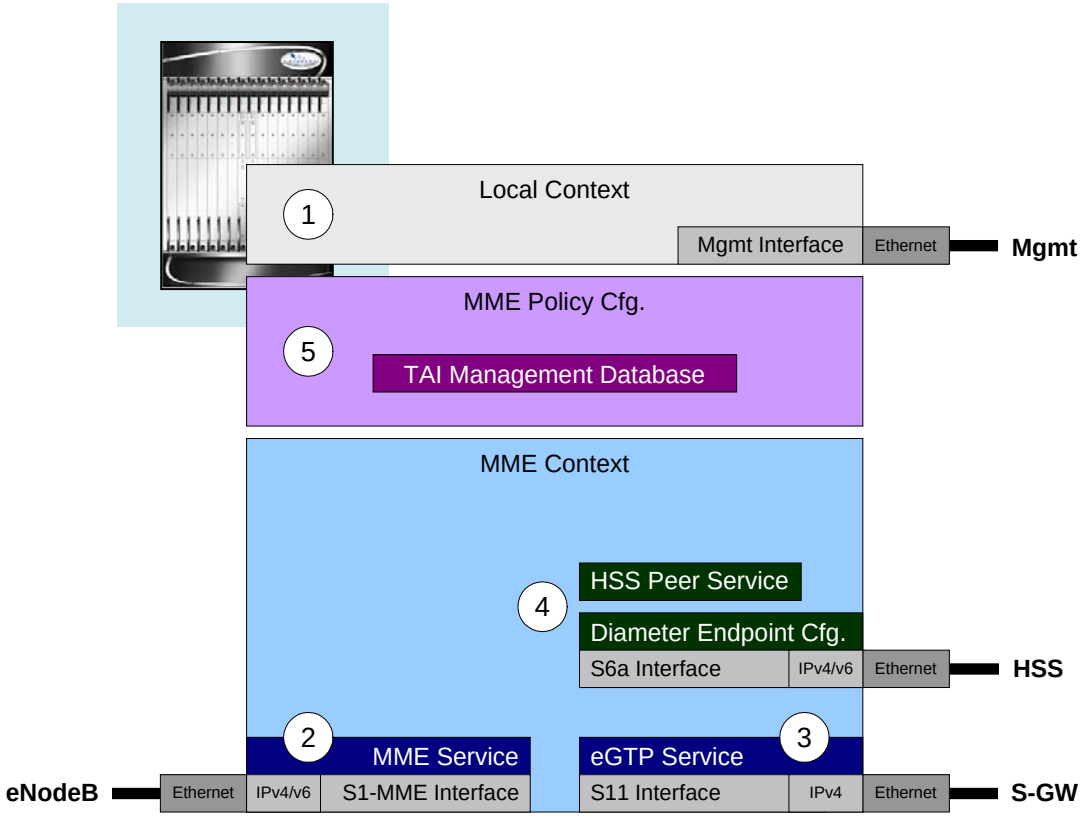
Table 2. Required Information for MME Policy Configuration

Required Information	Description

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.

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 by applying the example configuration in the Creating and Configuring the HSS Peer Service and Interface Association section.

Step 5 Configure MME policy information for static S-GW selection by applying the example configuration in the Configuring the MME Policy section.

Step 6 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
      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>
         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:

- The S1-MME IP address and the S6a interface can also be specified as IPv6 addresses using the **ipv6 address** command.
- 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 Association section.

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 Association

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

```
configure
   context <mme_context_name>
      diameter hss-endpoint <hss_cfg_name>
      exit
   diameter endpoint <hss_cfg_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
   port ethernet <slot_number/port_number>
      no shutdown
      bind interface <s6a_interface_name> <mme_context_name>
```

Configuring the MME Policy

Use the following example to configure the MME policy for static S-GW/P-GW discovery:

```
configure
   context <mme_context_name>
      mme-service <mme_svc_name>
         associate tai-mgmt-db <tai-mgmt-db_name>
         pgw-address <pgw_ip_address>
         exit
      exit
   mme-policy
      tai-mgmt-db <tai-mgmt-db_name>
         tai-mgmt-obj <tai-mgmt-obj_name>
```

```
tai mcc <num> mnc <num> tac <num>
sgw-address <ipv4_address> s5-s8-protocol <type> weight <num>
end
```

Notes:

- S5/S8 protocol types are: **pmip**, **gtp**, **both**.
- The **weight** command sets the priority of the S-GW for use during a weighted round-robin selection.

Configuring Optional Features on the MME

The configurations 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 Dynamic S-GW/P-GW Selection
- Configuring Gn/Gp Handover Capability
- Configuring Support for Dual Address Bearers

Configuring Dynamic S-GW/P-GW Selection

The configuration in this section replaces the MME policy configuration presented previously in this chapter. The MME policy configuration is used to set static S-GW/P-GW selection.

Use the following example to configure dynamic S-GW/P-GW 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 context <mme_context_name>
         dns sgw context <mme_context_name>
         end
```

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>
         gtpu bind address <Gn_intf_ip_address>
         exit
      mme-service <mme_svc_name>
         associate sgtpc-service <sgtp_svc_name>
         end
```

Configuring Support for 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
```

Chapter 3
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. Examples include APN and IP address pool configuration. Using these examples, enter the following commands to verify proper feature configuration:

show apn all

The output displays the complete configuration for the APN. In this example, an APN called apn1 is configured.

```
access point name (APN): apn1

authentication context: test

pdp type: ipv4

Selection Mode: subscribed

ip source violation: Checked drop limit: 10

accounting mode: gtpp No early PDUs: Disabled

max-primary-pdp-contexts: 1000000 total-pdp-contexts: 1000000

primary contexts: not available total contexts: not available

local ip: 0.0.0.0

primary dns: 0.0.0.0 secondary dns: 0.0.0.0

ppp keep alive period : 0 ppp mtu : 1500

absolute timeout : 0 idle timeout : 0

long duration timeout: 0 long duration action: Detection

ip header compression: vj

data compression: stac mppc deflate compression mode: normal

min compression size: 128

ip output access-group: ip input access-group:

ppp authentication:

allow noauthentication: Enabled imsi
```

```
 authentication:Disabled
```

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 SMC's CompactFlash or on an installed 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]**

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: If saving the file to an external network (non-local) device, the system disregards this keyword.
-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).

Keyword/Variable	Description
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 SMC's CompactFlash, 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 4
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 3. System Status and Performance Monitoring Commands

To do this:	Enter this command:
View Subscriber Information	
Display Session Resource Status	
View session resource status	**show resources session**
Display Subscriber Configuration Information	
View locally configured subscriber profile settings (must be in context where subscriber resides)	**show subscribers configuration username** *subscriber_name*
View remotely configured subscriber profile settings	**show subscribers aaa-configuration username** *subscriber_name*
View Subscribers Currently Accessing the System	
View a listing of subscribers currently accessing the system	**show subscribers all**
View information for all ggsn-only subscriber sessions	show subscribers ggsn-only all
View information for a specific subscriber	**show subscribers full username** *username*
View Subscriber Counters	
View counters for a specific subscriber	**show subscribers counters username** *subscriber_name*
View Recovered Session Information	
View session state information and session recovery status	**show subscriber debug-info { callid | msid | username }**
View Session Statistics and Information	
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 State PCF Statistics	

To do this:	Enter this command:
View session state PCF statistics	**show session progress pcf all**
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 Demux Manger status showing detailed statistics for IMSI Manager	show demux-mgr statistics imsimgr full
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**
View MME Master Manager logging facility statistics	**show logs facility mmgr**
Display Session Disconnect Reasons	
View session disconnect reasons with verbose output	**show session disconnect-reasons**
View MME Service Statistics	
Display a MME Service Status	
View all configured MME services session in details	show mme-service all verbose
Display MME Service Session Statistics	
View MME service session statistics in details	show mme-service session full verbose
View MME database statistics for all instances of DB in details	show mme-service db statistics verbose
View individual MME service statistics in concise mode	**show mme-service statistics mme-service** *mme_svc_name*
View MME-HSS Statistics	
View MME HSS session summary	**show mme-hss session summary all**
View MME HSS session statistics	**show mme-hss statistics all**
View MME HSS session statistics for a specific call id	**show mme-hss session full callid** *call_id*
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	

To do this:	Enter this command:
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 Command Line Reference for detailed information on using this command.

Chapter 5
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

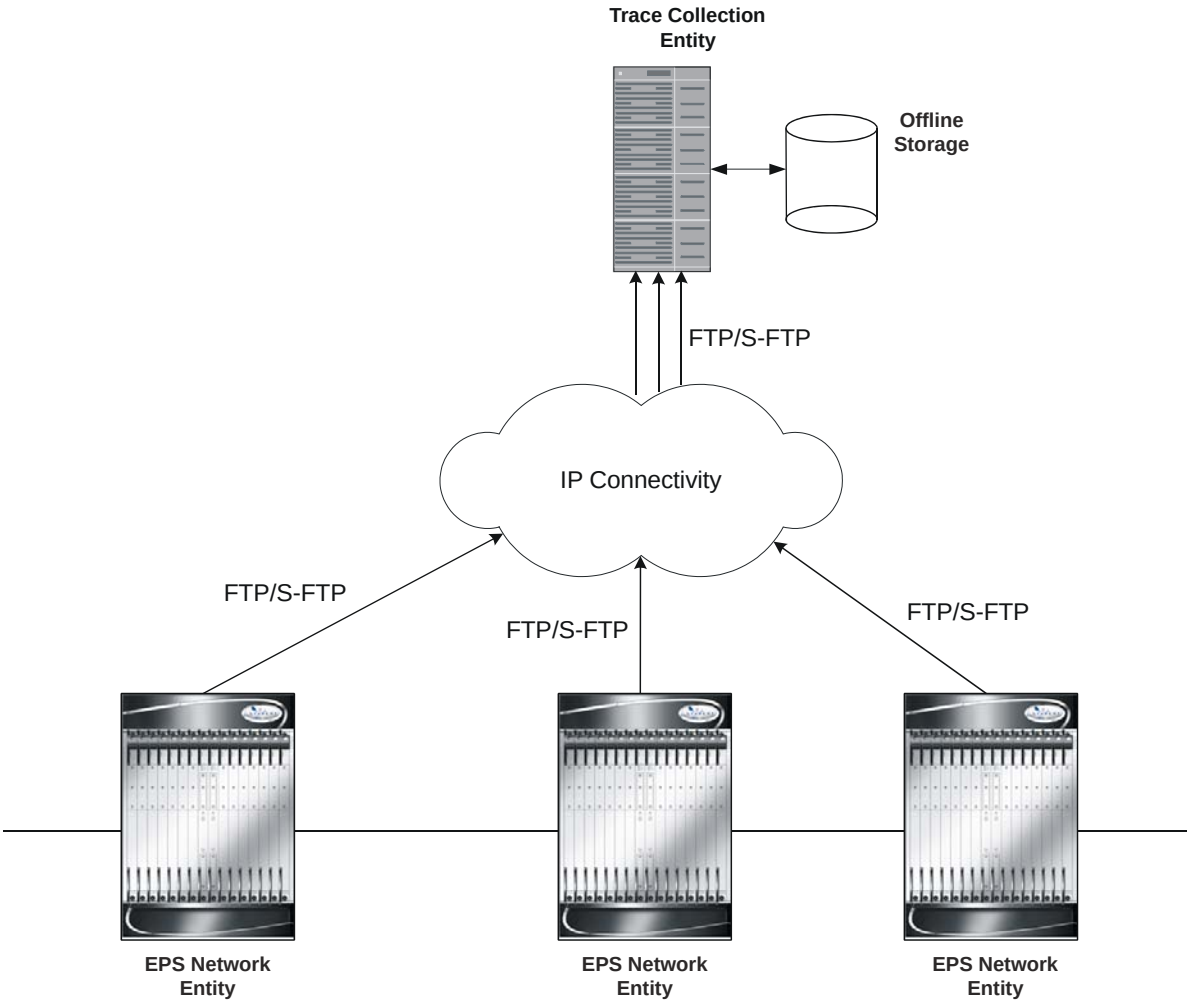
Important: Once the trace is provisioned it can be provisioned through the access cloud via various signaling interfaces.

The session level trace function consists of trace activation followed by triggers. The time between the two events is treated much like Lawful Intercept 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 11. 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/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).

Note: 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
S3	SGSN	Y	Y
S6a	HSS	Y	N

Interface Name	Remote Device	Trace Signaling (De)Activation RX	Trace Signaling (De)Activation TX
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 6
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
- Lawful Intercept 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.

Lawful Intercept Engineering Rules

The following engineering rules apply to Lawful Intercept on supported MME service:

- A maximum of 20000 Lawful Intercepts can be performed simultaneously.

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.