ERICSSON

# Features and Functions Management

## OPERATION DIRECTIONS

2/1543-AXB 250 05/8-V2 Uen AAV

# Contents


| | | |
|---|---|---|
| **1** | **Introduction** | **1** |
| 1.1 | Scope | 1 |
| 1.2 | Target Groups | 1 |
| **2** | **Prerequisites** | **1** |
| 2.1 | Planning | 2 |
| 2.2 | User | 2 |
| 2.3 | Licenses | 2 |
| **3** | **Managing Features and Node Functions** | **3** |
| 3.1 | Configuring Licensed Features | 3 |
| 3.2 | Configuring Node Functions | 3 |
| 3.3 | Checking the Consistency of the Configuration | 4 |
| 3.4 | Activating the Pending Configuration | 4 |
| 3.5 | Performing a Restart | 4 |
| 3.6 | Verifying the SGSN-MME Operation | 4 |
| 3.7 | Checkpointing and Setting the Default Configuration | 5 |
| **4** | **Licensed Features** | **5** |
| 4.1 | 3G Direct Tunnel (3GDT) | 5 |
| 4.2 | Access Aware Core Edge Support | 6 |
| 4.3 | Access Restriction | 7 |
| 4.4 | ANR Support | 8 |
| 4.5 | APN Resolve and Redirect | 9 |
| 4.6 | Authentication of Stationary Subscribers | 12 |
| 4.7 | Automated Acceptance Tests | 12 |
| 4.8 | Automatic Device Configuration Support | 13 |
| 4.9 | Automatic Device Detection for WCDMA | 14 |
| 4.10 | Cause Code Extensions in CDR | 15 |
| 4.11 | Cell Change Reporting | 18 |
| 4.12 | Combined Procedures, Gs Interface | 19 |
| 4.13 | Compression on the Gb Interface | 21 |
| 4.14 | Configurable and Adaptive Paging | 22 |
| 4.15 | Connection Suspend and Resume | 23 |

| | | |
|---|---|---|
| 4.16 | Control-Plane-Based Positioning | 24 |
| 4.17 | Conversational QoS | 25 |
| 4.18 | Coverage Extension Support | 26 |
| 4.19 | CS Fallback to 1xRTT | 27 |
| 4.20 | CS Fallback to WCDMA and GSM | 28 |
| 4.21 | Data over NAS | 29 |
| 4.22 | DoNAS with ROHC | 30 |
| 4.23 | DoNAS, PDN Type Non-IP | 30 |
| 4.24 | Dedicated Core Network | 32 |
| 4.25 | Detach of Inactive Subscribers GSM | 33 |
| 4.26 | Detach of Inactive Subscribers Dual Access | 33 |
| 4.27 | Detach of Inactive Subscribers WCDMA | 34 |
| 4.28 | Dual Access for GSM and WCDMA | 35 |
| 4.29 | Dual Access for WCDMA and LTE | 36 |
| 4.30 | Dual Transfer Mode | 36 |
| 4.31 | EDGE Support | 37 |
| 4.32 | Enhanced Uplink Support | 38 |
| 4.33 | Enhanced Uplink Support, Expansion 1 | 38 |
| 4.34 | Enhanced Uplink Support, Expansion 2 | 39 |
| 4.35 | Event-Based Monitoring | 40 |
| 4.36 | Extended Idle Mode Discontinuous Reception (eDRX) | 40 |
| 4.37 | Gateway Blacklisting | 41 |
| 4.38 | Gateway Restoration Procedures | 42 |
| 4.39 | Gb over IP | 43 |
| 4.40 | Geographically Redundant Pool | 44 |
| 4.41 | GTP-C Network Load Control | 44 |
| 4.42 | GTP ULI Support for Gn-SGSN | 45 |
| 4.43 | HSDPA Support Expansion 1 | 46 |
| 4.44 | HSDPA Support Expansion 2 | 46 |
| 4.45 | HSDPA Support Expansion 3 | 47 |
| 4.46 | HSDPA Support Expansion 4 | 48 |
| 4.47 | HSDPA Support Expansion 5 | 49 |
| 4.48 | IMEI Check | 50 |
| 4.49 | IMS-Based Telephony - MMTel | 50 |
| 4.50 | Integrated Traffic Capturing | 51 |
| 4.51 | Low Complexity UE Support | 52 |

| | | |
|---|---|---|
| 4.52 | IPsec for Secure Network Traffic | 53 |
| 4.53 | Lawful Intercept | 53 |
| 4.54 | Lawful Intercept, Exp 1 | 54 |
| 4.55 | Lawful Intercept, HI2, and XML-Based X1 | 54 |
| 4.56 | Location Based IP Address Allocation | 55 |
| 4.57 | LTE Broadcast | 56 |
| 4.58 | MBMS: Broadcast Services | 56 |
| 4.59 | Minimization of Drive Tests | 57 |
| 4.60 | Misconfigured MT Identification | 58 |
| 4.61 | MME Pool | 58 |
| 4.62 | MME Support of HeNB | 59 |
| 4.63 | MME Support for Closed Subscriber Group | 60 |
| 4.64 | Mobility-Based Policy | 61 |
| 4.65 | Monitoring Enhancements | 62 |
| 4.66 | MS-Activated Secondary PDP Context | 62 |
| 4.67 | Multi-Operator Core Network | 63 |
| 4.68 | Multiple PLMN Support | 65 |
| 4.69 | M2M/IoT: Direct Short Data Service | 66 |
| 4.70 | Near Real-Time Provision of CDRs | 66 |
| 4.71 | Network-Initiated Dedicated Bearers | 67 |
| 4.72 | Network-Requested Secondary PDP Context | 67 |
| 4.73 | NR Access Control | 68 |
| 4.74 | Packet Flow Control per PFC | 69 |
| 4.75 | Packet Handover | 70 |
| 4.76 | Paging Suppression for Fixed Wireless Access | 72 |
| 4.77 | Presence Reporting Area Support | 73 |
| 4.78 | Prioritization of Payload Users after Restart | 74 |
| 4.79 | Public Warning System | 75 |
| 4.80 | QoS Based on IMSI Series | 76 |
| 4.81 | QoS Based on RNC | 77 |
| 4.82 | RAN Information Management | 77 |
| 4.83 | Real-Time Charging Control Using CAMEL | 78 |
| 4.84 | Roaming Restrictions | 79 |
| 4.85 | S3/S4 Architecture Support | 81 |
| 4.86 | Selective Equivalent PLMN | 82 |
| 4.87 | Selective Service Request Handling | 83 |

| | | |
|---|---|---|
| 4.88 | SGSN Pool for GSM and WCDMA | 83 |
| 4.89 | SGSN-MME Support for MSC in Pool | 84 |
| 4.90 | Single Radio Voice Call Continuity | 85 |
| 4.91 | SMS over SGs | 87 |
| 4.92 | SS7 over IP (SIGTRAN) | 87 |
| 4.93 | Streaming QoS | 88 |
| 4.94 | Subscription-Based Restrictions | 89 |
| 4.95 | Support for Non-Standardized UE | 92 |
| 4.96 | Triple Access for GSM, WCDMA, and LTE | 92 |
| 4.97 | UE Dual Connectivity Support | 93 |
| 4.98 | UE Power-Saving Mode | 94 |
| 4.99 | UE Signaling Control | 95 |
| 4.100 | UE Tracer | 95 |
| 4.101 | Wi-Fi Integration | 96 |
| **5** | **Operation and Maintenance** | **96** |
| 5.1 | Parameters | 96 |
| **6** | **Compliance** | **97** |
| **Reference List** | | **99** |

# 1 Introduction

This document describes management and configuration procedures for license-controlled features and node functions on the SGSN-MME.

## 1.1 Scope

This document covers the following:

- Prerequisites for the configuration procedures
- Management and configuration of licensed features
- Management and configuration of node functions
- Supplementary configuration procedures, where applicable
- Configuration processes for checking the consistency of the configuration and for checkpointing and activating the configuration

Capacity licenses do not need configuration. For more information, see Installing Node-Based Licenses. If network-based licenses are used, see Activation of NeLS Client Licenses.

Features management and configuration are transacted through CLI commands. For more information, see Operation and Maintenance Description.

For information about parameters configured in this document, see SGSN-MME Licensed Capacities and Features.

Node functions are described together with the function for which they can modify the behavior.

## 1.2 Target Groups

This document is intended for personnel planning configuration changes and management of the SGSN-MME.

# 2 Prerequisites

This section outlines the prerequisites for the management of licensed features.

## 2.1 Planning

The planning phase of the management involves answering the following questions:

— What software licenses are required to configure and enable licensed features? For more information, see Installing Node-Based Licenses. If network-based licenses are used, see Activation of NeLS Client Licenses. Read the configuration steps and perform the prerequisites before enabling a feature.

— Is a restart required for activating the feature, and if so, at what restart level? To minimize disruption of network traffic, configure all the features planned for configuration before restarting the SGSN-MME. For more information, see Section 3.5 on page 4.

— What is an appropriate time for the activation or deactivation of the features, if a restart of the SGSN-MME is required? This is to minimize disruption of network traffic. For more information, see Section 3.5 on page 4.

## 2.2 User

To follow the CLI instructions in this document, the user must be logged on as an O&M user with configuration rights. For more information, see Operator Access Handling.

The person that performs management and configuration of features and functions needs to have an advanced understanding about the operation of SGSN-MME.

## 2.3 Licenses

A prerequisite to enable and manage licensed features is that the license-key file is loaded and the licenses are set to `granted`. For more information, see Installing Node-Based Licenses. If network-based licenses are used, see Activation of NeLS Client Licenses.

If a feature has not been purchased and no license key is included in the loaded license-key file, the following applies:

— The license is invalid for this feature.

— The CLI commands related to the feature are disabled.

For more information on available operations for licensed features, see License Management (CLI).

# 3 Managing Features and Node Functions

This section describes how to enable and configure licensed features and node functions.

To display the parameters related to node functions and optional features, use the get_config_area -can FeaturesAndFunctions CLI command.

## 3.1 Configuring Licensed Features

Configure all licensed features that are considered for activation or deactivation, before activating the pending configuration. For detailed prerequisites, configuration steps, and feature parameters for particular features, see Section 4 on page 5.

**Instructions**

Enable and configure a licensed feature as follows:

1. Verify that prerequisites are fulfilled. For information on prerequisites for management of licensed features, see Section 2 on page 1.
2. Perform any required or additional configuration.
3. Enable the feature by using the modify_feature_state CLI command.

A feature is active only after the pending configurations are activated, and if necessary, a restart is performed. For instructions on performing a restart, see Section 3.5 on page 4.

## 3.2 Configuring Node Functions

A node function is used to configure if a basic feature is enabled, and is sometimes also used for configuring the behavior of a licensed controlled feature.

**Instructions**

Enable or disable the node function by using the modify_node_function CLI command.

A node function is active only after the pending configurations are activated, and if necessary, a restart is performed. For instructions on performing a restart, see Section 3.5 on page 4.

## 3.3 Checking the Consistency of the Configuration

A consistency check must be performed before activating a pending configuration. The check verifies that the active configuration combined with the changes in the pending configuration is correct, and that it does not contain conflicting or illegal values. It also warns for changes that cause traffic disturbances or violate recommendations.

**Instructions**

Use the check_config CLI command to check the consistency of the configuration.

## 3.4 Activating the Pending Configuration

The modifications to the configured features take effect when the pending configuration is activated. A pending configuration cannot be activated unless a successful consistency check has been performed first, see Section 3.3 on page 3.

**Instructions**

Use the activate_config_pending CLI command to activate the pending configuration.

## 3.5 Performing a Restart

To find out if a restart is required, and at what level. For feature impact see Section 4 on page 5 and for node function impact see Parameter Description. If a feature or a node function is activated at runtime, no restart is required.

If a restart is required, proceed as follows:

**Instructions**

— To initiate a small restart, use the start_small_restart CLI command.

— To initiate a large restart, use the start_large_restart CLI command.

## 3.6 Verifying the SGSN-MME Operation

Verify the SGSN-MME operation by performing a health check on the SGSN-MME.

**Instructions**

Perform a health check on the SGSN-MME to verify the operation. For more information, see Health Check.

## 3.7 Checkpointing and Setting the Default Configuration

Perform a checkpoint to ensure that the current configuration is stored persistently. Set the checkpointed Software Configuration (SC) as the default SC to ensure that it is used in an event of a fallback. This is a safety precaution.

**Instructions**

1. Checkpoint the configuration and set the checkpointed SC as the default SC by using the checkpoint CLI command:

   ```
   <nodeid> <userName>@eqm01s0fp2 ANCB ~ # gsh checkpoint { -cpn
   <uniqueName> } –default_sc true
   ```

   **Note:** Using the `default_sc` parameter with the **`SetAsDefaultSc`** value set to **`true`**, sets the checkpointed SC as the default SC.

   For more information, see the SetAsDefaultSc parameter description.

# 4 Licensed Features

This section describes licensed features, prerequisites, and supplementary configuration, if applicable. For sections on configuring a feature and performing a restart, see Section 3.1 on page 3 and Section 3.5 on page 4 respectively.

## 4.1 3G Direct Tunnel (3GDT)

**Parameter** `3gdt`

**Activation** Runtime

**Valid for Access Type** WCDMA

**Key ID** FAT 102 3381/2040

### 4.1.1 Description

The 3G Direct Tunnel (3GDT) feature reduces the payload traffic through the SGSN-MME by transferring the payload traffic outside of the SGSN-MME. 3GDT increases the control signaling in the network. For more information, see 3G Direct Tunnel.

**Note:** For the SGSN-MME using the Gn interface, 3GDT is supported only for home subscribers.

### 4.1.2 Configuration

To enable the feature, fulfill the prerequisites in Table 1:

| For SGSN-MME Using the Gn or S4 Interface | Prerequisites |
|---|---|
| For SGSN-MME using the Gn interface | • The RNC and GGSN must be 3GDT compliant.<br>• The HLR configuration must be 3GDT compliant.<br>• The 3GDT prefix must be supported in DNS query. |
| For SGSN-MME using the S4 interface | • The RNC must be 3GDT compliant.<br>• The SGW must support the S12 interface. |

For information on prerequisites for management of licensed features, see Section 2 on page 1.

#### Instructions

For instructions on how to configure the feature, see 3G Direct Tunnel Configuration.

## 4.2 Access Aware Core Edge Support

**Parameter** `aace_support`

**Activation** Runtime

**Valid for Access Type**
GSM, WCDMA, LTE

**Key ID** FAT 102 3381/2022

### 4.2.1 Description

The Access Aware Core Edge feature allows the SGSN-MME to forward access-related information about a subscriber to the GGSN. This enables differentiation of services and charging schemes. For more information, see GSM and WCDMA Session Management and LTE Session Management respectively.

**Note:** Access Aware Core Edge feature is partly under restriction when run simultaneously as the Multiple PLMN feature. For example, the SGSN does not indicate a change of PLMN at an intra-SGSN Routing Area Update (RAU).

### 4.2.2 Configuration

To enable the feature, the following requirement must be fulfilled:

— Support in the GGSN, the SGW, or the PGW and the billing system.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

**Instructions**

Enable the Access Aware Core Edge Support feature, by setting the feature state to `ACTIVATED` for the `aace_support` parameter, using the modify_feature_state CLI command.

For more information on how to activate the configuration changes, see Section 3 on page 2.

## 4.3 Access Restriction

**Parameter** `access_restriction`

**Activation** Runtime

**Valid for Access Type** GSM, WCDMA, LTE

**Key ID** FAT 102 3381/2028

### 4.3.1 Description

The Access Restriction feature allows restricting the access to GSM or WCDMA Systems on a per-subscriber basis by settings in the HLR/HSS. For more information, see GSM Mobility Management or WCDMA Mobility Management.

The feature also allows restricting the access to LTE or NB-IoT Systems on a per-subscriber basis by settings in the HSS and on a per IMSI number series basis by settings in the MME. For more information, see LTE Mobility Management.

### 4.3.2 Configuration

To enable the feature, the following requirements must be fulfilled:

— Support in the HLR/HSS for restricting access to GSM or WCDMA Systems.

— Support in the HSS for restricting access to LTE Systems.

— The Access Restriction SW Feature License certificate.

— Optionally, if terminals capable of both CS and PS Attach are used, support in the Mobile services Switching Center (MSC) for restricting access to GSM or WCDMA Systems is also required.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

**Instructions**

Enable the Access Restriction feature, by setting the feature state to `ACTIVATED` for the `access_restriction` parameter, using the modify_feature_state CLI command.

When the feature is enabled in SGSN-MME (WG), it is optional to configure the cause code that is sent when attach requests are rejected, because of Access Restriction. Configure the `SGSNAccessRestrictionSamePlmn` parameter, using the modify_sgsn CLI command.

For more information on how to activate the configuration changes, see Section 3 on page 2.

## 4.4 ANR Support

**Parameter** `anr_support`

**Activation** Runtime

**Valid for Access Type** LTE

**Key ID** FAT 102 3381/2059

### 4.4.1 Description

The ANR Support feature is part of a self-configuration process in the network where the X2 interface is automatically set up between eNodeBs. During this process, the role of the MME is to relay messages between eNodeBs so that Stream Control Transmission Protocol (SCTP) connectivity can be dynamically set up between them. For more information, see SGSN-MME Technical Product Description Overview.

### 4.4.2 Configuration

Enable the ANR Support feature, by setting the feature state to `ACTIVATED` for the `anr_support` parameter, using the modify_feature_state CLI command.

For more information on how to activate the configuration changes, see Section 3 on page 2.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

## 4.5 APN Resolve and Redirect

The APN Resolve and Redirect feature includes the following functions, which are controlled by the same license, but can be used separately or in combination.

- APN Conversion
- APN Redirection
- APN Resolution Functional Extension
- APN Local Breakout Control
- APN-OI Replacement

### 4.5.1 APN Conversion

**Parameter** `apn_conversion_wg`

`apn_conversion_lte`

**Activation** Runtime

**Valid for Access Type** GSM, WCDMA, LTE

**Key ID** FAT 102 3381/2048

#### 4.5.1.1 Description

APN Conversion converts an APN requested by the UE according to the APN conversion criteria.

For more information, see APN Resolve and Redirect for LTE Access and APN Resolve and Redirect for GSM and WCDMA Access.

#### 4.5.1.2 Configuration

For instructions on how to configure APN Conversion, see Configuring APN Resolve and Redirect.

### 4.5.2 APN Redirection

**Parameter** `apn_redirection`

**Activation** Runtime

**Valid for Access Type**

GSM, WCDMA, LTE

**Key ID** FAT 102 3381/2048

#### 4.5.2.1 Description

The APN Redirection functionality replaces an invalid (for example, incorrectly formatted or misspelled) APN requested by the MS, or an APN converted by the SGSN-MME with either a subscribed APN or the SGSN-MME default APN.

For more information, see APN Resolve and Redirect for GSM and WCDMA Access and APN Resolve and Redirect for LTE Access.

#### 4.5.2.2 Configuration

For instructions on how to configure APN Conversion and APN Redirection, see Configuring APN Resolve and Redirect.

### 4.5.3 APN Resolution Functional Extension

**Parameter** `apn_resolution_extension`

**Activation** Runtime

**Valid for Access Type**

GSM, WCDMA, LTE

**Key ID** FAT 102 3381/2047

#### 4.5.3.1 Description

The APN Resolution Functional Extension functionality provides the connection from an MS to a specified GGSN or PGW. The GGSN or PGW selection is performed by adding an extension to the APN before a query is sent toward the DNS server.

**Note:** The APN Resolution Functional Extension function is applicable only for the PDP context activation procedure.

The APN Resolution Functional Extension function is applicable only for home subscribers.

For more information, see APN Resolve and Redirect for GSM and WCDMA Access and APN Resolve and Redirect for LTE Access.

#### 4.5.3.2 Configuration

For instructions on how to configure APN Resolution Functional Extension, see Configuring APN Resolve and Redirect.

### 4.5.4 APN Local Breakout Control

**Parameter** `apn_local_breakout_control`

**Activation** Runtime

**Valid for Access Type**
GSM, WCDMA, LTE

**Key ID** FAT 102 3381/2082

#### 4.5.4.1 Description

APN Local Breakout Control restricts the local breakout for roaming subscribers per IMSI number series to only specified APNs, when the subscription data allows it. For more information, see APN Resolve and Redirect for GSM and WCDMA Access and APN Resolve and Redirect for LTE Access.

#### 4.5.4.2 Configuration

For instructions on how to configure APN Local Breakout Control, see Configuring APN Resolve and Redirect.

### 4.5.5 APN-OI Replacement

**Parameter** `apn_oi_replacement`

**Activation** Runtime

**Valid for Access Type**
GSM, WCDMA, LTE

**Key ID** FAT 102 3381/2086

#### 4.5.5.1 Description

The APN Operator Identifier (APN-OI) Replacement functionality enables the SGSN-MME to redirect a UE to a specific PGW by replacing the APN-OI in the DNS query. For more information, see APN Resolve and Redirect for LTE Access and APN Resolve and Redirect for GSM and WCDMA Access.

#### 4.5.5.2 Configuration

For more information on how to configure APN-OI Replacement, see Configuring APN Resolve and Redirect.

## 4.6 Authentication of Stationary Subscribers

**Parameter** `authentication_stationary_subscriber`

**Activation** Runtime

**Valid for Access Type** GSM

**Key ID** FAT 102 3381/2011

### 4.6.1 Description

The Authentication of Stationary Subscribers feature allows periodic authentication of stationary subscribers. This increases both the protection from cloning and the level of confidentiality of the stationary subscribers user data. A stationary subscriber is a subscriber that stays within the same RA.

For more information, see Security.

### 4.6.2 Configuration

To enable and configure the feature, do as follows:

1. Define the time between each repetition of the authentication procedure for stationary subscribers by configuring the `GbPeriodicAuthenticationTimer` parameter, using the modify_gb CLI command.

2. Enable the Authentication of Stationary Subscribers feature, by setting the feature state to `ACTIVATED` for the `authentication_stationary_subscribers` parameter, using the modify_feature_state CLI command.

For more information on how to activate the configuration changes, see Section 3 on page 2.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

## 4.7 Automated Acceptance Tests

**Parameter** `automated_acceptance_tests`

**Activation** Runtime

**Valid for Access Type**

LTE, WCDMA

**Key ID** FAT 102 3381/2092

### 4.7.1 Description

The Automated Acceptance Tests (AAT) is an external graphic tool built on Testing and Test Control Notation (TTCN). The AAT is used to replace part of the manual acceptance testing. It is sold as a separate product.

### 4.7.2 Configuration

The `automated_acceptance_tests` parameter controls SGSN-MME support for AAT and must be configured, using the modify_feature_state CLI command.

## 4.8 Automatic Device Configuration Support

**Parameter** `adc`

**Activation** Large Restart

**Valid for Access Type** GSM

**Key ID** FAT 102 3381/2013

### 4.8.1 Description

The Automatic Device Configuration Support feature fully automates configuration and activation of services by letting the SGSN-MME initiate a device configuration procedure for new or unconfigured MSs using GPRS for GSM. The procedure is initiated when a new combination of International Mobile Subscriber Identity (IMSI) and IMEI Software Version (IMEISV) for Home Public Land Mobile Network (HPLMN) subscribers is detected. The Device Configuration Register (DCR) and the Device Management System (DMS) are new nodes required for running Automatic Device Configuration Support. Other nodes in the network do not require to be updated.

**Note:**

- If the `GbIdentityImeiEnabled` parameter is not enabled before activating ADC, the CDR content is affected.
- Both activation and deactivation of Automatic Device Configuration Support require a large restart to come into effect. With the large restart, a timer is set. This timer assures that Automatic Device Configuration (ADC) is inactive and it does not add to the load on the SGSN-MME for 60 minutes. As a result, the ADC does not log any MSs to the file that connect to the SGSN-MME during this period.
- Only MSs that connect by attach or Inter SGSN Routing Area Update (ISRAU) procedures to the SGSN-MME after activation are registered in the ADC file. This means that MSs already connected to the SGSN-MME are not logged in the file until they connect again.

### 4.8.2 Configuration

To enable the feature, the following requirement must be fulfilled:

— DCR and DMS are required for running ADC. Other nodes in the network do not require to be updated.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

**Instructions**

1. Check the state of the `GbIdentityImeiEnabled` parameter, by using the get_gb CLI command.
2. If the `GbIdentityImeiEnabled` parameter is disabled, enable it by using the modify_gb CLI command.
3. Enable the Automatic Device Configuration Support feature, by setting the feature state to `ACTIVATED` for the `adc` parameter, using the modify_feature_state CLI command.

For more information on how to activate the configuration changes, see Section 3 on page 2.

To disable the feature, the following configuration is optional:

1. Disable the `GbIdentityImeiEnabled` parameter, by using the modify_gb CLI command.

   **Note:** Several features can be affected if the `GbIdentityImeiEnabled` parameter is modified. If the parameter is only used by the ADC feature, it can be disabled.

## 4.9 Automatic Device Detection for WCDMA

**Parameter** `add`

**Activation** Runtime

**Valid for Access Type** WCDMA

**Key ID** FAT 102 3381/2049

### 4.9.1 Description

The ADD feature fully automates configuration and activation of services by letting the SGSN-MME initiate a device configuration procedure for new or unconfigured MSs using GPRS for WCDMA Systems. ADD includes the IMEISV in the `Update GPRS Location Request` message to the HLR/HSS each time there is a new or changed IMEISV in a Mobility Management (MM) context for Home Public Land Mobile Network (HPLMN) subscribers. ADD is according to 3GPP release 6.

### 4.9.2 Configuration

To enable the feature, the following requirement must be fulfilled:

— HLR/HSS, DCR, and DMS are required for running ADD.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

#### Instructions

Enable the Automatic Device Detection for WCDMA feature, by setting the feature state to `ACTIVATED` for the `add` parameter, using the modify_feature_state CLI command.

For more information on how to activate the configuration changes, see Section 3 on page 2.

## 4.10 Cause Code Extensions in CDR

The Cause Code Extensions in CDR feature grants licenses for the two features described in the following section. Only one of these features can be enabled at a time.

### 4.10.1 RAN Cause Codes in CDR

**Parameter** `ran_cause_codes_in_scdr`

**Activation** Runtime

**Valid for Access Type** GSM, WCDMA, LTE

**Key ID** FAT 102 3381/2058

#### 4.10.1.1 Description

The RAN Cause Codes in CDR feature are available for both the SGSN and the MME. This section contains descriptions of this feature for the SGSN and the MME separately.

#### SGSN

If the RAN Cause Codes in CDR feature is activated and the `ChRanCauseCodesInCdr` parameter is set to `true`, the Gn-SGSN and S4-SGSN add extended diagnostics information (maximum of three BSSGP or RANAP cause codes, if available) into the `recordExtensions` field of a CDR when the record is closed for each activated PDP context.

The recordExtensions field of a CDR includes:

— BSSGP or RANAP cause codes

  These cause codes are defined in SoC with 3GPP TS 48.018 for GSM and SoC with 3GPP TS 25.413 for WCDMA Systems.

— BSSGP or RANAP message type

  The message type is the BSSGP or RANAP message from which the cause code is extracted.

— BSSGP or RANAP message source

  The value 0 indicates that the message is sent from the SGSN to the BSC or RNC. The value 1 indicates that the message is sent from the BSC or RNC to the SGSN.

— Time stamp

**S4-SGSN and MME**

If the RAN Cause Codes in CDR feature is activated and the RanNasCauseCodesInPrivateExtension parameter is set to true, the S4-SGSN with access type WCDMA and MME add RAN/NAS cause codes to the Private Extension IE in Delete Session Request and Delete Bearer Command messages. These messages are then forwarded to the SGW over the S4 or S11 interface respectively. If there are no RAN/NAS cause codes, the Private Extension IE is not included. For the Delete Session Request message, the RAN/NAS cause codes are added for each EPS bearer of a specific PDN connection.

**MME**

If the RAN Cause Codes in CDR feature is activated and the RanNasCauseCodesInStandardIe parameter is set to true, the MME adds a RAN/NAS cause code to the RAN/NAS Release Cause IE in the following messages:

— Delete Session Request

— Delete Bearer Command

— Delete Bearer Response

— Create Bearer Response

— Update Bearer Response

For more information, see LTE Session Management.

**Note:** The licensed feature S-CDR Cause Code Extension can be enabled when one of the following conditions is fulfilled:

- The RAN Cause Codes in CDR feature is disabled.
- The RAN Cause Codes in CDR feature is enabled and the `ChRanCauseCodesInCdr` parameter is set to `false`

#### 4.10.1.2 Configuration

Enable the RAN Cause Codes in CDR feature, by setting the feature state to `ACTIVATED` for the `ran_cause_codes_in_scdr` parameter, using the modify_feature_state CLI command.

To include or exclude the extended diagnostics information in CDR, set the `ChRanCauseCodesInCdr` parameter, using the modify_charging CLI command.

To include or exclude a RAN/NAS cause code in the `Private Extension` IE, set the `RanNasCauseCodesInPrivateExtension` parameter, using the modify_gtp_v2 CLI command.

To include or exclude a RAN/NAS cause code in the `RAN/NAS Release Cause` IE, set the `RanNasCauseCodesInStandardIe` parameter, using the modify_gtp_v2 CLI command.

For more information on how to activate the configuration changes, see Section 3 on page 2.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

### 4.10.2 S-CDR Cause Code Extension

**Parameter** `s_cdr_cause_code_ext`

**Activation** Runtime

**Valid for Access Type** GSM, WCDMA

**Key ID** FAT 102 3381/2046

#### 4.10.2.1 Description

The S-CDR Cause Code Extension feature adds cause codes received from the BSC and RNC to the S-CDR, if a PDP context is deactivated and the CDR is closed.

**Note:** The licensed feature S-CDR Cause Code Extension can be enabled when one of the following conditions is fulfilled:

— The RAN Cause Codes in CDR feature is disabled.

— The RAN Cause Codes in CDR feature is enabled and the `ChRanCauseCodesInCdr` parameter is set to `false`

#### 4.10.2.2 Configuration

Enable the S-CDR Cause Code Extension feature, by setting the feature state to `ACTIVATED` for the `s_cdr_cause_code_ext` parameter, using the modify_feature_state CLI command.

For more information on how to activate the configuration changes, see Section 3 on page 2.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

## 4.11 Cell Change Reporting

**Parameter** `cell_change_reporting`

**Activation** Runtime

**Valid for Access Type** LTE

**Key ID** FAT 102 3381/2074

### 4.11.1 Description

The Cell Change Reporting feature enables the MME to subscribe to cell change events in the eNodeB for all UE devices in ECM-CONNECTED state. Location information for each cell change event is sent to the MME and then forwarded to the SGW.

For more information, see LTE Mobility Management.

**Note:** The Cell Change Reporting, the Mobility-Based Policy, and Presence Reporting Area Support features are mutually exclusive.

For information about the Mobility-Based Policy feature, see Section 4.64 on page 61.

For information about the Presence Reporting Area Support, see Section 4.77 on page 73.

### 4.11.2 Configuration

Enable the Cell Change Reporting feature, by setting the feature state to `ACTIVATED` for the `cell_change_reporting` parameter, using the modify_feature_state CLI command.

For more information on how to activate the configuration changes, see Section 3 on page 2.

For more information about related CLI commands, see GTPv2 (CLI).

For information on prerequisites for management of licensed features, see Section 2 on page 1.

## 4.12 Combined Procedures, Gs Interface

**Parameter** `combined_procedures_gs_if`

**Activation** Runtime for the `combined_procedures_gs_if` parameter, Large Restart to activate the Gs interface

**Valid for Access Type**GSM

**Key ID** FAT 102 3381/2004

### 4.12.1 Description

The Combined Procedures Gs Interface feature makes it possible for an MS in a network running in network mode of operation (NOM) 1 supporting both Circuit-Switched (CS) and Packet Switched (PS) services to connect to both services through the PS networks.

**Note:**

- Enable the IMEI Check feature to retain the International Mobile Station Equipment Identity (IMEI) check for CS services when Combined Procedures, Gs Interface is enabled. For more information, see Section 4.48 on page 50.
- Enable the Combined Procedures, Gs Interface feature in the SGSN before activating it in the BSC and MSC. It is also recommended to deactivate the feature Combined Procedures, Gs Interface in the BSC and MSC, before deactivating it in the SGSN.

### 4.12.2 Configuration

To enable the feature, the following requirements must be fulfilled:

- SS7 must be configured to support MSC/VLRs and then activated, see Configuring SS7-Based Interfaces.

— Support in the BSC. The NOM 1 must be activated.

— Support in the MSC. Combined procedures, Gs Interface must be activated.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

**Instructions**

1. If MSC/VLRs and Location Areas (LA) have already been created for combined procedures, continue to Step 4.
2. Create an MSC/VLR by using the create_msc CLI command.
3. Create an LA by using the create_la CLI command.

Before activating combined procedures communication over the Gs and Gb interfaces, the MSC/VLRs must be connected to the LAs in the SGSN-MME. Also, the MSC/VLRs must be supported by the SS7 configuration.

4. Connect an MSC/VLR to an LA by using the create_msc_la CLI command. Repeat this step until all MSC/VLRs and LAs are configured in the SGSN-MME.
5. Configure the Gs interface as follows:
    a. Configure the SS7 network to incorporate the Gs interface.
    b. Bind the following to the core network:
        — IP services defined for SS7 over IP
        — The IP addresses for the traffic over the interface
    c. As an option, configure an SSN value other than 98 to identify the message distribution to BSSAP+ and protocol settings (for example, node properties for the timer values used for supervising BSSAP+ operations in the SGSN-MME).

    For more information, refer to Gs Interface Description.
6. Enable the Gs interface by setting the `GsInterface` parameter to `on` by using the modify_gs CLI command.

    **Note:** The SS7 configuration must be ready when the `GsInterface` parameter is set to `on`. This parameter change requires a Large Restart.
7. Enable the Combined Procedures Gs Interface feature, by setting the feature state to `ACTIVATED` for the `combined_procedures_gs_if` parameter, by using the modify_feature_state CLI command.
8. Check the consistency of the pending configurations using the check_config command.

9. Activate the pending configurations using the activate_config_pending command.

10. Issue a large restart using the start_large_restart command so that the changes take effect.

To display the configuration classes and parameters related to the Gs Interface, use the following commands:

— get_config_area -can InterfaceGs

— get_config_area -can InterfaceGsSs7

For more information on how to finalize the configuration changes, see Section 3 on page 2.

## 4.13 Compression on the Gb Interface

**Parameter** data_compression_v42bis

**Activation** Runtime

**Valid for Access Type** GSM

**Key ID** FAT 102 3381/2005

**Parameter** pci_compression_rfc1144

**Activation** Runtime

**Valid for Access Type** GSM

**Key ID** FAT 102 3381/2006

### 4.13.1 Description

The Compression on the Gb Interface feature can improve the throughput on the radio interface. The throughput gain is highly dependent on the application and on the radio conditions. For data that has already been compressed, it is possible that there is no additional improvement.

The compressions included in Compression on the Gb Interface are as follows:

— TCP/IP header compression

— V.42 bis data compression

The TCP/IP header compression and the V.42 bis data compression on the Gb interface depend on the MS capabilities, and are negotiated with SGSN-MME during PDP context activation.

TCP/IP header compression reduces the size of the header, thus reducing the total size of the message, transmitted over the Gb interface. The header compression performed in the SGSN-MME has impact on the SGSN-MME resources. So as not to affect SGSN-MME characteristics, the total number of simultaneously activated PDP contexts using TCP/IP header compression is limited. Under poor radio conditions and because of mobility, the use of TCP/IP header compression can degrade performance, as several retransmissions could be needed.

V.42 bis data compression performed in the SGSN-MME has an impact on the SGSN-MME resources (using Central Processing Unit [CPU] cycles). Not to affect SGSN-MME characteristics too much, there is a fixed limit on the total number of simultaneously activated PDP contexts using data compression. V.42 bis data compression typically increases, and can double, the SGSN-MME transmission efficiency compared with uncompressed data (end-to-end IP payload packets). A compressed message means that less data is sent over the air interface and the Gb interface. The SGSN-MME compresses data packets larger than 200 bytes, and only when compression yields an advantage.

### 4.13.2 Configuration

To enable the feature, the following requirements must be fulfilled:

— To activate the TCP/IP header compression, the subscribed Quality of Service (QoS) parameter Peak Throughput Class must be higher than or equal to the `GbPciCompThroughputLim` parameter.

— To activate the V.42 bis data compression, the subscribed QoS parameter Peak Throughput Class must be higher than or equal to the `GbDataCompThroughputLim` parameter.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

#### Instructions

Enable the Compression on the Gb Interface feature, by setting the feature state to `ACTIVATED` for the `pci_compression_rfc1144` and `data_compression_v42bis` parameters, using the modify_feature_state CLI command.

For more information on how to activate the configuration changes, see Section 3 on page 2.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

## 4.14 Configurable and Adaptive Paging

**Parameter** `gsm_adaptive_paging`

`lte_adaptive_paging`

**Activation** Runtime

**Valid for Access Type**
GSM, LTE

**Key ID** FAT 102 3381/2078 (GSM)

FAT 102 3381/2103 (LTE)

### 4.14.1 Description

The Configurable and Adaptive Paging feature enables the SGSN-MME paging based on the selected paging profile for GSM and LTE access types. With the Configurable and Adaptive Paging feature, the SGSN-MME can use fewer paging attempts to locate an MS or a UE device, so that the signaling in the radio network is reduced.

For more information, see LTE Mobility Management and GSM Mobility Management.

### 4.14.2 Configuration

Enable the Configurable and Adaptive Paging for GSM feature, by setting the feature state to `ACTIVATED` for the `gsm_adaptive_paging` parameter, using the modify_feature_state CLI command.

Enable the Configurable and Adaptive Paging for LTE feature, by setting the feature state to `ACTIVATED` for the `lte_adaptive_paging` parameter, using the modify_feature_state CLI command.

For more information on how to activate the configuration changes, see Section 3 on page 2.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

For information on how to configure the paging profile table and the paging profile selection table, see Configuring Adaptive Paging.

## 4.15 Connection Suspend and Resume

**Parameter** `connection_suspend_and_resume`

**Activation** Runtime

**Valid for Access Type**LTE

**Key ID** FAT 102 3381/2118

### 4.15.1 Description

The Connection Suspend and Resume feature allows the MME to store information needed to resume a UE that has been suspended. Using the Connection Suspend and Resume procedures allows for UE services to be resumed faster, since both the S1-AP signaling and the radio signaling are reduced.

For more information, see Massive IoT, LTE Mobility Management, and S1-MME Interfaces Description.

### 4.15.2 Configuration

The use of the Connection Suspend and Resume feature requires support for User Plane CIoT EPS optimization in the MME, the eNodeB, and the UE.

Enable the feature by configuring the `connection_suspend_and_resume` parameter, using the modify_feature_state CLI command.

For more information on how to activate the configuration changes, see Section 3 on page 2.

For information on prerequisites for the management of licensed features, see Section 2 on page 1.

## 4.16 Control-Plane-Based Positioning

**Parameter** `location_services`

**Activation** Runtime

**Valid for Access Type**
GSM, WCDMA, LTE

**Key ID** FAT 102 3381/2036

### 4.16.1 Description

The Control-Plane-Based Positioning feature enables external clients to get MS or UE location data from the PLMN by connecting to a Gateway Mobile Location Center (GMLC).

For more information, see Control-Plane-Based Positioning.

**Note:** If communication between the SGSN-MME and GMLC is enabled over the Lg Interface or the SLg interface, other nodes in the network are entitled to query the SGSN-MME.

### 4.16.2 Configuration

For information on how to activate the Control-Plane-Based Positioning feature, see Control-Plane-Based Positioning.

## 4.17 Conversational QoS

**Parameter** `conversational_qos_class`

**Activation** Runtime

**Valid for Access Type** GSM, WCDMA

**Key ID** FAT 102 3381/2032

### 4.17.1 Description

The Conversational QoS feature enables configuration of the conversation class when configuring QoS. For more information, see Quality of Service. For statistical purposes set the state of the feature to `on`.

To disable the Conversational QoS feature, remove the conversational class configuration from the QoS configuration.

**Note:** The Conversational QoS feature is enabled when the license is granted. The feature cannot be enabled manually, that is, the system ignores the feature states `on` and `off`, and takes only into account if the license is granted or invalid. For information on how to load a license key file, see Installing Node-Based Licenses. If network-based licenses are used, see Activation of NeLS Client Licenses.

### 4.17.2 Configuration

Enable the Conversational QoS feature, by setting the feature state to `ACTIVATED` for the `conversational_qos_class` parameter, using the modify_feature_state CLI command.

For more information on how to activate the configuration changes, see Section 3 on page 2.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

For more CLI commands, see QoS - Policy Map (CLI).

# 4.18 Coverage Extension Support

| | |
|---|---|
| **Parameter** | `ec_gsm_iot_support`<br>`ec_lte_iot_support` |
| **Activation** | Runtime |
| **Valid for Access Type** | GSM, LTE |
| **Key ID** | FAT 102 3381/2109 |

## 4.18.1 Description

Coverage Extension Support in SGSN-MME includes the following features:

— EC-GSM IoT Support

— Coverage Extension Support, LTE

When these features are enabled, the signal coverage is extended through repeated signaling over the radio interface. Coverage Extension Support results in an improved signaling range, and increased signaling quality between connected MTC devices and the radio network.

For more information, see Massive IoT.

## 4.18.2 Configuration of EC-GSM IoT Support

To enable or disable the Configuration of EC-GSM IoT Support feature, configure the `ec_gsm_iot_support` parameter by using the modify_feature_state CLI command.

**Note:** The EC-GSM IoT Support feature is enabled at the next `BVC_RESET`, after the `ec_gsm_iot_support` parameter is configured.

For more information on how to configure EC-GSM IoT Support, see Configuring Massive IoT.

## 4.18.3 Configuration of Coverage Extension Support, LTE

To enable or disable the Configuration of Coverage Extension Support LTE feature, configure the `ec_lte_iot_support` parameter by using the modify_feature_state CLI command.

For more information on how to configure Coverage Extension Support, LTE, see Configuring Massive IoT.

# 4.19 CS Fallback to 1xRTT

**Parameter** `csfb_to_1xrtt`

**Activation** Runtime

**Valid for Access Type** LTE

**Key ID** FAT 102 3381/2063

## 4.19.1 Description

The CS Fallback to 1xRTT feature applies to both single and dual radio UE. For dual radio UE, the registration and updates in the LTE and in the CS domains are handled by the UE in the separate networks. For single radio UE, the CS registration is handled in the LTE network.

UE with dual radio configuration attaches separately to each RAT (E-UTRAN, 1xRTT) and maintains separate registration and mobility procedure handling to each RAT. It can then exit the E-UTRAN to handle a CS call, perform registration signaling, or send and receive a Short Message Service (SMS) message in 1xRTT..

For UE with a single radio configuration, 1xRTT messages are tunneled back and forth over the S102 interface which connects the MME to the 1xCS Interworking Solution (IWS). The S1-MME interface is extended with support for new messages.

For more information, see EPS Support for CS Services, S102 Interface Description, Configuring IP-Based Interfaces, and S1-MME Interface Description.

## 4.19.2 Configuration

To enable the feature, the following requirements must be fulfilled:

— Support in eNodeB for CS fallback function

— The CS Fallback to WCDMA/GSM, must be set to off, see Section 4.20 on page 28

For information on prerequisites for management of licensed features, see Section 2 on page 1.

### Instructions

1. Optionally, modify the default value of S1TUeContextReleaseCSFB, the maximum time the MME waits for a UE context release request message from the eNodeB, as a response to a CSFB request to 1xRTT, see S1-MME Interface (CLI).

2. Enable the CS Fallback to 1xRTT feature, by setting the feature state to `ACTIVATED` for the `csfb_to_1xrtt` parameter, using the modify_feature_state CLI command.

For more information on how to activate the configuration changes, see Section 3 on page 2.

## 4.20 CS Fallback to WCDMA and GSM

**Parameter** csfb_to_wg

**Activation** Runtime

**Valid for Access Type**LTE

**Key ID** FAT 102 3381/2062

### 4.20.1 Description

The CS Fallback to WCDMA and GSM feature provides the possibility to perform voice calls for a UE initially connected to EPS. The SGSN-MME supports CS Fallback (CSFB) to WCDMA with PS Handover (HO) and CSFB to WCDMA and GSM without PS HO. During the CSFB to GSM procedure, the non-GBR bearers for the UE are suspended. When the UE returns to E-UTRAN, the suspended bearers can be resumed. For more information, see EPS Support for CS Services.

### 4.20.2 Configuration

To enable the feature, the following requirements must be fulfilled:

— Support in the MSC/VLR

— Support for the SGs Interface

— The SMS over SGs feature must be set to on, see Section 4.91 on page 87

— The CS Fallback to 1xRTT must be set to off, see Section 4.19 on page 26

— The CSFB to WCDMA with PS HO requires that the Packet Handover feature is set to on, see Section 4.75 on page 69.

— Support in the eNodeB

— Support in the UE

For information on prerequisites for management of licensed features, see Section 2 on page 1.

#### Instructions

1. Optionally, modify the default value of S1TUeContextReleaseCSFBtoWG, the maximum time the MME waits for a UE context release request message from the eNodeB, as a response to a CSFB request to WCDMA or GSM, see S1-MME Interface (CLI).

2. Enable the CS Fallback to WCDMA and GSM feature, by setting the feature state to `ACTIVATED` for the `csfb_to_wg` parameter, using the modify_feature_state CLI command.

For more information on how to activate the configuration changes, see Section 3 on page 2.

## 4.21 Data over NAS

**Parameter** `data_over_nas`

**Activation** Runtime

**Valid for Access Type** LTE

**Key ID** FAT 102 3381/2112

### 4.21.1 Description

In 3GPP technical specifications, the Data over NAS feature or Data Transport over NAS feature is referred to as Control Plane Cellular IoT (CIoT) EPS optimization or Data Transport in Control Plane CIoT EPS optimization.

The DoNAS feature enables transfer of user data in the NAS PDUs, without setting up user plane data radio bearers in the RAN. GTP-U tunnels are used for data transport between the MME and the SGW. The rate of user data sent to and from a UE using DoNAS can be controlled. For more details, see Massive IoT.

DoNAS also supports the SMS service over NAS. The SMS messages are transmitted over the SGs interface without requiring the NB-IoT UEs to perform a combined procedure.

**Note:** This feature is only valid for the access type NB-IoT, which is a subset of LTE.

For more information on DoNAS, see Massive IoT.

### 4.21.2 Configuration

For information on prerequisites for management of licensed features, see Section 2 on page 1.

For information on configuration prerequisites for the DoNAS feature, see Configuring Massive IoT.

Enable the Data over NAS feature, by setting the feature state to `ACTIVATED` for the `data_over_nas` parameter, using the modify_feature_state CLI command.

For more information on how to activate the configuration changes, see Section 3 on page 2.

## 4.22 DoNAS with ROHC

**Parameter** donas_rohc

**Activation** Runtime

**Valid for Access Type** LTE

**Key ID** FAT 102 3381/2117

### 4.22.1 Description

The DoNAS with Robust Header Compression (ROHC) feature provides a standard method to compress the header of the internet packets, which performs well over wireless links.

When Control Plane CIoT EPS optimization is used for IP PDN connections, the MME supports the IP header compression based on the ROHC framework to optimize the using of radio capacity.

### 4.22.2 Configuration

The DoNAS feature must be enabled before the DoNAS with ROHC feature can be enabled.

Enable the DoNAS with ROHC feature, by setting the feature state to ACTIVATED for the donas_rohc parameter, using the modify_feature_state CLI command.

For more information about DoNAS with ROHC, see Massive IoT.

For more information about configuring DoNAS with ROHC, see Configuring Massive IoT.

For more information on how to activate the configuration changes, see Section 3 on page 2.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

## 4.23 DoNAS, PDN Type Non-IP

The DoNAS, PDN Type Non-IP feature allows the NB-IoT UEs to use generic or proprietary data protocols to deliver Non-IP data, instead of sending an IP header with the data packages.

The MME supports the following two mechanisms to transport non-IP data between the Enterprises (AS) and the Core Network (CN). They are controlled by the same license.

— Non-IP Data Delivery over SGi

— Non-IP Data Delivery over SCEF

The DoNAS feature must be enabled before the DoNAS, PDN Type Non-IP feature can be enabled.

For more information about DoNAS, PDN Type Non-IP, see Massive IoT.

For more information about configuring DoNAS, PDN Type Non-IP, seeConfiguring Massive IoT.

### 4.23.1 Non-IP Data Delivery over SGi

**Parameter** `donas_non_ip_over_sgi`

**Activation** Runtime

**Valid for Access Type**LTE

**Key ID** FAT 102 3381/2115

#### 4.23.1.1 Description

The Non-IP Data Delivery over SGi function enables handling of the PDN Type Non-IP over the S11-U interface and the SGi interface.

For more information, see Massive IoT.

#### 4.23.1.2 Configuration

For instructions on how to configure the Non-IP data delivery over SCEF function, see Configuring Massive IoT.

### 4.23.2 Non-IP Data Delivery over SCEF

**Parameter** `donas_non_ip_over_scef`

**Activation** Runtime

**Valid for Access Type**LTE

**Key ID** FAT 102 3381/2115

#### 4.23.2.1 Description

The Non-IP Data Delivery over SCEF function enables handling of the PDN Type Non-IP over the SCEF.

For more information, see Non-IP Data Delivery over SCEF.

#### 4.23.2.2 Configuration

For instructions on how to configure the Non-IP data delivery over SCEF function, see Configuring Non-IP Data Delivery over SCEF.

## 4.24 Dedicated Core Network

**Parameter** `decor_lte`

**Activation** Runtime

**Valid for Access Type** LTE

**Key ID** FAT 102 3381/2114

### 4.24.1 Description

The Dedicated Core Network (DECOR) feature provides the possibility to separate core networks for different services within a PLMN. There can be several motivations, for example, to isolate specific UEs or subscribers, or to provide the Dedicated Core Network (DCN) with specific security, Quality of Service (QoS), characteristics, functions, or resilience.

For more information, see Dedicated Core Network.

### 4.24.2 Configuration

To enable the feature, fulfill the following requirements:

— The eNodeB must support NAS message rerouting function.

— The DNS server must be upgraded with DCN MMEGI.

— When the DCN selection type is `dns`, the DNS server must support UE Usage Type in the service parameter of DNS query.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

#### Instructions

Enable the Dedicated Core Network feature, by setting the feature state to `ACTIVATED` for the `decor_lte` parameter, using the modify_feature_state CLI command.

For more information on how to activate the configuration changes, see Section 3 on page 2.

## 4.25 Detach of Inactive Subscribers GSM

**Parameter** `detach_inactive_subscriber`

**Activation** Runtime

**Valid for Access Type** GSM

**Key ID** FAT 102 3381/2010

### 4.25.1 Description

The Detach of Inactive Subscribers GSM feature allows detaching of inactive subscribers from the SGSN-MME for GSM, and thus freeing capacity. For more information, see GSM Mobility Management.

### 4.25.2 Configuration

To enable and configure the feature, do as follows:

1. Specify the minimum amount of time that has to elapse before an inactive subscriber is detached from the SGSN-MME because of inactivity, by using the modify_sgsn CLI command. Configure the `SGSNMsInactivityTimeLimit` parameter.
2. Enable the Detach of Inactive Subscribers GSM feature, by setting the feature state to `ACTIVATED` for the `detach_inactive_subscriber` parameter, using the modify_feature_state CLI command.

For more information on how to activate the configuration changes, see Section 3 on page 2.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

## 4.26 Detach of Inactive Subscribers Dual Access

**Parameter** `detach_inactive_subscriber_da`

**Activation** Runtime

**Valid for Access Type** GSM, WCDMA

**Key ID** FAT 102 3381/2052

### 4.26.1 Description

Detach of Inactive Subscribers Dual Access enables detaching of inactive subscribers from the SGSN-MME for GSM and WCDMA access types, which frees

capacity. For more information, see GSM Mobility Management and WCDMA Mobility Management.

**Note:** This feature is only applicable for the SGSN supporting the Gn interface. It is not valid for the SGSN supporting the S4 interface.

### 4.26.2 Configuration

To enable and configure the feature, do as follows:

1. Specifying the minimum amount of time that has to elapse before an inactive subscriber is detached from the SGSN because of inactivity, by using the modify_sgsn CLI command. Configure the `SGSNMsInactivityTimeLimit` parameter.

2. Enable the Detach of Inactive Subscribers Dual Access feature, by setting the feature state to `ACTIVATED` for the `detach_inactive_subscriber_da` parameter, using the modify_feature_state CLI command.

For more information on how to activate the configuration changes, see Section 3 on page 2.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

## 4.27 Detach of Inactive Subscribers WCDMA

**Parameter** `detach_inactive_subscriber_wcdma`

**Activation** Runtime

**Valid for Access Type** WCDMA

**Key ID** FAT 102 3381/2051

### 4.27.1 Description

The Detach of Inactive Subscribers WCDMA feature allows detaching of inactive subscribers from the SGSN-MME for WCDMA Systems. This frees capacity. For more information, see WCDMA Mobility Management.

### 4.27.2 Configuration

To enable and configure the feature, do as follows:

1. Specifying the minimum amount of time that has to elapse before an inactive subscriber is detached from the SGSN because of inactivity, by using the modify_sgsn CLI command. Configure the `SGSNMsInactivityTimeLimit` parameter.

2. Enable the Detach of Inactive Subscribers WCDMA feature, by setting the feature state to `ACTIVATED` for the `detach_inactive_subscribers_wcdma` parameter, using the modify_feature_state CLI command.

For more information on how to activate the configuration changes, see Section 3 on page 2.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

## 4.28 Dual Access for GSM and WCDMA

**Parameter** `dual_access_support`

**Activation** Runtime

**Valid for Access Type**
GSM, WCDMA

**Key ID** FAT 102 3381/2019

### 4.28.1 Description

The Dual Access for GSM and WCDMA feature enables the SGSN-MME to handle GSM and WCDMA subscribers simultaneously. An SGSN-MME for GSM and WCDMA access types can attach and activate PDP contexts, and negotiate throughput capacity for both GSM and WCDMA. There is no need to configure the SGSN-MME for GSM and WCDMA access types to handle a fixed number of GSM and WCDMA subscribers. This is because the feature provides dynamic capacity distribution between access types based on the actual network load. For more information on extension with this feature, see Reconfiguring Access Types (GSM and WCDMA).

**Note:** Dual Access for GSM and WCDMA is mandatory for SGSN-MMEs for GSM and WCDMA access types.

### 4.28.2 Configuration

Enable the Dual Access for GSM and WCDMA feature, by setting the feature state to `ACTIVATED` for the `dual_access_support` parameter, using the modify_feature_state CLI command.

For more information on how to activate the configuration changes, see Section 3 on page 2.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

## 4.29 Dual Access for WCDMA and LTE

**Parameter** dual_access_lw

**Activation** Runtime

**Valid for Access Type**
WCDMA, LTE

**Key ID** FAT 102 3381/2064

### 4.29.1 Description

The Dual Access for WCDMA and LTE feature enables the SGSN-MME to handle WCDMA and LTE subscribers simultaneously. An SGSN-MME for WCDMA and LTE access types can attach and activate PDP contexts or EPS bearers for both WCDMA and LTE. There is no need to configure the SGSN-MME for WCDMA and LTE access types to handle a fixed number of WCDMA and LTE subscribers. This is because the feature provides dynamic capacity distribution between access types based on the actual network load. For more information on extension with this feature, see Reconfiguring Access Types (WCDMA and LTE).

**Note:** Dual Access for WCDMA and LTE is mandatory for SGSN-MMEs for WCDMA and LTE access types.

### 4.29.2 Configuration

Enable the Dual Access for WCDMA and LTE feature, by setting the feature state to ACTIVATED for the dual_access_lw parameter, using the modify_feature_state CLI command.

For more information on how to activate the configuration changes, see Section 3 on page 2.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

## 4.30 Dual Transfer Mode

**Parameter** dual_transfer_mode

**Activation** Runtime

**Valid for Access Type**GSM

**Key ID** FAT 102 3381/2016

### 4.30.1 Description

Dual Transfer Mode enables GPRS class B MSs to transfer both voice over the CS network and data over the PS network simultaneously. A voice conversation can

be kept ongoing in parallel with, for example, email or Multimedia Messaging Service (MMS) transfer. Dual Transfer Mode is important in the context of WCDMA Systems services as it provides enhanced possibilities to extend advanced WCDMA Systems services into the GSM coverage area. For example, multimedia services can be offered, where the voice and sound is carried over the CS network, and the visual content is distributed over the PS network.

**Note:** The Dual Transfer Mode feature is applicable for GSM only. In WCDMA Systems, the corresponding function is defined by the standard.

### 4.30.2 Configuration

To enable the feature, the following requirement must be fulfilled:

— Support is also needed in Base Station Subsystem (BSS) and MSC.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

#### Instructions

Enable the Dual Transfer Mode feature, by setting the feature state to `ACTIVATED` for the `dual_transfer_mode` parameter, using the modify_feature_state CLI command.

For more information on how to activate the configuration changes, see Section 3 on page 2.

## 4.31 EDGE Support

**Parameter** `edge_support`

**Activation** Runtime

**Valid for Access Type** GSM

**Key ID** FAT 102 3381/2002

### 4.31.1 Description

The EDGE Support feature supports for EDGE in the GSM and GPRS network. EDGE technology improves the throughput on the radio interface significantly. EDGE uses high-level modulation to increase the GSM data throughput. It enables higher peak rates and triples the spectral efficiency. When negotiation for a new PDP context is done with the request for EDGE capabilities, the SGSN-MME acknowledges this and sets up the PDP context accordingly.

### 4.31.2 Configuration

Enable the EDGE Support feature, by setting the feature state to `ACTIVATED` for the `edge_support` parameter, using the modify_feature_state CLI command.

For more information on how to activate the configuration changes, see Section 3 on page 2.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

## 4.32 Enhanced Uplink Support

**Parameter** `enhanced_uplink_mbr`

**Activation** Runtime

**Valid for Access Type** WCDMA

**Key ID** FAT 102 3381/3006

### 4.32.1 Description

The Enhanced Uplink Support feature increases the maximum supported uplink bit rate to 4 Mbps. For more information on Enhanced Uplink Support, see Quality of Service.

**Note:** The Enhanced Uplink Support feature is delivered as a capacity license, thus it is enabled when the license key is loaded. This feature cannot be enabled manually. For more information on how to load a license key file, see Installing Node-Based Licenses. If network-based licenses are used, see Activation of NeLS Client Licenses.

## 4.33 Enhanced Uplink Support, Expansion 1

**Parameter** `enhanced_uplink_mbr`

**Activation** Runtime

**Valid for Access Type** WCDMA

**Key ID** FAT 102 3381/3006

### 4.33.1 Description

The Enhanced Uplink Support, Expansion 1 feature increases the maximum supported uplink bit rate to 8 Mbps. For more information on Enhanced Uplink Support, Expansion 1, see Quality of Service.

### 4.33.2 Configuration

To enable the feature, the following requirement must be fulfilled:

— The license-controlled capacity Enhanced Uplink Support (2–4 Mbps) must be granted, see Section 4.32 on page 38.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

**Note:** The Enhanced Uplink Support, Expansion 1 feature is delivered as a capacity license, thus it is enabled when the license key is loaded. This feature cannot be enabled manually. For more information on how to load a license key file, see Installing Node-Based Licenses. If network-based licenses are used, see Activation of NeLS Client Licenses.

## 4.34 Enhanced Uplink Support, Expansion 2

**Parameter** `enhanced_uplink_mbr`

**Activation** Runtime

**Valid for Access Type** WCDMA

**Key ID** FAT 102 3381/3006

### 4.34.1 Description

The Enhanced Uplink Support, Expansion 2 feature increases the maximum supported uplink bit rate to 16 Mbps. For more information on Enhanced Uplink Support, Expansion 2, see Quality of Service.

### 4.34.2 Configuration

To enable the feature, the following requirements must be fulfilled:

— The license-controlled capacity Enhanced Uplink Support (up to 4 Mbps) must be granted, see Section 4.32 on page 38.

— The license-controlled capacity Enhanced Uplink Support, Expansion 1 (up to 8 Mbps) must be granted, see Section 4.33 on page 38.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

**Note:** The Enhanced Uplink Support, Expansion 2 feature is delivered as a capacity license, thus it is enabled when the license key is loaded. This feature cannot be enabled manually. For more information on how to load a license key file, see Installing Node-Based Licenses. If network-based licenses are used, see Activation of NeLS Client Licenses.

# 4.35 Event-Based Monitoring

**Parameter** `ebm`

**Activation** Runtime

**Valid for Access Type**
GSM, WCDMA, LTE

**Key ID** FAT 102 3381/2042

## 4.35.1 Description

The Event-Based Monitoring (EBM) feature enables logging of both successful and unsuccessful signaling events, formatted according to logging criteria. The formatted event information is either logged to file or streamed in real time to the Post-Processing System, or both logged and streamed.

For more information about the EBM feature, see Event-Based Monitoring.

## 4.35.2 Configuration

To enable the feature, the following requirement must be fulfilled:

— Post-Processing System

For information on prerequisites for management of licensed features, see Section 2 on page 1.

### Instructions

For information on how to configure the feature, refer to Configuring Event-Based Monitoring.

# 4.36 Extended Idle Mode Discontinuous Reception (eDRX)

**Parameter** `edrx_lte`

`edrx_gsm`

**Activation** Runtime

**Valid for Access Type**
LTE, GSM

**Key ID** FAT 102 3381/2110

### 4.36.1 Description

The eDRX feature improves battery life of a device by reducing the time available for paging. For devices that have eDRX enabled, the SGSN-MME supports delaying paging requests until the device is in the paging window for LTE access, including NB-IoT, and in the Paging Occasion for GSM access.

For more information about the eDRX feature, see Massive IoT.

### 4.36.2 Configuration of eDRX for LTE

To enable or disable the Extended Idle Mode Discontinuous Reception (eDRX) feature for LTE including NB-IoT, configure the `edrx_lte` parameter using the modify_feature_state CLI command.

**Example**

```
gsh modify_feature_state -fsi edrx_lte -fs ACTIVATED
```

For more information on how to configure eDRX for LTE access, including NB-IoT, see Configuring Massive IoT.

### 4.36.3 Configuration of eDRX for GSM

To enable or disable the Extended Idle Mode Discontinuous Reception (eDRX) feature for GSM, configure the `edrx_gsm` parameter using the modify_feature_state CLI command.

**Example**

```
gsh modify_feature_state -fsi edrx_gsm -fs ACTIVATED
```

For more information on how to configure eDRX for GSM access, see Configuring Massive IoT.

## 4.37 Gateway Blacklisting

| | |
|---|---|
| **Parameter** | `gw_blacklisting` |
| **Activation** | Runtime |
| **Valid for Access Type** | GSM, WCDMA, LTE |
| **Key ID** | FAT 102 3381/2081 |

### 4.37.1 Description

The Gateway Blacklisting feature enables the SGSN-MME to track the status of the SGWs and PGWs in the serving PLMN. The feature also enables the operator at any time to define the status of any gateway as "blocked" or "available". For more information, see Gateway Blacklisting .

### 4.37.2 Configuration

For information about prerequisites for management of licensed features, see Section 2 on page 1.

**Instructions**

Enable the Gateway Blacklisting feature, by setting the feature state to `ACTIVATED` for the `gw_blacklisting` parameter, using the modify_feature_state CLI command.

For more information about the configuration of the Gateway Blacklisting feature, see Gateway Blacklisting (CLI).

For more information about how to activate the configuration changes, see Section 3 on page 2.

## 4.38 Gateway Restoration Procedures

| | |
|---|---|
| **Parameter** | `gw_failure_restoration_gsm`, `gw_failure_restoration_wcdma`, `gw_failure_restoration_lte` |
| **Activation** | Runtime |
| **Valid for Access Type** | GSM, WCDMA, LTE |
| **Key ID** | FAT 102 3381/2080 (GSM)<br>FAT 102 3381/2104 (WCDMA)<br>FAT 102 3381/2105 (LTE) |

### 4.38.1 Description

The Gateway Restoration Procedures feature restores the PDP contexts, the EPS bearers, or both when the related GGSN, PGW, or SGW node cannot be reached or is restarted. Applications that use these PDP contexts or EPS bearers are restored

immediately afterward. Also, the following can be fulfilled for WCDMA (S4-SGSN only) and LTE network:

— Configure the SGSN-MME to specify the restoration action based on IMSI number series when the interface between the SGW and the PGW is the S8 interface.

— Configure the MME to specify the restoration action to be used when the interface between the SGW and the PGW is the S5 interface.

For more information about this feature, see Gateway Restoration Procedures.

### 4.38.2 Configuration

For instructions on how to configure the feature, see Configuring Gateway Restoration Procedures.

For more information on how to activate the configuration changes, see Section 3 on page 2.

For more information on prerequisites for the management of licensed features, see Section 2 on page 1.

## 4.39 Gb over IP

**Parameter** `gb_over_ip`

**Activation** Small Restart

**Valid for Access Type** GSM

**Key ID** FAT 102 3381/2014

### 4.39.1 Description

The Gb over IP feature introduces the possibility to use User Datagram Protocol (UDP) over IP as bearer over the Gb interface. For more information, see Gb Interface Description.

### 4.39.2 Configuration

To enable the feature, the following requirement must be fulfilled:

— Support in the BSS

For information on prerequisites for management of licensed features, see Section 2 on page 1.

**Instructions**

For instructions on how to configure the feature, see Configuring IP-Based Interfaces.

## 4.40 Geographically Redundant Pool

**Parameter** `geo_redundant_pool`

**Activation** Runtime

**Valid for Access Type** LTE

**Key ID** FAT 102 3381/2083

### 4.40.1 Description

The Geographically Redundant Pool feature provides resilience against MME outage, S1-MME link failure, and S11 link failure, by continuous user data replication mechanisms between MMEs in a pool. The basic idea is to replicate UE contexts and subscription information in a pool environment, which are used by MMEs in recovery scenarios. For more information, see Geographically Redundant Pool.

### 4.40.2 Configuration

For instructions on how to configure the feature, see Configuring Geographically Redundant Pool.

## 4.41 GTP-C Network Load Control

**Parameter** `gtpc_network_load_control`

**Activation** Runtime

**Valid for Access Type** LTE

**Key ID** FAT 102 3381/2123

### 4.41.1 Description

The GTP-C Network Load Control feature enables the MME to select the SGW and PGW based on the GTP-C load control information (LCI). This function helps to achieve a balanced load network by using the dynamic load information.

For more information, see LTE Session Management.

### 4.41.2 Configuration

For instructions on how to configure the feature, see Configuring Session and Mobility Management.

## 4.42 GTP ULI Support for Gn-SGSN

**Parameter** `gtp_user_location`

**Activation** Runtime

**Valid for Access Type**
GSM, WCDMA

**Key ID** FAT 102 3381/2044

### 4.42.1 Description

The GTP ULI Support for Gn-SGSN feature adds the possibility of charging differentiation by informing other Network Elements of the position of the UE.

The latest UE position is included in the User Location Information (ULI) IE. The ULI IE is included in the `Create PDP Context Request` or `Update PDP Context Request` message to the GGSN. The ULI IE field can be Cell Group Identity (CGI) for GSM or Service Area Identity (SAI) for WCDMA.

**Note:** The ULI forwarding is a basic function for an S4-SGSN (GSM and WCDMA).

The Home Zone Charging Differentiation is an extension to the GTP ULI Support for Gn-SGSN feature. It is possible to adapt the charging differentiation based on the different Home Zone areas. When the UE is within a Home Zone area, the SGSN sends the `Create PDP Context` or `Update PDP Context Request` message to the GGSN. When the UE crosses a Home Zone boundary, the SGSN sends the `Update PDP Context Request` message to the GGSN. The ULI IE and RAT type are included in the message that the SGSN sends. The charging system can collect charging information from the S-CDRs, G-CDRs, or both.

**Note:** The Home Zone Charging Differentiation is also applicable to S4-SGSN (GSM).

The SGSN-MME does not apply Home Zone Charging Differentiation with a PS Handover, SNRS Relocation, or IRAT PS Handover.

For More information about Home Zone Charging Differentiation, see GSM Mobility Management and WCDMA Mobility Management.

### 4.42.2 Configuration

For instructions on how to configure GTP ULI Support for Gn-SGSN, see Configuring GTP ULI Support for Gn-SGSN.

## 4.43 HSDPA Support Expansion 1

**Parameter** qos_hsdpa_mbr

**Activation** Runtime

**Valid for Access Type** WCDMA

**Key ID** FAT 102 3381/3005

### 4.43.1 Description

The High-Speed Downlink Packet Access (HSDPA) Support feature provides improved data rates for the end user. HSDPA is useful for applications such as audio or video download and file transfer.

HSDPA Support Expansion 1 supports Maximum Bit Rates of up to 8 Mbps (that is, the capacity limit is set to 8, which is the HSDPA Support Capacity Limit capacity license value). For higher Maximum Bit Rates (up to 16, 32, 48, or 84 Mbps) HSDPA Support Expansion 2, HSDPA Support Expansion 3, HSDPA Support Expansion 4, and HSDPA Support Expansion 5 can be added. For more information, see Quality of Service.

If this license-controlled capacity is not granted, the maximum supported bit rate is 2 Mbps.

### 4.43.2 Configuration

To enable the feature, the following requirement must be fulfilled:

— Support in the GGSN, HLR/HSS, MS, and WCDMA RAN

For information on prerequisites for management of licensed features, see Section 2 on page 1.

**Note:** The HSDPA Support Expansion 1 feature is delivered as a capacity license, thus it is enabled when the license key is loaded. This feature cannot be enabled manually. For more information on how to load a license key file, see Installing Node-Based Licenses. If network-based licenses are used, see Activation of NeLS Client Licenses.

## 4.44 HSDPA Support Expansion 2

**Parameter** qos_hsdpa_mbr

**Activation** Runtime

**Valid for Access Type** WCDMA

**Key ID** FAT 102 3381/3005

### 4.44.1 Description

The HSDPA Support Expansion 2 feature supports Maximum Bit Rates of up to 16 Mbps (that is, the capacity limit is set to 16, which is the HSDPA Support Capacity Limit capacity license value). For higher Maximum Bit Rates (up to 32 Mbps, 48 Mbps, or 84 Mbps), HSDPA Support Expansion 3, HSDPA Support Expansion 4, and HSDPA Support Expansion 5 can be added. For more information, see Quality of Service.

To get the correct information in the CDR for HSDPA Support Expansion 2, the `ChCdrOutputFormat` parameter must be configured to the value `R7`, `R8`, `2009A`, `2009B`, `2010A`, `2011B`, or `latest`. Otherwise, the QoS elements in the `listOfTrafficVolumes` CDR field are truncated from 15 to 12 octets and information is lost.

The capacity limit is set to 16, which is the HSDPA Support Capacity Limit capacity license value.

### 4.44.2 Configuration

To enable the feature, the following requirements must be fulfilled:

— The license-controlled capacity HSDPA Support Expansion 1 must be active, see Section 4.43 on page 46.

— Support in the GGSN, HLR/HSS, MS, and WCDMA RAN.

— Support for the extended Maximum Bit Rate (MBR) downlink byte (octet 15) of QoS, as defined in SoC with 3GPP TS 24.008.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

**Note:** The HSDPA Support Expansion 2 feature is delivered as a capacity license, thus it is enabled when the license key is loaded. This feature cannot be enabled manually. For more information on how to load a license key file, see Installing Node-Based Licenses. If network-based licenses are used, see Activation of NeLS Client Licenses.

## 4.45 HSDPA Support Expansion 3

**Parameter** `qos_hsdpa_mbr`

**Activation** Runtime

**Valid for Access Type**WCDMA

**Key ID** FAT 102 3381/3005

### 4.45.1 Description

The HSDPA Support Expansion 3 feature supports Maximum Bit Rates of up to 32 Mbps (that is, the capacity limit is set to 32, which is the HSDPA Support Capacity Limit capacity license value). For higher Maximum Bit Rates (up to 48 Mbps or 84 Mbps), HSDPA Support Expansion 4 and HSDPA Support Expansion 5 can be added. For more information, see Quality of Service.

### 4.45.2 Configuration

To enable the feature, the following requirements must be fulfilled:

— The license-controlled capacity HSDPA Support Expansion 2 must be active, see Section 4.44 on page 46.

— Support in the GGSN, HLR/HSS, MS, and WCDMA RAN.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

**Note:** The HSDPA Support Expansion 3 feature is delivered as a capacity license, thus it is enabled when the license key is loaded. This feature cannot be enabled manually. For more information on how to load a license key file, see Installing Node-Based Licenses. If network-based licenses are used, see Activation of NeLS Client Licenses.

## 4.46 HSDPA Support Expansion 4

**Parameter** qos_hsdpa_mbr

**Activation** Runtime

**Valid for Access Type**WCDMA

**Key ID** FAT 102 3381/3005

### 4.46.1 Description

The HSDPA Support Expansion 4 feature supports Maximum Bit Rates of up to 48 Mbps (that is, the capacity limit is set to 48, which is the HSDPA Support Capacity Limit capacity license value). For higher Maximum Bit Rates (up to 84 Mbps), HSDPA Support Expansion 5 can be added. For more information, see Quality of Service.

### 4.46.2 Configuration

To enable the feature, the following requirements must be fulfilled:

— The license-controlled capacity HSDPA Support Expansion 3 must be active, see Section 4.45 on page 47.

— Support in the GGSN, HLR/HSS, MS, and WCDMA RAN.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

**Note:** The HSDPA Support Expansion 4 feature is delivered as a capacity license, thus it is enabled when the license key is loaded. This feature cannot be enabled manually. For more information on how to load a license key file, see Installing Node-Based Licenses. If network-based licenses are used, see Activation of NeLS Client Licenses.

## 4.47 HSDPA Support Expansion 5

**Parameter** `qos_hsdpa_mbr`

**Activation** Runtime

**Valid for Access Type** WCDMA

**Key ID** FAT 102 3381/3005

### 4.47.1 Description

The HSDPA Support Expansion 5 feature supports Maximum Bit Rates of up to 84 Mbps (that is, the capacity limit is set to 84, which is the HSDPA Support Capacity Limit capacity license value). For more information, see Quality of Service.

**Note:**

— The HSDPA Support Expansion 5 feature is not applicable for MBMS.

### 4.47.2 Configuration

To enable the feature, the following requirements must be fulfilled:

— The license-controlled capacity HSDPA Support Expansion 4 must be active, see Section 4.46 on page 48.

— Support in the GGSN, HLR/HSS, MS, and WCDMA RAN.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

**Note:** The HSDPA Support Expansion 5 feature is delivered as a capacity license, thus it is enabled when the license key is loaded. This feature cannot be enabled manually. For more information on how to load a license key file, see Installing Node-Based Licenses. If network-based licenses are used, see Activation of NeLS Client Licenses.

## 4.48 IMEI Check

**Parameter** `imei_check`

**Activation** Runtime

**Valid for Access Type** GSM, WCDMA, LTE

**Key ID** FAT 102 3381/2023

### 4.48.1 Description

The IMEI Check feature provides means of network access control for specific mobile equipment. This can be used, for example, for discouraging theft of mobile equipment. The feature can be activated independently for each radio access type. For more information about the IMEI Check feature, see IMEI Check.

### 4.48.2 Configuration

Enable the IMEI Check feature, by setting the feature state to `ACTIVATED` for the `imei_check` parameter, using the modify_feature_state CLI command.

For more information on how to activate the configuration changes, see Section 3 on page 2.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

## 4.49 IMS-Based Telephony - MMTel

**Parameter** `mmtel`

**Activation** Runtime

**Valid for Access Type** LTE

**Key ID** FAT 102 3381/2075

### 4.49.1 Description

The IMS-Based telephony - MMTel feature is a license-controlled feature for the SGSN-MME. The feature allows Packet Switched access for IMS-based voice, IMS

Emergency Service (referred to as IMS emergency session support in 3GPP), and other multimedia services that are anchored in the IMS. The feature supports IMS Emergency Service for authenticated UE, unauthenticated UE with SIM cards, and unauthenticated UE without SIM cards.

This feature is enhanced by Service Priority Based Paging, which is used to prioritize the paging for specific services, such as MT VoLTE calls, based on the ARP of the received `Downlink Data Notification` (DDN) message. For more information on this enhancement, see LTE Mobility Management.

This feature requires activation of the Network-Initiated Dedicated Bearers feature. For more information on the Network-Initiated Dedicated Bearers feature, see Section 4.71 on page 67.

### 4.49.2 Configuration

For instructions on how to configure the feature and Service Priority Based Paging, see Configuring MMTel Service.

## 4.50 Integrated Traffic Capturing

**Parameter** `integrated_traffic_capture`

**Activation** Runtime

**Valid for Access Type** GSM, WCDMA, LTE

**Key ID** FAT 102 3381/2037

### 4.50.1 Description

The Integrated Traffic Capturing (ITC) feature is used as a replacement or as a complement in external protocols and interface probes, to simplify troubleshooting of traffic-related faults, by capturing traffic on multiple interfaces. ITC supports the following features:

— ITC Gb captures traffic over both Gb-over-IP and Gb-over-Frame Relay.

— ITC GTP-U captures GTP-U traffic over the Gn/Gp, the S4-U, and the Iu-U interfaces.

— ITC GTP-C captures GTP-C traffic for any IP Network.

— ITC SCTP captures SCTP traffic for any IP Network.

When an ITC job is started, traffic is captured in the ITC capture buffers. The captured traffic is defined by the ITC filters configured for an ITC job. The capture buffers can be saved in capture files formatted as Packet Capture (PCAP) for

further analysis in the Network Protocol Analyzer. The logs are stored on the File Service Board (FSB).

The ITC supports capturing of IPv6 traffic for GTP-C and SCTP traffic protocols. The GTP-C traffic is captured on the AP, while the SCTP traffic is captured on the SS7/SCTP DP.

For more information, see Capturing Traffic using ITC.

### 4.50.2 Configuration

Enable the Integrated Traffic Capturing feature, by setting the feature state to `ACTIVATED` for the `integrated_traffic_capture` parameter, using the modify_feature_state CLI command.

For more information on how to activate the configuration changes, see Section 3 on page 2.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

For more information about related CLI commands, see Integrated Traffic Capturing (CLI).

## 4.51 Low Complexity UE Support

**Parameter** `iot_m2m_low_complexity_ue_support`

**Activation** Runtime

**Valid for Access Type** LTE

**Key ID** FAT 102 3381/2095

### 4.51.1 Description

The Low Complexity UE Support feature enables the MME to store the UE Radio Capability for Paging information and notify the eNodeB of this information in the `Paging` message. The presence of the UE Radio Capability for Paging information indicates that the network is dealing with a low-complexity UE. With this information, the eNodeB performs a power boost when paging these low-complexity UEs, so the paging coverage is extended.

The low-complexity UEs are targeted to the low-end (for example, low average revenue per user, low data rate, or delay tolerant) applications, for example, some Machine-Type Communications (MTC). A low complexity UE has reduced Tx and Rx capabilities compared to other UE of different categories. Category-0 and Category-M1 belong to low complexity UEs.

For more information, see Massive IoT.

### 4.51.2 Configuration

Enable the Low Complexity UE Support feature, by setting the feature state to `ACTIVATED` for the `iot_m2m_low_complexity_ue_support` parameter, using the modify_feature_state CLI command.

For more information, see Configuring Massive IoT.

## 4.52 IPsec for Secure Network Traffic

**Parameter** `ipsec_support`

**Activation** Runtime

**Valid for Access Type** GSM, WCDMA, LTE

**Key ID** FAT 102 3381/2034

### 4.52.1 Description

The IPsec for Secure Network Traffic feature enables secure transmission between SGSN-MMEs, and between SGSN-MMEs and GGSNs. It can also be used to secure the link between the SGSN-MMEs and the Elements or the Network Management Systems, or for Lawful Interception (LI) purposes.

### 4.52.2 Configuration

For instructions on how to configure the feature, see Configuring IP-Based Interfaces.

## 4.53 Lawful Intercept

**Parameter** `lawful_interception`

**Activation** Small Restart

**Valid for Access Type** GSM, WCDMA, LTE

**Key ID** FAT 102 3381/2035

### 4.53.1 Description

The Lawful Intercept (LI) feature allows law enforcement agencies to access information about the activities of the subscribers and their user data. For more information about LI, contact the local Ericsson support.

### 4.53.2 Configuration

Enable the Lawful Intercept feature, by setting the feature state to ACTIVATED for the lawful_interception parameter, using the modify_feature_state CLI command.

For more information on how to activate the configuration changes, see Section 3 on page 2.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

## 4.54 Lawful Intercept, Exp 1

**Parameter** lawful_interception_var2

**Activation** Small Restart

**Valid for Access Type**
GSM, WCDMA, LTE

**Key ID** FAT 102 3381/2089

### 4.54.1 Description

Lawful Intercept, Exp 1 is a market-specific variant of Lawful Interception. For more information about LI, contact the local Ericsson support.

### 4.54.2 Configuration

Enable the Lawful Intercept, Exp 1 feature, by setting the feature state to ACTIVATED for the lawful_interception_var2 parameter, using the modify_feature_state CLI command.

For more information on how to activate the configuration changes, see Section 3 on page 2.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

## 4.55 Lawful Intercept, HI2, and XML-Based X1

**Parameter** lawful_intercept_hi2_and_xml_based_x1

**Activation** Small Restart

**Valid for Access Type**LTE

**Key ID** FAT 102 3381/2035

### 4.55.1 Description

The Lawful Intercept, HI2, and XML-based X1 feature is a market-specific variant of Lawful Intercept. For more information about LI, contact the local Ericsson support.

**Note:** The Lawful Intercept, HI2, and XML-based X1 feature is mutually exclusive with the Lawful Intercept feature.

### 4.55.2 Configuration

Enable the Lawful Intercept, HI2, and XML-based X1 feature, by setting the feature state to `ACTIVATED` for the `lawful_intercept_hi2_and_xml_based_x1` parameter, using the modify_feature_state CLI command.

For more information on how to activate the configuration changes, see Section 3 on page 2.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

## 4.56 Location Based IP Address Allocation

**Parameter** `loc_based_ip_allocation_gsm`

`loc_based_ip_allocation_wcdma`

`loc_based_ip_allocation_lte`

**Activation** Runtime

**Valid for Access Type**

GSM, WCDMA, LTE

**Key ID** FAT 102 3381/2091 (GSM)

FAT 102 3381/2101 (WCDMA)

FAT 102 3381/2102 (LTE)

### 4.56.1 Description

The Location Based IP Address Allocation feature is an end-to-end feature involving both the SGSN-MME and the GGSN or PGW. With this feature, the GGSN or PGW allocates IP addresses to UEs based on their locations and the SGSN-MME helps to ensure that the IP addresses correspond to the locations. For more information about the feature, see Location Based IP Address Allocation.

### 4.56.2 Configuration

For instructions on how to configure the feature, see Configuring Location Based IP Address Allocation.

## 4.57 LTE Broadcast

**Parameter** `embms_support`

**Activation** Runtime

**Valid for** LTE

**Key ID** FAT 102 3381/2077

### 4.57.1 Description

The LTE Broadcast feature enables broadcast services in the LTE radio network, for example, broadcast of TV channels and background applications such as downloading of files. For more information, see LTE Broadcast.

### 4.57.2 Configuration

To enable the feature, the following requirement must be fulfilled:

— Support in the Multimedia Broadcast Multicast Service Gateway (MBMS-GW) and the Multi-cell/Multicast Coordination Entities (MCE).

**Instructions**

Enable the LTE Broadcast feature, by setting the feature state to `ACTIVATED` for the `embms_support` parameter, using the modify_feature_state CLI command.

For more information on how to activate the configuration changes, see Section 3 on page 2.

## 4.58 MBMS: Broadcast Services

**Parameter** `mbms_broadcast`

**Activation** Runtime

**Valid for Access Type** WCDMA

**Key ID** FAT 102 3381/2041

### 4.58.1 Description

The MBMS: Broadcast Services feature enables broadcast services in the WCDMA Systems radio network for streaming applications, for example, broadcast of TV channels and background applications such as downloading of files. For more information, see MBMS.

### 4.58.2 Configuration

To enable the feature, the following requirements must be fulfilled:

— Support in the GGSN and the RNC.

— For MBMS sessions using the streaming traffic class, the license-controlled feature Streaming QoS must be activated, see Section 4.93 on page 88.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

**Instructions**

Enable the MBMS: Broadcast Services feature, by setting the feature state to `ACTIVATED` for the `mbms_broadcast` parameter, using the modify_feature_state CLI command.

For more information on how to activate the configuration changes, see Section 3 on page 2.

## 4.59 Minimization of Drive Tests

**Parameter** `mdt`

**Activation** Runtime

**Valid for Access Type** LTE

**Key ID** FAT 102 3381/2113

### 4.59.1 Description

With the Minimization of Drive Tests (MDT) feature, the MME transfers user consent for MDT activation from the HSS to the eNodeB. If MDT Mapping is enabled on the MME, the MME associates the MDT trace with the IMEI-TAC. The mapping data can be logged in log files on the MME, streamed to the TCE, or both logged and streamed.

For more information about this feature, see Minimization of Drive Tests.

### 4.59.2 Configuration

Before enabling this feature, check that the eNodeB, HSS, and OSS support MDT.

For more information on prerequisites for management of licensed features, see Section 2 on page 1.

#### Instructions

For information on how to configure this feature, see Configuring Minimization of Drive Tests.

## 4.60 Misconfigured MT Identification

**Parameter** `misconfig_mt_id`

**Activation** Runtime

**Valid for Access Type**
GSM, WCDMA, LTE

**Key ID** FAT 102 3381/2045

### 4.60.1 Description

The Misconfigured MT Identification feature provides logging of PDP context requests rejected and PDN connection requests rejected with `cause code #33`. Furthermore, replaced APNs are also logged with `cause code #33` because of APN redirection. For more information about APN redirection, see APN Resolve and Redirect for LTE Access. Both the rejects and the replaced APNs are stored in the Session Event Log. For more information, see Session Event Log.

### 4.60.2 Configuration

Enable the Misconfigured MT Identification feature, by setting the feature state to `ACTIVATED` for the `misconfig_mt_id` parameter, using the modify_feature_state CLI command.

For more information on how to activate the configuration changes, see Section 3 on page 2.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

## 4.61 MME Pool

**Parameter** `mme_pool`

**Activation** Runtime

**Valid for Access Type** LTE

**Key ID** FAT 102 3381/2053

### 4.61.1 Description

The MME Pool feature provides a flexible and efficient network architecture with built-in network redundancy. Each eNodeB is connected to all SGSN-MMEs in the pool. If one SGSN-MME becomes unavailable, the attached UE is provided service by another SGSN-MME in the pool. The load on pools containing members of different capacity can be balanced by adjusting the `RelativeMmeCapacity` of each member. For more information, see MME Pool.

### 4.61.2 Configuration

To enable the feature, the following requirements must be fulfilled:

— Support in eNodeB

— Support, preferably, in OSS

For information on prerequisites for management of licensed features, see Section 2 on page 1.

#### Instructions

For instructions on how to configure the feature, see MME Pool and Managing an MME Pool.

## 4.62 MME Support of HeNB

**Parameter** `support_henb`

**Activation** Runtime

**Valid for Access Type** LTE

**Key ID** FAT 102 3381/2084

### 4.62.1 Description

The MME Support of HeNB feature enables the MME to support small cells (Home eNodeBs) in addition to macro cells (traditional macro eNodeBs) for improving the coverage and the capacity, especially indoors. The MME searches primarily for the target Home eNodeB (HeNB) that is connected to the MME directly. If the MME fails to find the target HeNB, the MME searches for the HeNB GW that is connected to the target HeNB.

For information about HeNB supported S1-based handover, see LTE Mobility Management.

For information about HeNB supported IRAT handover, see Inter-System Mobility Management.

For information about HeNB supported the Self-Organizing Network (SON), see S1-MME Interface Description.

### 4.62.2 Configuration

For instructions on how to configure the feature, see Configuring Session and Mobility Management.

## 4.63 MME Support for Closed Subscriber Group

**Parameter** `closed_subscriber_group`

**Activation** Runtime

**Valid for Access Type** LTE

**Key ID** FAT 102 3381/2088

### 4.63.1 Description

The optional MME Support for Closed Subscriber Group (CSG) feature provides UE access control to a specified CSG. This feature supports the closed access mode and the hybrid access mode.

In the closed access mode, a CSG identifies a set of users permitted to access specified CSG cells of Home eNodeBs (HeNBs) or HeNB GWs. Access to a CSG implies the UE has permission to access all cells within the specified CSG. In the hybrid access mode, the MME determines the CSG membership status for the UE according to the CSG ID and CSG subscription data, and then informs the HeNB or HeNB GW of the CSG membership. In both the closed access mode and hybrid access mode, the MME reports the user CSG information for the UE to the SGW.

**Note:**

- This feature operates only with HeNBs/HeNB GWs and not with traditional macro eNodeBs.
- This feature requires the MME Support of HeNB feature to be enabled.
- In the closed access mode, the UE using IMS Emergency Service is not affected by this feature.

For more information, see Closed Subscriber Group.

### 4.63.2 Configuration

For instructions on how to configure this feature, see Configuring Session and Mobility Management.

## 4.64 Mobility-Based Policy

**Parameter** `mobility_based_policy_gsm`

`mobility_based_policy_wcdma`

`mobility_based_policy_lte`

**Activation** Runtime

**Valid for Access Type** GSM, WCDMA, LTE

**Key ID** FAT 102 3381/2121 (GSM)

FAT 102 3381/2106 (WCDMA)

FAT 102 3381/2090 (LTE)

### 4.64.1 Description

The Mobility-Based Policy feature enables direct communication between the MME and Gn-SGSN (WCDMA) and the Service-Aware Policy Controller (SAPC). The SGSN-MME and SAPC are connected over the Smp interface, which is based on Diameter on top of SCTP.

By using the Smp interface, the SGSN-MME can report the User Location Information to the SAPC for deploying location-based policies. The MME and the Gn-SGSN (WCDMA) can report the change of UE presence in a Presence Reporting Area (PRA) to the SAPC and the MME can also report the change of UE location to the SAPC.

Besides location-based policies, the MME and the Gn-SGSN can use policies from the SAPC for RAT/Frequency Selection Priority (RFSP) selection. The MME can also use policies from the SAPC for PGW selection.

The MME and Gn-SGSN (WCDMA) can also use policies from the SAPC for GGSN/PGW selection.

For more information about the Mobility-Based Policy feature, see Mobility-Based Policy.

**Note:** For LTE, the Mobility-Based Policy, the Cell Change Reporting, and Presence Reporting Area Support features are mutually exclusive.

For information about the Cell Change Reporting feature, see Section 4.11 on page 18. For information about the Presence Reporting Area Support feature, see Section 4.77 on page 73.

**Note:** The Smp interface was named Sx interface in SGSN-MME 1.9 and the previous releases. For backward compatibility, Sx is still kept in operation and maintenance-related fields.

### 4.64.2 Configuration

For instructions on how to configure the feature, see Configuring Mobility-Based Policy.

## 4.65 Monitoring Enhancements

**Parameter** `monitoring_enhancements`

**Activation** Runtime

**Valid for Access Type** LTE

**Key ID** FAT 102 3381/2120

### 4.65.1 Description

The Monitoring Enhancements (MONTE) feature allows for information on specific events that is normally internal to the MME to be made available to the Service Capability Exposure Function (SCEF) node. For more information, see Massive IoT.

### 4.65.2 Configuration of MONTE

To enable or disable the MONTE feature, configure the `monitoring_enhancements` parameter using the modify_feature_state CLI command.

**Example**

```
gsh modify_feature_state -fsi monitoring_enhancements -fs
ACTIVATED
```

**Note:** The monitoring_enhancements parameter is not supported in this release.

## 4.66 MS-Activated Secondary PDP Context

**Parameter** `secondary_context`

**Activation** Runtime

**Valid for Access Type**

GSM, WCDMA

**Key ID** FAT 102 3381/2009

### 4.66.1 Description

The MS-Activated Secondary PDP Context feature enables a subscriber to have multiple active PDP contexts initiated from the MS using a single IP address and one APN. For more information, see GSM and WCDMA Session Management.

**Note:** The MS-Activated Secondary PDP Context feature is only applicable for the SGSN supporting the Gn interface. It is not valid for the SGSN supporting the S4 interface.

### 4.66.2 Configuration

Enable the MS-Activated Secondary PDP Context feature, by setting the feature state to `ACTIVATED` for the `secondary_context` parameter, using the modify_feature_state CLI command.

For more information on how to activate the configuration changes, see Section 3 on page 2.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

## 4.67 Multi-Operator Core Network

**Parameter** `mocn_gsm`

`mocn_wcdma`

`mocn_lte`

**Activation** Runtime

**Valid for Access Type**

GSM, WCDMA, LTE

**Key ID** FAT 102 3381/2030 (GSM)

FAT 102 3381/2096 (WCDMA)

FAT 102 3381/2097 (LTE)

### 4.67.1 Description

The MOCN feature allows two or more operators to share a common radio network, while maintaining separate core networks, see Support for Shared Networks.

### 4.67.2 Configuration

To enable the feature, fulfill the requirements in Table 2.

| Access Type | Prerequisites |
|---|---|
| GSM | • Support in the BSC and MSC.<br>• An NRI bit length 5–8 bits.<br>• Common PLMNs used by non-supporting UEs must be configured as MOCN enabled, and the common PLMNs must not equal to any of dedicated PLMNs. This requires the feature Multiple PLMN Support.<br>• When the node function mocn_gs_coexistence_allowed using the modify_node_function CLI command, the Combined Procedures, Gs Interface, and the MOCN features can be enabled at the same time. |
| WCDMA | • Support in the RNC and MSC.<br>• An NRI bit length 5–8 bits.<br>• Network selection supported in supporting UEs.<br>• Only common PLMNs used by non-supporting UEs must be configured as MOCN enabled, and the common PLMNs must not equal to any of dedicated PLMNs. This requires the feature Multiple PLMN Support. |
| LTE | Support in the eNodeB. |

When activating MOCN in a network, it is recommended to first enable the function in the SGSN-MME, and then gradually enable MOCN in the RNCs/BSCs.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

#### Instructions

Enable the Multi-Operator Core Network feature, by setting the feature state to `ACTIVATED` for the `mocn_gsm`, `mocn_wcdma`, and `mocn_lte` parameters, using the modify_feature_state CLI command.

For more information on how to activate the configuration changes, see Section 3 on page 2.

For instructions on how to configure the feature for PLMN and NRI, see PLMN Identification (CLI) and Network Resource Identifier (CLI), respectively.

## 4.68 Multiple PLMN Support

**Parameter** `multiple_plmn_support`

**Activation** Runtime

**Valid for Access Type**
GSM, WCDMA, LTE

**Key ID** FAT 102 3381/2003

### 4.68.1 Description

The Multiple PLMN Support feature allows up to 10 PLMNs to share SGSN-MME. For more information, see GSM Mobility Management, WCDMA Mobility Management, and LTE Mobility Management.

### 4.68.2 Configuration

To enable and configure the feature, do as follows:

1. Optionally, include the PLMN identifier in the CDRs, by using the modify_charging CLI command. Configure the `ChSgsnIncludePlmnInformation` parameter.

   **Note:** This step is only applicable for GSM and WCDMA.

2. Enable the Multiple PLMN Support feature, by setting the feature state to `ACTIVATED` for the `multiple_plmn_support` parameter, using the modify_feature_state CLI command.

For more information on how to activate the configuration changes, see Section 3 on page 2.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

**Note:** If a single SGW node planned to support multiple PLMNs, it requires to return the unique node name in the DNS configuration according to the standard.

If the SGW node supporting multiple PLMNs has multiple node names according to the PLMN in the DNS configuration for an operator preference, it requires that all the TAIs belonging to these PLMNs return all these node names for the serving GW node in the DNS configuration.

## 4.69 M2M/IoT: Direct Short Data Service

**Parameter** `sds_support`

**Activation** Runtime

**Valid for Access Type** LTE

**Key ID** FAT 102 3381/2107

### 4.69.1 Description

This is a customized M2M/IoT feature, which provides the Short Data Service over the SGs-Lite interface for the SDS capable UEs. The SGs-Lite interface connects the MME and the SDS GW, and the interface is based on Transmission Control Protocol (TCP).

For more information about the M2M/IoT: Direct Short Data Service feature, contact the local Ericsson support.

## 4.70 Near Real-Time Provision of CDRs

**Parameter** `gtpprime`

**Activation** Small restart

**Valid for Access Type**

GSM, WCDMA

**Key ID** FAT 102 3381/2015

### 4.70.1 Description

The Near Real-Time Provision of CDRs feature renders possible the output of CDRs to the charging gateway or billing system within 30 seconds after generation in the SGSN. For more information, see CDR-Based Charging.

### 4.70.2 Configuration

For instruction on how to configure the feature, see Configuring CDR-Based Charging.

## 4.71 Network-Initiated Dedicated Bearers

**Parameter** `dedicated_bearers`

**Activation** Runtime

**Valid for Access Type** LTE

**Key ID** FAT 102 3381/2054

### 4.71.1 Description

The Network-initiated Dedicated Bearers feature is a licensed feature which enables establishment of multiple, dedicated bearers, in addition to the default bearers. For more information on dedicated bearers, see LTE Session Management.

If a license for the feature has been granted, it is possible to enable or disable the use of dedicated bearers by using the modify_feature_state CLI command. If the feature is disabled by configuration, only default bearers can be established. When a node is upgraded, and the license for the feature has been granted for that node, the feature is enabled automatically.

### 4.71.2 Configuration

Enable the Network-Initiated Dedicated Bearers feature, by setting the feature state to `ACTIVATED` for the `dedicated_bearers` parameter, using the modify_feature_state CLI command.

For more information on how to activate the configuration changes, see Section 3 on page 2.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

## 4.72 Network-Requested Secondary PDP Context

**Parameter** `nw_init_sec_pdpctxt`

**Activation** Runtime

**Valid for Access Type**

GSM, WCDMA

**Key ID** FAT 102 3381/2057

### 4.72.1 Description

The network can request secondary PDP contexts associated with an activated primary PDP context. A secondary PDP context reuses the IP address and APN from the primary PDP context. The primary PDP context and the associated secondary PDP context connect to the same PDN with a different guaranteed QoS. For more information, see GSM and WCDMA Session Management.

**Note:** This feature is not applicable to the S4-SGSN on the GSM network.

### 4.72.2 Configuration

Enable the Network-Requested Secondary PDP Context feature, by setting the feature state to `ACTIVATED` for the `nw_init_sec_pdpctxt` parameter, using the modify_feature_state CLI command.

**Note:** Do not set the `SGSNAllowQosUpgrade` parameter to `noCommonFlag`. For more information, see SGSN-MME Licensed Capacities and Features.

For more information on how to activate the configuration changes, see Section 3 on page 2.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

## 4.73 NR Access Control

**Parameter** `nr_access_control`

**Activation** Runtime

**Valid for Access Type** LTE

**Key ID** FAT 102 3381/2119

### 4.73.1 Description

The NR Access Control feature enables the MME to control whether NR as secondary RAT is restricted or not. For more information, see 5G EPC.

### 4.73.2 Configuration

Enable the NR Access Control feature for LTE Systems, by setting the feature state to `ACTIVATED` for the `nr_access_control` parameter, using the modify_feature_state CLI command.

For more information on how to activate the configuration changes, see Section 3 on page 2.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

## 4.74 Packet Flow Control per PFC

**Parameter** `pfc_flow_control`

**Activation** Runtime

**Valid for Access Type** GSM

**Key ID** FAT 102 3381/2020

### 4.74.1 Description

The Packet Flow Control per PFC feature makes the radio network a part of QoS provisioning by involving it in QoS negotiations. Before the SGSN-MME can start BSS PFC signaling, the BSS must support BSS PFC messages. For more information, see Quality of Service

.

**Note:** Activate Packet Flow Control per PFC feature in the SGSN-MME, before activating it in the BSS.

### 4.74.2 Configuration

To enable the feature, the following requirement must be fulfilled:

— Support in the BSS and MS

For information on prerequisites for management of licensed features, see Section 2 on page 1.

#### Instructions

Enable the Packet Flow Control per PFC feature, by setting the feature state to `ACTIVATED` for the `pfc_flow_control` parameter, using the modify_feature_state CLI command.

For more information on how to activate the configuration changes, see Section 3 on page 2.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

# 4.75 Packet Handover

The Packet Handover feature includes PS Handover, SRNS Relocation, and Load-based Handover functionalities.

## 4.75.1 PS Handover

**Parameter** ps_ho

**Activation** Runtime

**Valid for Access Type**
WCDMA, GSM, LTE

**Key ID** FAT 102 3381/2039

### 4.75.1.1 Description

Packet Handover provides intra-SGSN Packet Switched (PS) handover, inter-SGSN PS Handover, and Inter-Radio Access Technology (IRAT) PS Handover. The Packet Handover feature is required for SRVCC from LTE to WCDMA with PS Handover support. For further information, see Section 4.90 on page 85.

IRAT PS Handover is handover between different Radio Access Networks (RANs), for example, between GSM and WCDMA or between WCDMA and LTE over the S3 or the Gn interface. For more information, see Inter-System Mobility Management. To enable an IRAT PS Handover from LTE to WCDMA over the Gn interface, the SRNS Relocation needs to be used as well. For more information on this, see Section 4.75.2 on page 71.

If an SGSN-MME Pool move operation is in progress for the MS, Packet Handover (GSM) attempts are rejected by both the old and new SGSN-MME.

### 4.75.1.2 Configuration

To enable the functionality, the following requirement must be fulfilled:

— Support in the RNC and MS

For information on prerequisites for management of licensed features, see Section 2 on page 1.

#### Instructions

Enable the Packet Handover feature, by setting the feature state to ACTIVATED for the ps_ho parameter, using the modify_feature_state CLI command.

For more information on setting up the commands with a MOCN-enabled PLMN, see these sections in Support for Shared Networks:

— Allowing SRNS Relocation or IRAT PS Handover Procedures into or within a MOCN-Enabled PLMN (to WCDMA Systems)

— Allowing PS Handover or IRAT PS Handover Procedures into or within a MOCN-Enabled PLMN (to GSM Systems)

For more information on how to activate the configuration changes, see Section 3 on page 2.

## 4.75.2 SRNS Relocation

**Parameter** `srns_relocation`

**Activation** Runtime

**Valid for Access Type** WCDMA

**Key ID** FAT 102 3381/2031

### 4.75.2.1 Description

SRNS Relocation enables handovers of active PS connections between RNCs. Both Intra-SGSN SRNS Relocation and Inter-SGSN SRNS Relocation are enabled. For more information, see WCDMA Mobility Management. Furthermore, the SRNS Relocation enables the IRAT PS Handover from LTE to WCDMA over the Gn interface in the target SGSN. For an IRAT PS Handover from LTE to WCDMA over the Gn interface, the target SGSN cannot differentiate it from an Inter-SGSN SRNS Relocation over the Gn interface. In this case, the SRNS Relocation needs to be used in the target SGSN to enable the IRAT PS Handover from LTE to WCDMA over the Gn interface.

### 4.75.2.2 Configuration

To enable the functionality, the following requirement must be fulfilled:

— Support in the RNC and MS

For information on prerequisites for management of licensed features, see Section 2 on page 1.

#### Instructions

Enable the SRNS Relocation feature, by setting the feature state to `ACTIVATED` for the `srns_relocation` parameter, using the modify_feature_state CLI command.

For more information on setting up the commands with a MOCN-enabled PLMN, see Support for Shared Networks.

For more information on how to activate the configuration changes, see Section 3 on page 2.

### 4.75.3 Load-based Handover

**Parameter** `loadbased_ho`

**Activation** Runtime

**Valid for Access Type** WCDMA

**Key ID** FAT 102 3381/2038

#### 4.75.3.1 Description

Load-Based Handover enables an RNC to trigger an IRAT PS Handover from WCDMA Systems to GSM. For more information, see Inter-System Mobility Management.

#### 4.75.3.2 Configuration

To enable the functionality, the following requirements must be fulfilled:

— Support in the RNC and MS

— The prerequisite for activating Load-based handover is that PS Handover is activated.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

**Instructions**

Enable the Load-based Handover feature, by setting the feature state to `ACTIVATED` for the `loadbased_ho` parameter, using the modify_feature_state CLI command.

For more information on how to activate the configuration changes, see Section 3 on page 2.

## 4.76 Paging Suppression for Fixed Wireless Access

**Parameter** `paging_suppression_for_fwa`

**Activation** Runtime

**Valid for Access Type** LTE

**Key ID** FAT 102 3381/2122

### 4.76.1 Description

The Paging Suppression for Fixed Wireless Access feature reduces the signalling for the Fixed Wireless Access devices which do not need to be paged. For more information, see LTE Mobility Management.

### 4.76.2 Configuration

Configure and enable the feature by following the instructions in LTE Mobility Management.

For more information on how to activate the configuration changes, see Section 3 on page 2.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

## 4.77 Presence Reporting Area Support

**Parameter** `presence_reporting_area_support`

**Activation** Runtime

**Valid for Access Type** LTE

**Key ID** FAT 102 3381/2108

### 4.77.1 Description

The licensed-controlled Presence Reporting Area Support feature enables the MME to send Presence Reporting Area (PRA) information to the PCRF through SGW and PGW. PRA information is sent only when there is a change in the PRA status of the UE, meaning that the information is sent when the UE enters or leaves a pre-defined PRA. A PRA is composed of a list of cells, Macro eNodeBs, Home eNodeBs, and Tracking Areas (TAs).

**Note:** The Presence Reporting Area Support feature is mutually exclusive from the Cell Change Reporting and Mobility-Based Policy features.

For information about the Cell Change Reporting feature, see Section 4.11 on page 18.

For information about the Mobility-Based Policy feature, see Section 4.64 on page 61.

For more information, see Presence Reporting Area Support.

### 4.77.2 Configuration

Enable the Presence Reporting Area Support feature, by setting the feature state to ACTIVATED for the presence_reporting_area_support parameter, using the modify_feature_state CLI command.

For more information on how to activate the configuration changes, see Section 3 on page 2.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

#### Configure a PRA Definition in PCRF

**Note:** For a UE-dedicated PRA, the PRA ID must be in the range of 0-8388607.

#### Configure a PRA Definition in MME

Define a PRA on the MME using the create_presence_reporting_area CLI command.

1. Optionally, define one or more Geographical Areas (GAs) as follows:
   - Create a GA using the create_ga CLI command.
   - Add a range of Tracking Areas (TAs) to the GA, using the create_ga_ta_range CLI command.
2. Optionally, define one or more Global eNodeBs range using the create_global_enodeb_range CLI command.
3. Optionally, define one or more ECGI ranges using the create_ecgi_range CLI command.
4. Configure one or more PRAs using the create_presence_reporting_area CLI command using the previously defined GAs, Global eNodeB ranges, or ECGI ranges.

**Note:** For Core Network predefined PRA, the PRA ID must be in the range of 8388608-16777215.

**Note:** Up to 2000 ranges can be configured for each PRA. A PRA must be configured with at least one GA, Global eNodeB range, or ECGI range.

To verify whether a location is in or out of a PRA, use the test_pra Toolbox command.

## 4.78 Prioritization of Payload Users after Restart

**Parameter** prioritise_payload_users

**Activation** Runtime

**Valid for Access Type**GSM

**Key ID** FAT 102 3381/2017

### 4.78.1 Description

The Prioritization of Payload Users after Restart feature improves the service availability for active subscribers after an SGSN restart. Activation of payload traffic, PDP contexts, and SMS are given higher priority than other types of subscriber activities. For more information, see GSM Mobility Management.

### 4.78.2 Configuration

Enable the Prioritization of Payload Users after Restart feature, by setting the feature state to `ACTIVATED` for the `prioritise_payload_users` parameter, using the modify_feature_state CLI command.

For more information on how to activate the configuration changes, see Section 3 on page 2.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

## 4.79 Public Warning System

**Parameter** `public_warning_system`

**Activation** Runtime

**Valid for Access Type**LTE

**Key ID** FAT 102 3381/2076

### 4.79.1 Description

The Public Warning System (PWS) feature enables warning messages regarding disasters and other emergencies, such as earthquakes and tsunamis, to be sent to the public. Warning messages are broadcast to a notification area that is based on the geographical information as specified by the warning message provider.

For more information on the Public Warning System, see Public Warning System.

### 4.79.2 Configuration

Configure and enable the feature by following the instructions in Configuring the Public Warning System.

# 4.80 QoS Based on IMSI Series

**Parameter** highest_qos_imsi

**Activation** Runtime

**Valid for Access Type** GSM, WCDMA, LTE

**Key ID** FAT 102 3381/2021

## 4.80.1 Description

The QoS Based on IMSI Series feature allows the operator to allocate resources to subscribers based on their IMSI numbers, APN, or both.

The QoS Based on IMSI Series feature consists of the following functions:

— QoS Policy Maps Based on IMSI Number Series

— QoS Profiles Based on APN

— QoS Downgrade for Gn-SGSN (GSM and WCDMA)

— QoS Downgrade for LTE

**Note:** UEs attached to the SGSN-MME before the feature is enabled are not affected. The UEs keep their original QoS policy maps. To enable the new QoS policy to take effect for the UEs, perform a large restart.

For more information, refer to Quality of Service.

## 4.80.2 Configuration

For information on prerequisites for management of licensed features, see Section 2 on page 1.

For more information on how to configure the feature, refer to the following sections:

— Configuring QoS Policy Maps Based on IMSI Number Series

— Configuring a QoS Profile Based on APN

— Configuring QoS Downgrade for GSM and WCDMA

— Configuring QoS Downgrade for LTE

For more information on how to activate the configuration changes, see Section 3 on page 2.

## 4.81 QoS Based on RNC

**Parameter** highest_qos_rnc

**Activation** Runtime

**Valid for Access Type** WCDMA

**Key ID** FAT 102 3381/2061

### 4.81.1 Description

The QoS Based on RNC feature enables the operator to set the highest QoS profiles based on the capability of the RNC.

**Note:** The RABs of PDP contexts set up before the enabling of the feature are not affected.

For more information, refer to Quality of Service

### 4.81.2 Configuration

Enable the QoS Based on RNC feature, by setting the feature state to ACTIVATED for the highest_qos_rnc parameter, using the modify_feature_state CLI command.

For more information on how to activate the configuration changes, see Section 3 on page 2.

For more information on how to configure the feature, refer to Quality of Service Management.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

## 4.82 RAN Information Management

**Parameter** rim_transfer

**Activation** Runtime

**Valid for Access Type** GSM, WCDMA, LTE

**Key ID** FAT 102 3381/2025

### 4.82.1 Description

The RIM feature allows the BSS, RNC, or eNodeB to assist an MS or a UE device at cell reselection while in packet transfer mode. This significantly reduces the

service outage time. The RIM feature supports subscribers roaming among the BSC, RNC, and eNodeB. For more information, see GSM Mobility Management and Inter-System Mobility Management.

**Note:** Both enabling and disabling the RAN Information Management (RIM) feature require the followings:

— A small restart.

— A reset of the signaling BVCs, using the action_gb_ip_nse_reset_signaling_bvc CLI command.

These steps are also required for the activation or deactivation to come into effect.

### 4.82.2 Configuration

To enable the feature, the following requirements must be fulfilled:

— MSs supporting NACC according to 3GPP.

— The BSC, RNC, and eNodeB supporting the RIM procedure.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

#### Instructions

Enable the RAN Information Management feature, by setting the feature state to `ACTIVATED` for the `rim_transfer` parameter, using the modify_feature_state CLI command.

For more information on how to activate the configuration changes, see Section 3 on page 2.

## 4.83 Real-Time Charging Control Using CAMEL

**Parameter** `camel_phase3`

**Activation** Large Restart

**Valid for Access Type** GSM, WCDMA

**Key ID** FAT 102 3381/2001

### 4.83.1 Description

Real-Time Charging Control Using CAMEL supports real-time monitoring of PDP contexts both in the HPLMN and when roaming into a visited PLMN. For more information, refer to CAMEL-Based Charging.

The large restart guarantees both that the subscription information in the SGSN-MME and HLR is identical and that the HLR is provided with the correct information for deciding how to proceed with an attach. If a `FeatureState` parameter changes from `on` to `off`, or the other way around, the list of features offered by the SGSN-MME to the HLR at attach is updated. The large restart enables the HLR to consider this update.

**Note:** This feature is only applicable for the SGSN supporting the Gn interface.

### 4.83.2 Configuration

To enable the feature, the following requirement must be fulfilled:

— The SSN 146 for CAMEL Application Part (CAP) must be configured in the SS7 stack in the SGSN-MME. For more information, see Configuring SS7-Based Interfaces.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

**Instructions**

1. Set the IMSI number series to support CAMEL. For more information, see Configuring Session and Mobility Management.
2. Enable the Real-Time Charging Control Using CAMEL feature, by setting the feature state to `ACTIVATED` for the `camel_phase3` parameter, using the modify_feature_state CLI command.

For more information on how to activate the configuration changes, see Section 3 on page 2.

## 4.84 Roaming Restrictions

The Roaming Restrictions feature includes the following functionalities, which are controlled by the same license, but can be used separately or in combination.

— Roaming Restrictions Based on IMSI Number Series

— Roaming Restrictions Based on IMEI TAC

**Note:** Roaming Restrictions Based on IMEI TAC is only applicable for LTE access.

### 4.84.1 Roaming Restrictions Based on IMSI Number Series

**Parameter** `national_roaming_restriction`

**Activation** Runtime

**Valid for Access Type**
GSM, WCDMA, LTE

**Key ID** FAT 102 3381/2007

#### 4.84.1.1 Description

The Roaming Restrictions Based on IMSI Number Series functionality enables the SGSN-MME to restrict the access to an LA or GA for certain MSs or UEs based on IMSI number series.

**Note:** UEs that were attached to the SGSN-MME before the enabling of this feature are not affected.

For more information, refer to GSM Mobility Management, WCDMA Mobility Management, and LTE Mobility Management.

This functionality was previously called the National Roaming Restriction.

#### 4.84.1.2 Configuration

To enable the functionality, the following requirement must be fulfilled:

— The Roaming Restrictions SW Feature License certificate

For information on prerequisites for management of licensed features, see Section 2 on page 1.

**Instructions**

Enable the Roaming Restrictions Based on IMSI Number Series functionality, by setting the feature state to `ACTIVATED` for the `national_roaming_restriction` parameter using the modify_feature_state CLI command.

For more information on how to activate the configuration changes, see Section 3 on page 2.

For more information on how to configure the functionality, seeConfiguring Roaming Restrictions.

For more information about related CLI commands, see Roaming Restriction (CLI).

### 4.84.2 Roaming Restrictions Based on IMEI TAC

**Parameter** `roaming_restriction_based_on_imei_tac`

**Activation** Runtime

**Valid for Access Type**LTE

**Key ID** FAT 102 3381/2100

### 4.84.2.1 Description

The Roaming Restrictions Based on IMEI TAC functionality enables the SGSN-MME to restrict the access to a GA for certain device types based on IMEI TAC or IMEI TAC SV.

For more information, see LTE Mobility Management.

### 4.84.2.2 Configuration

To enable the functionality, the following requirement must be fulfilled:

— The Roaming Restrictions SW Feature License certificate

For information on prerequisites for management of licensed features, see Section 2 on page 1.

**Instructions**

Enable the Roaming Restriction Based on IMEI TAC functionality, by setting the feature state to `ACTIVATED` for the `roaming_restriction_based_on_imei_tac` parameter using the modify_feature_state CLI command.

For more information on how to activate the configuration changes, see Section 3 on page 2.

For more information on how to configure the functionality, see Configuring Roaming Restrictions.

For more information about related CLI commands, see Roaming Restriction (CLI).

## 4.85 S3/S4 Architecture Support

**Parameter** `s3_s4_architecture_support`

**Activation** Runtime

**Valid for Access Type**
GSM, WCDMA

**Key ID** FAT 102 3381/2065

### 4.85.1 Description

The S3/S4 Architecture Support feature is based on GTPv2 protocol and introduces SGSN support for the S3, S4, S16, and S6d interfaces. This brings EPC benefits to WCDMA/GSM networks and implements a uniform IP-based architecture for all access types.

### 4.85.2 Configuration

For instructions on how to enable the feature, see Reconfiguring an SGSN to Support the S-interfaces

**Note:** When the S3/S4 Architecture Support feature is set from `on` to `off`, Ericsson recommends performing large restart to clean up PDN connections using the S4 interface immediately. Hence, the UE can quickly get data services by connecting to the GGSN.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

For more information on how to activate the configuration changes, see Section 3 on page 2.

## 4.86 Selective Equivalent PLMN

**Parameter** `equivalent_plmns`

**Activation** Runtime

**Valid for Access Type**
GSM, WCDMA, LTE

**Key ID** FAT 102 3381/2012

### 4.86.1 Description

The main purpose of Selective Equivalent PLMN is to steer the MS into selecting a PLMN network within the shared network group of networks at cell selection and cell reselection. For more information, see GSM Mobility Management, WCDMA Mobility Management, and LTE Mobility Management.

### 4.86.2 Configuration

Enable the Selective Equivalent PLMN feature, by setting the feature state to `ACTIVATED` for the `equivalent_plmns` parameter, using the modify_feature_state CLI command.

For more information on how to activate the configuration changes, see Section 3 on page 2.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

For more information on available operations for EPL, see Equivalent PLMN (CLI).

## 4.87 Selective Service Request Handling

**Parameter** `selective_service_request`

**Activation** Runtime

**Valid for Access Type** WCDMA

**Key ID** FAT 102 3381/2072

### 4.87.1 Description

The Selective Service Request Handling feature enables the SGSN to re-establish Radio Access Bearers (RABs) selectively upon the reception of downlink payload packets sent from the GGSN. In case a Service Request message is initiated from the network, for example, paging as a result of receiving downlink payload packets, the SGSN re-establishes the necessary RABs only for the actively used PDP contexts instead of re-establishing all RABs. This feature saves the scarce radio resources in the radio network and the MS. For more information, see GSM and WCDMA Session Management.

### 4.87.2 Configuration

Enable the Selective Service Request Handling feature, by setting the feature state to `ACTIVATED` for the `selective_service_request` parameter, using the modify_feature_state CLI command.

For more information on how to activate the configuration changes, see Section 3 on page 2.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

## 4.88 SGSN Pool for GSM and WCDMA

**Parameter** `sgsn_pool`

**Activation** Small Restart

**Valid for Access Type** GSM, WCDMA

**Key ID** FAT 102 3381/2018

### 4.88.1 Description

The SGSN-MMEs can be configured to work in a pool to serve the Base Station Systems (BSSs) or the Radio Network Controllers (RNCs) in the pool service areas. For more information, refer to SGSN Pool.

### 4.88.2 Configuration

To enable the feature, the following requirements must be fulfilled:

— Support in the BSC

— Support for Gb over IP

— Support preferably in the OSS

— Support in the RNC

For information on prerequisites for management of licensed features, see Section 2 on page 1.

#### Instructions

For instructions on how to enable the feature, see Migration to SGSN Pool.

## 4.89 SGSN-MME Support for MSC in Pool

| | |
|---|---|
| **Parameter** | `msc_pool_sgs` (for LTE) |
| | `msc_pool_sv` (for LTE) |
| | `msc_pool_gs` (for GSM) |
| **Activation** | Runtime |
| **Valid for Access Type** | GSM, LTE |
| **Key ID** | FAT 102 3381/2098 (SGs) |
| | FAT 102 3381/2099 (Sv) |
| | FAT 102 3381/2056 (Gs) |

### 4.89.1 Description

When the MSCs are pooled for CS services and the network is running in Network Operation Mode 1, the SGSN-MME Support for MSC in Pool feature is a prerequisite. The SGSN-MME Support for MSC in Pool feature enables load distribution of the MSs between the MSCs that belong to the pool.

To determine which MSC/VLR to contact, the SGSN-MME uses an MSC selection algorithm. The MSC selection algorithm can be the IMSI hashing algorithm or the algorithm of MSC Selection Based on NRI. For more information about the MSC selection algorithms, see SGSN-MME Support for MSC in Pool.

### 4.89.2 Configuration

To enable the feature, fulfill the requirements in Table 3.

| Access Type | Prerequisites |
|---|---|
| GSM | • Support in the BSC<br>• Support in the MSC/VLR<br>• Support for the Gs interface<br>• Support for the Combined Procedure, Gs interface feature |
| LTE | • Support in the MSC/VLR<br>• Support for the SMS over SGs feature or support for the Sv interface. |

For information on prerequisites for management of licensed features, see Section 2 on page 1.

#### Instructions

For instructions on how to configure the feature, see SGSN-MME Support for MSC in Pool.

## 4.90 Single Radio Voice Call Continuity

**Parameter** srvcc

**Activation** Runtime

**Valid for Access Type** LTE

**Key ID** FAT 102 3381/2073

### 4.90.1 Description

The Single Radio Voice Call Continuity (SRVCC) feature enables the handover of UEs from the LTE network to the WCDMA, GSM, or 1xRTT network for voice calls that are anchored in IP Multimedia Subsystem (IMS). The following SRVCC procedures are supported by the SGSN-MME:

— LTE to WCDMA with CS and PS Handover

— LTE to WCDMA with CS only

— LTE to GSM with CS only

— LTE to 1xRTT with CS only

**Note:** LTE to WCDMA with CS and PS Handover requires that the Packet Handover feature is enabled.

For LTE to WCDMA or GSM with CS only, the non-voice bearers are transferred to the PS domain in WCDMA or GSM through the Routing Area Update (RAU) procedure.

During an SRVCC handover from LTE to WCDMA or GSM, the MME selects an MSC supporting Sv that is configured on the MME or returned from the DNS query. The choice depends on the `SvMscDnsQueryEnabled` parameter setting. For more details, see SGSN-MME Support for MSC in Pool.

The SGSN-MME supports SRVCC for IMS Emergency calls to the WCDMA, GSM, and 1xRTT networks. The SGSN-MME supports SRVCC where the MSCs are pooled.

## 4.90.2 Configuration

Before enabling the feature, fulfill the following requirements:

— Support in the MSC-S

— Support in the HSS

— Support for the Sv Interface (for SRVCC procedures to GSM and WCDMA CS networks)

— Support for the S102 interface (for SRVCC procedures to the 1xRTT CS network)

— Support in the eNodeB

— Support in the UE

— Support for `Uplink S1 CDMA2000 Tunneling` and `Downlink S1 CDMA2000 Tunneling` messages over the S1-MME interface

— Support for CS Fallback to 1xRTT (for SRVCC procedures to the 1xRTT CS network). See Section 4.20 on page 28.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

### Instructions

Enable the Single Radio Voice Call Continuity feature, by setting the feature state to `ACTIVATED` for the `srvcc` parameter, using the modify_feature_state CLI command.

For more information on how to configure the SRVCC feature, see Configuring EPS Support for CS Services.

For more information on how to activate the configuration changes, see Section 3 on page 2.

## 4.91 SMS over SGs

**Parameter** `sms_over_sgs`

**Activation** Runtime

**Valid for Access Type** LTE

**Key ID** FAT 102 3381/2060

### 4.91.1 Description

The SMS over SGs feature provides a transparent transfer of SMS between the UE and the MSC/VLR through signaling relay by the SGSN-MME. The feature uses the S1-MME interface toward the UE and the SGs interface toward the MSC/VLR. The SGSN-MME does not act as a Termination Point for SMS. For more information, see EPS Support for CS Services.

### 4.91.2 Configuration

To enable the feature, the following requirements must be fulfilled:

— Support in the MSC/VLR

— Support for the SGs Interface

For information on prerequisites for management of licensed features, see Section 2 on page 1.

**Instructions**

Enable the SMS over SGs feature, by setting the feature state to `ACTIVATED` for the `sms_over_sgs` parameter, using the modify_feature_state CLI command.

For more information on how to activate the configuration changes, see Section 3 on page 2.

## 4.92 SS7 over IP (SIGTRAN)

**Parameter** `ss7_over_ip`

**Activation** Runtime

**Valid for Access Type**

GSM, WCDMA

**Key ID** FAT 102 3381/2024

### 4.92.1 Description

The SS7 over IP (SIGTRAN) feature enables configuring SS7 signaling over an IP Network. The SGSN-MME supports SS7 over IP on all SS7-based interfaces. For more information, see SS7 Description.

### 4.92.2 Configuration

To enable the feature, the following requirements must be fulfilled:

— The SS7 over IP (SIGTRAN) feature license is installed.

— Sufficient IP infrastructure is available on the physical site where the SGSN-MME is located.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

**Note:** SS7 over IP (SIGTRAN) is enabled when the license is granted. The feature cannot be enabled manually, that is, the system ignores the feature states `on` and `off`. For information on how to load a license key file, see License Management.

**Instructions**

Supplementary configuration is required for SS7 to transport IP traffic.

For more information about supplementary configuration, deactivating the feature, and deleting the SS7 over IP configuration, see Configuring SS7-Based Interfaces and Configuring IP-Based Interfaces.

## 4.93 Streaming QoS

**Parameter** `streaming_qos_class`

**Activation** Runtime

**Valid for Access Type**
GSM, WCDMA

**Key ID** FAT 102 3381/2027

### 4.93.1 Description

The Streaming QoS feature enables configuration of secured quality end-to-end in terms of Guaranteed Bit Rate for subscribers and sessions. For statistical purposes set the state of the feature to `on`. For more information, see Quality of Service.

**Note:** The Streaming QoS feature is enabled when the license is granted. The feature cannot be enabled manually, that is, the system ignores the feature states `on` and `off`, and takes only into account if the license is granted or invalid. For information on how to load a license key file, see License Management.

### 4.93.2 Configuration

To enable the feature, the following requirement must be fulfilled:

— Support in the WCDMA Systems RAN and MSs

For information on prerequisites for management of licensed features, see Section 2 on page 1.

#### Instructions

For instructions on how to configure the feature, see Configuring SS7-Based Interfaces and Configuring IP-Based Interfaces.

To deactivate the feature and deleting the SS7-over-IP configuration, see Configuring SS7-Based Interfaces and Configuring IP-Based Interfaces.

## 4.94 Subscription-Based Restrictions

The Subscription-Based Restrictions feature enables access control on the subscriber level. The licensed feature consists of the following three functions:

— ODB Support for PS Service

— ODB Support for SMS Service

— Regional Subscription

### 4.94.1 ODB Support for PS Service

**Parameter** `subscription_restriction`

**Activation** Runtime

**Valid for Access Type** GSM, WCDMA, LTE

**Key ID** FAT 102 3381/2079

#### 4.94.1.1 Description

ODB Support for PS Service enables operators to regulate access of subscribers to PS service.

The "All Packet Oriented Services Barred" Operator Determined Barring (ODB) category is supported.

For LTE, the ODB category is supported over the S6a interface. For ODB subscribers whose access to the PS services is regulated, all APNs are blocked. Operators can configure an ODB-free APN list, which allows the ODB subscribers to access the APNs that are configured in the ODB-free APN list. For more information, see LTE Mobility Management.

For GSM and WCDMA, the ODB category is supported over the Gr interface or S6d interface. For more information, see GSM and WCDMA Session Management, GSM Mobility Management, and WCDMA Mobility Management.

**Note:** ODB Support for PS Service is not applicable to the emergency service.

### 4.94.2 ODB Support for SMS Service

**Parameter** `subscription_restriction`

**Activation** Runtime

**Valid for Access Type** GSM, WCDMA

**Key ID** FAT 102 3381/2079

#### 4.94.2.1 Description

ODB Support for SMS Service enables operators to regulate access of subscribers to MO-SMS service.

The node function odb_for_sms must be enabled using the modify_node_function CLI command

With ODB Support for SMS Service, ODB for SMS service is supported over the Gr interface.

The SGSN supports the following six SMS-related ODB categories:

- All outgoing calls barred
- International outgoing calls barred
- International outgoing calls except those to the home PLMN country barred
- Interzonal outgoing calls barred
- Interzonal outgoing calls except those to the home PLMN country barred
- Interzonal outgoing calls AND international outgoing calls except those directed to the home PLMN country barred

When a subscriber sends an SMS message, the SGSN checks for ODB categories that are indicated from the HLR and stored at the SGSN. If the SMS service fits into any of the ODB categories, short message transfer of the subscriber fails.

For more details about the ODB Support for SMS Service function, see GSM Mobility Management, WCDMA Mobility Management, and SMS.

### 4.94.3 Regional Subscription

**Parameter** `regional_subscription`

**Activation** Runtime

**Valid for Access Type** LTE

**Key ID** FAT 102 3381/2085

#### 4.94.3.1 Description

The Regional Subscription enhancement defines regional subscription areas (regions) where access is either allowed or restricted for a specific subscriber. The regions are identified by regional subscription zone identities, containing zone codes (ZCs), configured for each subscriber in the HSS.

**Note:** A regional subscription restriction is not applicable to emergency services.

This enhancement is only applicable to the S6a interface.

For more information on the Regional Subscription enhancement, see LTE Mobility Management.

### 4.94.4 Configuration

For information on how to configure ODB Support for PS Service, see Configuring Session and Mobility Management.

For information on how to configure ODB Support for SMS Service, see Configuring Session and Mobility Management.

For information on how to configure Regional Subscription, see Configuring Regional Subscription.

For more information on how to activate the configuration changes, see Section 3 on page 2.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

# 4.95 Support for Non-Standardized UE

**Parameter** non_3gpp_compliant_ue

**Activation** Runtime

**Valid for Access Type**

GSM, WCDMA

**Key ID** FAT 102 3381/2050

## 4.95.1 Description

The Support for Non-Standardized UEs feature handles terminal-related faults related to non-3GPP compliance in the optional Information Elements (IEs) fields. This makes it possible to turn off optional IEs in messages without affecting the 3GPP compliant handsets, and gives the possibility to add the behavior of upcoming non-3GPP compliant MSs over time. Only faults that occur because of optional IE fields in the MSs or PC cards are handled.

The SGSN-MME can retransmit an identical message up to five times. However, if the message is not acknowledged by the MS after the number of retransmissions set by the parameter GbIuNon3GPPCompliantRetransmissionLevel (default set to three), the SGSN-MME changes the message by excluding the optional IEs.

## 4.95.2 Configuration

1. To configure which optional IE is excluded from the message, contact Ericsson Support.
2. To enable the feature, it is optional to change the default number of retransmissions to the MS, by using the modify_gb_iu CLI command. Configure the GbIuNon3GPPCompliantRetransmissionLevel parameter.
3. Enable the Support for Non-Standardized UE feature, by setting the feature state to ACTIVATED for the non_3gpp_compliant_ue parameter, using the modify_feature_state CLI command.

For more information on how to activate the configuration changes, see Section 3 on page 2.

# 4.96 Triple Access for GSM, WCDMA, and LTE

**Parameter** triple_access_lwg

**Activation** Runtime

**Valid for Access Type**
GSM, WCDMA, LTE

**Key ID** FAT 102 3381/2066

### 4.96.1 Description

The Triple Access for GSM, WCDMA, and LTE feature enables the SGSN-MME to handle GSM, WCDMA, and LTE subscribers simultaneously. An SGSN-MME provides for GSM, WCDMA, and LTE access types, dynamic capacity distribution between access types based on the actual network load. There is no need to configure the SGSN-MME to handle a fixed number of GSM, WCDMA, and LTE subscribers. For more information on extension with this feature, see Reconfiguring Access Types (GSM, WCDMA, and LTE).

**Note:** The Triple Access for GSM, WCDMA, and LTE feature is mandatory for SGSN-MMEs for GSM, WCDMA, and LTE access types.

### 4.96.2 Configuration

Enable the Triple Access for GSM, WCDMA, and LTE feature, by setting the feature state to `ACTIVATED` for the `triple_access_lwg` parameter, using the modify_feature_state CLI command.

For more information on how to activate the configuration changes, see Section 3 on page 2.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

## 4.97 UE Dual Connectivity Support

**Parameter** `dual_connectivity_support`

**Activation** Runtime

**Valid for Access Type**LTE

**Key ID** FAT 102 3381/2116

### 4.97.1 Description

The UE Dual Connectivity Support feature allows 5G New Radio (NR) to be controlled by eNodeB, and enables SGSN-MME to support dynamic radio resource switching between LTE and NR. For more information, see SGSN-MME Technical Product Description Overview.

### 4.97.2 Configuration

Enable the feature for LTE systems by setting the feature state to ACTIVATED for the dual_connectivity_support parameter, using the modify_feature_state CLI command.

For more information on how to activate the configuration changes, see Section 3 on page 2.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

## 4.98 UE Power-Saving Mode

| | |
|---|---|
| **Parameter** | psm_gsm |
| | psm_lte |
| **Activation** | Runtime |
| **Valid for Access Type** | GSM, LTE |
| **Key ID** | FAT 102 3381/2093 (GSM) |
| | FAT 102 3381/2111 (LTE |

### 4.98.1 Description

SGSN-MME supports Power Saving Mode (PSM) enabled devices, for instance M2M and IoT devices, which require longer battery life than conventional UEs. For more information, see Massive IoT.

### 4.98.2 Configuration

Enable the UE Power-Saving Mode feature for LTE Systems, by setting the feature state to ACTIVATED for the psm_lte parameter, using the modify_feature_state CLI command.

Enable the UE Power-Saving Mode feature for GSM Systems, by setting the feature state to ACTIVATED for the psm_gsm parameter, using the modify_feature_state CLI command.

For more information on how to activate the configuration changes, see Section 3 on page 2.

For information on prerequisites for management of licensed features, see Section 2 on page 1.

## 4.99 UE Signaling Control

**Parameter** `ue_signalling_control`

**Activation** Runtime

**Valid for Access Type**
GSM, WCDMA, LTE

**Key ID** FAT 102 3381/2067

### 4.99.1 Description

The UE Signaling Control feature is used for measuring and optionally controlling messages of high rates from UE devices. Measurements are performed per UE on specific message type and radio access type, according to the configuration. Control actions include ignoring same messages, rejecting requests, and detaching the UE.

For more information about the feature, see UE Signaling Control.

### 4.99.2 Configuration

This feature can be configured for Measurement Only mode or Measurement and Control mode. For information about configuring the feature, see Configuring UE Signaling Control.

## 4.100 UE Tracer

**Parameter** `ue_trace_mme`

**Activation** Runtime

**Valid for Access Type**
GSM, WCDMA, LTE

**Key ID** FAT 102 3381/2055

### 4.100.1 Description

The UE Tracer feature enables signaling messages to be traced over the specified interfaces for specific UEs. Signaling messages can also be traced by configuring a UE trace trigger to capture UEs with the specified problem. UE Tracer logs provide detailed information about signaling messages at the UE level for the traced UEs. The information is useful for identifying and understanding the network behavior caused by a specific UE. For more information about the feature, see UE Tracer.

### 4.100.2 Configuration

For information on prerequisites for management of licensed features, see Section 2 on page 1.

**Instructions**

For instructions on how to configure the feature, see Configuring UE Tracer.

## 4.101 Wi-Fi Integration

**Parameter** `wifi_ue_throughput_mobility`

**Activation** Runtime

**Valid for Access Type** LTE

**Key ID** FAT 102 3381/2087

### 4.101.1 Description

The Wi-Fi Integration feature enables the LTE network to interwork with the Wi-Fi network. The feature includes the UE Throughput Based Mobility to/from Wi-Fi functionality. For information about the UE Throughput Based Mobility to/from Wi-Fi functionality, see Wi-Fi Integration.

### 4.101.2 Configuration

For information about configuring this functionality, see Configuring Wi-Fi Integration.

# 5 Operation and Maintenance

## 5.1 Parameters

To display the parameters related to node functions and optional features, use the get_config_area -can FeaturesAndFunctions CLI command.

# 6 Compliance

For compliance information on 3GPP interfaces, see:

- SoC with 3GPP TS 24.008
- SoC with 3GPP TS 25.413
- SoC with 3GPP TS 29.060
- SoC with 3GPP TS 29.272
- SoC with 3GPP TS 29.274
- SoC with 3GPP TS 32.251
- SoC with 3GPP TS 32.298
- SoC with 3GPP TS 48.018

# Reference List

**Network License Server (NeLS) CPI Library References**

[1] Activation of NeLS Client Licenses
USER GUIDE, 6/1553-AVA 901 45/1