MME Service Configuration Mode Commands

The MME Service Configuration Mode is used to create and manage the LTE Mobility Management Entity (MME) services for the LTE/SAE network. This service works in conjunction with MME-HSS Service and eGTP Service.

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Important The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

Caution Restarting the MME service leads to termination of UE sessions at the MME, purge of subscriber data and closure of all connections towards peer nodes such as eNodeB, HSS, S-GW, etc. It may also lead to termination of other services associated with the MME. It is strongly advised to make any configuration changes that restarts the service only while in maintenance mode or at startup.

associate

Associates or disassociates supportive services and policies, such as an Evolved GPRS Tunnelling Protocol (eGTP) service, an HSS peer service, or an MME policy subscriber map with an MME service.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description

associate { { egtp-service *egtp_svc_name* **| egtp-sv-service** *egtp_sv_svc_name* **| foreign-plmn-guti-mgmt-db** *db_name* **| henbgw-mgmt-db** *db_name* **| hss-peer-service** *hss_svc_name* **| ipne-service** *ipne_svc_name* **| location-service** *location_svc_name* **| lte-emergency-profile** *profile_name* **| network-global-mme-id-mgmt-db | s102-service** *s102_svc_name* **[context** *context_name* **] | sbc-service** *sbc_svc_name* **| sctp-param-template** *template_name* **| sgs-service** *sgs_svc_name* **| sgtpc-service** *sgtpc_svc_name* **} [context** *ctx_name* **] | subscriber-map** *map_name* **| tai-mgmt-db** *database_name* **}**
no associate { egtp-service | egtp-sv-service | foreign-plmn-guti-mgmt-db | henbgw-mgmt-db | hss-peer-service | ipne-service | location-service | lte-emergency-profile | network-global-mme-id-mgmt-db | s102-service | sctp-param-template | sgs-service | sgtpc-service | subscriber-map | tai-mgmt-db }

no

Disassociates a previously associated service with this MME service.

egtp-service *egtp_svc_name*

Associates an eGTP service with MME service.

egtp_svc_name specifies the name for a pre-configured eGTP service to associate with the MME service. The eGTP service provides eGTP-C protocol interface support between EPS nodes. For more information on the eGTP service, refer to the **egtp-service** command in the *Context Configuration Mode Commands* chapter and the *eGTP Service Configuration Mode Commands* chapter.

Only one eGTP service can be associated with a service. The eGTP service should be configured prior to issuing this command.

egtp-sv-service *egtp_sv_svc_name*

Associates an eGTP Sv service with this MME service.

egtp_sv_svc_name specifies the name for a pre-configured eGTP Sv service to associate with the MME service. For more information on the eGTP Sv service, refer to the **egtp-service** command in the *Context Configuration Mode Commands* chapter.

foreign-plmn-guti-mgmt-db *db_name*

Associates a Foreign PLMN GUTI management database with this MME service.

db_name specifies the name for a pre-configured foreign PLMN GUTI management database to associate with the MME service. For more information on the Foreign PLMN GUTI management database, refer to the **foreign-plmn-guti-mgmt-db** command in the *LTE Policy Configuration Mode Commands* chapter.

Only one Foreign PLMN GUTI management database can be associated to an MME service. The Foreign PLMN GUTI management database should be configured prior to issuing this command.

Multiple MME services can be associated to the same Foreign PLMN GUTI management database.

henbgw-mgmt-db *db_name*

Important In Release 20.0, HeNBGW is not supported. This keyword must not be used in Release 20.0. For more information, contact your Cisco account representative.

Associates the specified HeNB-GW management database with the MME service.

db_name specifies the name for an LTE MME HeNB-GW Management Database to associate with the MME service as an alphanumeric string of 1 through 64 characters. This is required to support S1 HANDOVERs to Home eNodeBs connected via a HeNB-GW.

hss-peer-service *hss_svc_name*

Associates an HSS peer service with this MME service.

hss_svc_name specifies the name for a pre-configured HSS peer service to associate with the MME service as an alphanumeric string of 1 through 64 characters. The HSS peer service provides S6a and S13 interface support via the Diameter protocol between the MME and an HSS (S6a) or EIR (S13). For more information about the HSS peer service, refer to the **hss-peer-service** command in the *Context Configuration Mode Commands* chapter and the *HSS Peer Service Configuration Mode Commands* chapter.

Only one HSS peer service can be associated to a service. The HSS peer service should be configured prior to issuing this command.

ipne-service *ipne_svc_name*

Associates an IPNE service with this MME service.

ipne_svc_name must be an alphanumeric string of 1 to 63 characters to identify a pre-configured, uniquely-named IPNE service. For more information about the IPNE service, refer to the sections for the *IPNE Service Configuration Mode Commands* and the *IPNE Endpoint Configuration Mode Commands*.

location-service ***location_svc_name***

Associates a location service with this MME service. Only one location service should be associated with an MME Service.

location_svc_name specifies the name for a pre-configured location service to associate with the MME service as an alphanumeric string of 1 through 64 characters. For more information about Location Services (LCS), refer to the **location-service** command in the *Context Configuration Mode Commands* chapter and the *Location Services Configuration Mode Commands* chapter.

lte-emergency-profile ***profile_name***

Associates an LTE emergency profile with this MME service.

profile_name specifies the name for a pre-configured LTE emergency profile to associate with the MME service as an alphanumeric string of 1 through 64 characters. For more information about the LTE emergency profile, refer to the **lte-emergency-profile** command in the *LTE Policy Configuration Mode Commands* chapter and the *LTE Emergency Profile Configuration Mode Commands* chapter.

network-global-mme-id-mgmt-db

Associates the configured global MME ID management database with this MME service. The global MME ID management database is configured through the LTE Policy Configuration Mode using the **network-global-mme-id-mgmt-db** command.

s102-service ***s102_svc_name*** **[context** ***context_name*** **]**

Associates the specified S102 service that manages the S102 interface with this MME service.

s102_svc_name specifies the name for a pre-configured S102 service to associate with this MME service. Enter a string of 1 through 63 alphanumeric characters.

context *context_name* identifes the context in which the S102 service has been created and configured.

Each MME service can be associated with one unique S102 service.

The S102 service is **not** a critical parameter for the MME service. Removing this configuration will **not** restart the MME service.

For more information about the S102 service, refer to the **s102-service** command in the *Global Configuration Mode Commands* chapter and the *S102 Service Configuration Mode Commands* chapter.

sbc-service ***sbc_svc_name***

Important Beginning with Release 18.4, this keyword is only accessible or configurable if a valid SBc license key is installed. For information about obtaining such a license, contact your Cisco Representative.

Associates the specified SBc service with this MME service.

sbc_svc_name specifies the name for a pre-configured SBc service to associate with this MME service as an alphanumeric string of 1 through 63 characters.

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

The SBc service is **not** a critical parameter for the MME service. Removing this configuration will **not** restart the MME service.

For more information about the SBc service, refer to the **sbc-service** command in the *Global Configuration Mode Commands* chapter, the *SBc Service Configuration Mode Commands* chapter, and the *Cell Broadcast Center - SBc Interface* feature chapter in the *MME Administration Guide*.

sctp-param-template *template_name*

Associates a Stream Control Transmission Protocol (SCTP) parameter template with this MME service.

template_name specifies the name for a pre-configured SCTP parameter template to associate with this MME service as an alphanumeric string of 1 through 63 characters. For more information on the SCTP parameter template, refer to the **sctp-param-template** command in the *Global Configuration Mode Commands* chapter and the *SCTP Parameter Template Configuration Mode Commands* chapter.

sgs-service *sgs_svc_name*

Associates an SGs service with this MME service.

sgs_svc_name specifies the name for a pre-configured SGs service to associate with the MME service as an alphanumeric string of 1 through 64 characters. For more information on the SGs service, refer to the **sgs-service** command in the *Context Configuration Mode Commands* chapter and the *MME SGs Service Configuration Mode Commands* chapter.

sgtpc-service *sgtpc_svc_name*

Associates an SGTPC service with this MME service.

sgtpc_svc_name specifies the name for a pre-configured SGTPC service to associate with the MME service as an alphanumeric string of 1 through 64 characters.

Important When co-locating an SGSN and MME, the MME Service cannot be associated with the same SGTP service that is used by the SGSN.

For more information on the SGTPC service, refer to the **sgtp-service** command in the *Context Configuration Mode Commands* chapter and the *SGTP Service Configuration Mode Commands* chapter.

context *ctx_name*

Identifies a specific context name where the named service is configured. If this keyword is omitted, the named service must exist in the same context as the MME service.

ctx_name is name of the configured context of the named service expressed as an alphanumeric string of 1 through 63 characters that is case sensitive.

subscriber-map *map_name*

Associates this MME service with a pre-configured subscriber map.

map_name specifies the name of a pre-configured subscriber map to associate with the MME service as an alphanumeric string of 1 through 64 characters. For more information on subscriber maps, refer to the **subscriber-map** command in the *LTE Policy Configuration Mode Commands* chapter and the *LTE Subscriber Map Configuration Mode Commands* chapter.

tai-mgmt-db *database_name*

Associates this MME service with a pre-configured TAI Management Database.

database_name specifies the name of a pre-configured TAI Management Database to associate with the MME service as alphanumeric string of 1 through 64 characters. For more information on subscriber maps, refer to the **tai-mgmt-db** command in the *LTE Policy Configuration Mode Commands* chapter and the *LTE TAI Management Database Configuration Mode Commands* chapter.

Usage Guidelines

Use this command to associate a pre-configured service or policy with an MME service.

Caution This is a critical configuration. The MME service cannot be started without this configuration. Any change to this configuration will cause the MME service to be restarted. Removing or disabling this configuration will stop the MME service.

Examples

The following command associates a pre-configured eGTP service called *egtp1* in the *dst_ctx* context to an MME service:
associate egtp-service egtp1 context dst_ctx

The following command associates a pre-configured HSS peer service called *hss1* in the same context as MME service to an MME service:
associate hss-peer-service hss1

bind s1-mme

Binds the MME service to a logical IP interface serving as the S1-MME interface.

Important Before modifying this bind configuration using the **no bind s1-mme** command, we recommend that the MME Administrator use the **clear mme-service db record** command, under the Exec mode, to empty the MME records database.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description **bind s1-mme { ipv4-address** *address* **[ipv4-address** *secondary_address* **] | ipv6-address** *address* **[ipv6-address** *secondary_address* **] } [crypto-template** *name* **] [max-subscribers** *number* **]**
no bind s1-mme

no

Removes a previously configured IP address used for binding the SCTP (local bind address) to communicate with the eNodeBs using an S1-MME interface.

{ ipv4-address *address* [ipv4-address *secondary_address*] | ipv6-address *address* [ipv6-address *secondary_address*] }

Specifies the IP address for the interface configured as an S1-MME interface in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation. Optionally configure a secondary IP address for either address type.

crypto-template *name*

Specifies an existing crypto template name used when implementing IP Security (IPSec) on the S1-MME interface. *name* is an alphanumeric string of 1 through 104 characters.

max-subscribers ***number***

Specifies the maximum number of subscribers that can access this service on this interface as an integer from 0 through 8000000.

For Release 15.0, the ASR 5500 platform supports up to 10,000,000 MME UE sessions.

Usage Guidelines

Use this command to associate the MME service with a specific logical IP address that will be used for binding the SCTP socket that communicates with the eNodeB using S1AP. Only one IP address can be configured with this command for one MME service.

The MME passes the IP address during setting up the SCTP association with the eNodeB.

Caution This is a critical configuration. The MME service can not be started without this configuration. Any change to this configuration will cause the MME service to be restarted. Removing or disabling this configuration will stop the MME service.

Important Up to two IPv4 or IPv6 addresses can be configured to support SCTP multi-homing.

Examples

The following command would bind the logical IP interface with the address of *192.168.3.1* to the MME service to interact with eNodeB:
bind s1-mme ipv4-address 192.168.3.1

The following command disables a binding that was previously configured:
no bind s1-mme

csg-change-notification

This command enables or disables the Closed Subscriber Group (CSG) Information reporting (notification) mechanism on the MME. When enabled, the MME includes the CSG Information Reporting Action IE with the appropriate Action field for subscribers.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description

[default | no] csg-change-notification

default

By default, this feature is disabled. Using the **default** command prefix causes the MME to reset the configuration for this parameter to the default so that the feature is disabled.

no

Disables the feature.

Usage Guidelines

Use this command to enable or disable CSG change notification to the SGW/PGW.

By default **csg-change-notification** is disabled; the MME does not send CSG notification to the SGW/PGW.

dns

Specifes the context where the Domain Name System (DNS) client service is configured for DNS query to select an MSC, P-GW, S-GW, peer SGSN or peer MME for this MME service.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description **dns { msc | peer-mme | peer-sgsn | pgw | sgw } [context** *ctx_name* **]**
no dns { msc | peer-mme | peer-sgsn | pgw | sgw }

no

Removes a previously specified context having a DNS client service configured for DNS query to select a MSC, peer MME, peer SGSN, P-GW or S-GW with this MME service.

msc

Specifies the context where a DNS client service is configured for DNS queries for selecting a Mobile Switching Center (MSC) for SRVCC.

peer-mme

Specifies the context where a DNS client service is configured for DNS queries for selecting a peer MME.

peer-sgsn

Specifies the context where a DNS client service is configured for DNS queries for selecting a peer SGSN for inter-RAT handovers.

pgw

Specifies the context where a DNS client service is configured for DNS queries for selecting a P-GW.

sgw

Specifies the context where a DNS client service is configured for DNS queries for selecting an S-GW.

context *ctx_name*

Optionally associates the specific context name where the DNS client service is configured for this MME service. If this keyword is omitted, the DNS client service is configured to use the same context as this MME service.

ctx_name is name of the configured context of the DNS client service expressed as an alphanumeric string of 1 through 79 characters that is case sensitive.

Usage Guidelines

Use this command to specify a pre-configured context where a DNS client service is configured.

The DNS Client service configured in the specified context provides the DNS query support to locate MSCs, peer MMEs, peer-SGSNs, P-GWs, or S-GWs for this MME service. For more information on DNS Client service and support, refer to the *DNS Client Service Configuration Mode Commands* chapter.

A maximum of one context can be specified for each keyword.

Examples

The following command associates a pre-configured context *dns_ctx1* where a DNS client service is configured for DNS query to MSC for this MME service:
dns msc context dns_ctx1

The following command associates a pre-configured context *dns_ctx1* where a DNS client service is configured for DNS query to P-GW for this MME service:
dns pgw context dns_ctx1

The following command associates a pre-configured context *dns_ctx2* where a DNS client service is configured for DNS query to S-GW:
dns sgw context dns_ctx2

emm

Defines the Evolved Mobility Management timer parameters, such as timeout durations for timers and retransmission counts, for Non-Access Stratum (NAS) message retransmission in MME service.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description **emm { implicit-detach-timeout** *detach_dur* **| mobile-reachable-timeout** *mob_reach_dur* **| t3346-timeout** *t3346_dur* **| t3412-extended-timeout** *t3412_ext_dur* **| t3412-timeout** *t3412_dur* **| t3413-timeout** *t3413_dur* **| t3422-timeout** *t3422_dur* **| t3423-timeout** *t3423_dur* **| t3450-timeout** *t3450_dur* **| t3460-timeout** *t3460_dur* **| t3470-timeout** *t3470_dur* **}**
default emm { implicit-detach-timeout | mobile-reachable-timeout | t3346-timeout | t3412-extended-timeout | t3412-timeout | t3413-timeout | t3422-timeout | t3423-timeout | t3450-timeout | t3460-timeout | t3470-timeout }

default

Resets the specified timer timeout to the system default value.

implicit-detach-timeout *detach_dur*

Sets the timer timeout duration (in seconds) after which subscriber will implicitly detached from the network if there is no activity. Generally this timer value is 240 seconds (4 minutes) more than the timeout value of the T3423 timer.

This timer starts when mobile reachable timer expires while the network is in EMM-IDLE mode and ISR is activated and stops when a NAS signalling connection established.

detach_dur is an integer from 1 through 12000. Default: 3480

mobile-reachable-timeout *mob_reach_dur*

Sets the timeout timer duration (in seconds) after which reachability procedure will be discarded and reattempt starts.

mob_reach_dur is an integer from 1 through 12000. Default: 3480

t3346-timeout *t3346_dur*

Sets the EMM backoff timer duration (in seconds). If an EMM request is rejected by MME because of congestion, it shall have EMM cause as congestion (#22) and shall include back-off timer (T3346) IE. The back-off timer shall be chosen randomly and shall be 10% below or above the configured T3346 timer value.

t3346_dur is an integer from 0 through 11160 (0-186 minutes). Default: 1500 seconds (25 minutes).

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

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

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

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

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

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

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

t3412-extended-timeout *t3412_ext_dur*

Sets the extended periodic TAU timer duration (in seconds), enabling the Operator to configure longer values for the periodic TAU timer and Mobile Reachable timer. This helps the MME to reduce network load from periodic TAU signaling and to increase the time until the UE detects a potential need for changing the RAT or PLMN.

t3412_ext_dur is an integer from 0 through 1116000 (0-186 minutes). Default: 3600 seconds (60 minutes).

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

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

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

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

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

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

t3412-timeout ***t3412_dur***

Sets the timeout duration (in seconds) for the T3412 timer. This timer is used for periodic tracking area update (P-TAU). When this timer expires, the periodic tracking area updating procedure starts and the timer is set to its initial value for the next start.

This timer starts when the UE goes from EMM-CONNECTED to EMM-IDLE mode and stops when the UE enters EMM-CONNECTED mode.

t3412_dur is an integer from 1 through 11160. Default: 3240

t3413-timeout ***t3413_dur***

Sets the timeout duration (in seconds) for the T3413 timer. The timer starts when MME initiates the EPS paging procedure to the EMM entity in the network and requests the lower layer to start paging. This timer stops for the paging procedure when a response received from the UE.

t3413_dur is an integer from 1 through 20. Default: 6

t3422-timeout ***t3422_dur***

Sets the timeout duration (in seconds) for the T3422 timer. This timer starts when MME initiates the detach procedure by sending a DETACH REQUEST message to the UE and stops upon receipt of the DETACH ACCEPT message.

t3422_dur is tan integer from 1 through 20. Default: 6

t3423-timeout ***t3423_dur***

Sets the timeout duration (in seconds) for the T3423 timer. This timer starts when UE enters the EMM-DEREGISTERED state or when entering EMM-CONNECTED mode. It stops while the UE is in EMM-REGISTERED.NO-CELL-AVAILABLE state and Idle mode Signalling Reduction (ISR) is activated.

t3423_dur is an integer from 1 through 11160. Default: 3240

t3450-timeout ***t3450_dur***

Sets the timeout duration (in seconds) for the T3450 timer. This timer starts when MME initiates the Globally Unique Temporary Identifier (GUTI) reallocation procedure by sending a GUTI REALLOCATION COMMAND message to the UE and stops upon receipt of the GUTI REALLOCATION COMPLETE message.

This timer is also used for the Tracking Area update procedure.

t3450_dur is an integer from 1 through 20. Default: 6

t3460-timeout ***t3460_dur***

Sets the timeout duration (in seconds) for the T3460 timer. This timer starts when the network initiates the authentication procedure by sending an AUTHENTICATION REQUEST message to the UE and stops upon receipt of the AUTHENTICATION RESPONSE message.

t3460_dur is an integer from 1 through 20. Default: 6

t3470-timeout *t3470_dur*

Sets the timeout duration (in seconds) for the T3470 timer. The MME starts this timer when the network initiates the identification procedure by sending an IDENTITY REQUEST message to the UE and stops upon receipt of the IDENTITY RESPONSE message.

t3470_dur is an integer from 1 through 20. Default: 6

Usage Guidelines

Use this command to set EMM timers.

The following tables describe the triggers and states for timers:

Table 1: EPS Mobility Management Timers – UE Side

Timer	State	Cause of Start	Normal Stop	On Expiry
T3402	• EMM-DEREGISTERED • EMM-REGISTERED	• At attach failure and the attempt counter is equal to 5. • At tracking area updating failure and the attempt counter is equal to 5.	• ATTACH REQUEST sent • TRACKING AREA UPDATE REQUEST sent	Initiation of the attach procedure or TAU procedure
T3410	EMM-REGISTERED-INITIATED	ATTACH REQUEST sent	• ATTACH ACCEPT received • ATTACH REJECT received	Start T3411 or T3402 as described in subclause 5.5.1.2.6
T3411	• EMM-DEREGISTERED.ATTEMPTING-TO-ATTACH • EMM-REGISTERED.ATTEMPTING-TO-UPDATE	• At attach failure due to lower layer failure, T3410 timeout or attach rejected with other EMM cause values than those treated in subclause 5.5.1.2.5. • At tracking area updating failure due to lower layer failure, T3430 timeout or TAU rejected with other EMM cause values than those treated in subclause 5.5.3.2.5.	• ATTACH REQUEST sent • TRACKING AREA UPDATE REQUEST sent	Retransmission of the ATTACH REQUEST or TRACKING AREA UPDATE REQUEST

Timer	State	Cause of Start	Normal Stop	On Expiry
T3412	EMM-REGISTERED	In EMM-REGISTERED, when EMM-CONNECTED mode is left.	• When entering state EMM-DEREGISTERED or • When entering EMM-CONNECTED mode.	Initiation of the periodic TAU procedure
T3416	• EMM-REGISTERED-INITIATED • EMM-REGISTERED • EMM-DEREGISTERED-INITIATED • EMM-TRACKING-AREA-UPDATING-INITIATED • EMM-SERVICE-REQUEST-INITIATED	RAND and RES stored as a result of a UMTS authentication challenge	• SECURITY MODE COMMAND received • SERVICE REJECT received • TRACKING AREA UPDATE ACCEPT received • AUTHENTICATION REJECT received • AUTHENTICATION FAILURE sent • EMM-DEREGISTERED or EMM-NULL entered	Delete the stored RAND and RES
T3417	EMM-SERVICE-REQUEST-INITIATED	• SERVICE REQUEST sent • EXTENDED SERVICE REQUEST sent in case f and g in subclause 5.6.1.1	• Bearers have been set up • SERVICE REJECT received	Abort the procedure

Timer	State	Cause of Start	Normal Stop	On Expiry
T3417ext	EMM-SERVICE-REQUEST-INITIATED	• EXTENDED SERVICE REQUEST sent in case d in subclause 5.6.1.1 • EXTENDED SERVICE REQUEST sent in case e in subclause 5.6.1.1 and the CSFB response was set to "CS fallback accepted by the UE".	• Inter-system change from S1 mode to A/Gb mode or Iu mode is completed • Inter-system change from S1 mode to A/Gb mode or Iu mode is failed • SERVICE REJECT received	Abort the procedure
T3418	• EMM-REGISTERED-INITIATED • EMM-REGISTERED • EMM-TRACKING-AREA-UPDATING-INITIATED • EMM-DEREGISTERED-INITIATED • EMM-SERVICE-REQUEST-INITIATED	AUTHENTICATION FAILURE (EMM cause = #20 "MAC failure" or #26 "Non-EPS authentication unacceptable") sent	AUTHENTICATION REQUEST received	On first expiry, the UE should consider the network as false
T3420	• EMM-REGISTERED-INITIATED • EMM-REGISTERED • EMM-DEREGISTERED-INITIATED • EMM-TRACKING-AREA-UPDATING-INITIATED • EMM-SERVICE-REQUEST-INITIATED	AUTHENTICATION FAILURE (cause = #21 "synch failure") sent	AUTHENTICATION REQUEST received	On first expiry, the UE should consider the network as false
T3421	EMM-DEREGISTERED-INITIATED	DETACH REQUEST sent	DETACH ACCEPT received	Retransmission of DETACH REQUEST

Timer	State	Cause of Start	Normal Stop	On Expiry
T3423	EMM-REGISTERED	T3412 expires while the UE is in EMM-REGISTERED-NO-CELL-AVAILABLE and ISR is activated.	• When entering state EMM-DEREGISTERED or • When entering EMM-CONNECTED mode.	Set TIN to "P-TMSI"
T3430	EMM-TRACKING-AREA-UPDATING-INITIATED	TRACKING AREA UPDATE REQUEST sent	• TRACKING AREA UPDATE ACCEPT received • TRACKING AREA UPDATE REJECT received	Start T3411 or T3402 as described in subclause 5.5.3.2.6
T3440	• EMM-REGISTERED-INITIATED • EMM-TRACKING-AREA-UPDATING-INITIATED • EMM-DEREGISTERED-INITIATED • EMM-SERVICE-REQUEST-INITIATED • EMM-REGISTERED	• ATTACH REJECT, DETACH REQUEST, TRACKING AREA UPDATE REJECT with any of the EMM cause values #11, #12, #13, #14 or #15 • SERVICE REJECT received with any of the EMM cause values #11, #12, #13 or #15 • TRACKING AREA UPDATE ACCEPT received after the UE sent TRACKING AREA UPDATE REQUEST in EMM-IDLE mode with no "active" flag	• Signalling connection released • Bearers have been set up	Release the signalling connection and proceed as described in subclause 5.3.1.2
T3442	EMM-REGISTERED	SERVICE REJECT received with EMM cause #39	TRACKING AREA UPDATE REQUEST sent	None

Timer	State	Cause of Start	Normal Stop	On Expiry
NOTE 1: The default value of this timer is used if the network does not indicate another value in an EMM signalling procedure.				
NOTE 2: The value of this timer is provided by the network operator during the attach and tracking area updating procedures.				
NOTE 3: The value of this timer may be provided by the network in the ATTACH ACCEPT message and TRACKING AREA UPDATE ACCEPT message. The default value of this timer is identical to the value of T3412.				
NOTE 4: The value of this timer is provided by the network operator when a service request for CS fallback is rejected by the network with EMM cause #39 "CS domain temporarily not available".				

Table 2: EPS Mobility Management Timers – Network Side

Timer	State	Cause of Start	Normal Stop	On Expiry1st, 2nd, 3rd, 4th EXPIRY (NOTE 1)
T3413	EMM-REGISTERED	Paging procedure initiated	Paging procedure completed	Network dependent
T3422	EMM-DEREGISTERED-INITIATED	DETACH REQUEST sent	DETACH ACCEPT received	Retransmission of DETACH REQUEST
T3450	EMM-COMMON-PROC-INIT	• ATTACH ACCEPT sent • TRACKING AREA UPDATE ACCEPT sent with GUTI • GUTI REALLOCATION COMMAND sent	• ATTACH COMPLETE received • TRACKING AREA UPDATE COMPLETE received • GUTI REALLOCATION COMPLETE received	Retransmission of the same message type, i.e. ATTACH ACCEPT, TRACKING AREA UPDATE ACCEPT or GUTI REALLOCATION COMMAND

Timer	State	Cause of Start	Normal Stop	On Expiry1st, 2nd, 3rd, 4th EXPIRY (NOTE 1)
T3460	EMM-COMMON-PROC-INIT	• AUTHENTICATION REQUEST sent • SECURITY MODE COMMAND sent	• AUTHENTICATION RESPONSE received • AUTHENTICATION FAILURE received • SECURITY MODE COMPLETE received • SECURITY MODE REJECT received	Retransmission of the same message type, i.e. AUTHENTICATION REQUEST or SECURITY MODE COMMAND
T3470	EMM-COMMON-PROC-INIT	IDENTITY REQUEST sent	IDENTITY RESPONSE received	Retransmission of IDENTITY REQUEST
Mobile reachable timer	All except EMM-DEREGISTERED	Entering EMM-IDLE mode	NAS signalling connection established	Network dependent, but typically paging is halted on 1st expiry
Implicit detach timer	All except EMM-DEREGISTERED	The mobile reachable timer expires while the network is in EMM-IDLE mode and ISR is activated	NAS signalling connection established	Implicitly detach the UE on 1st expiry
NOTE 1: Typically, the procedures are aborted on the fifth expiry of the relevant timer. Exceptions are described in the corresponding procedure description.				
NOTE 2: The value of this timer is network dependent.				

Table 3: EPS Session Management Timers – UE Side

Timer	State	Cause of Start	Normal Stop	On Expiry1st, 2nd, 3rd, 4th EXPIRY (NOTE 1)
T3480	PROCEDURE TRANSACTION PENDING	BEARER RESOURCE ALLOCATION REQUEST sent	ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST received or MODIFY EPS BEARER CONTEXT REQUEST received or BEARER RESOURCE ALLOCATION REJECT received	Retransmission of BEARER RESOURCE ALLOCATION REQUEST
T3481	PROCEDURE TRANSACTION PENDING	BEARER RESOURCE MODIFICATION REQUEST sent	ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST received or MODIFY EPS BEARER CONTEXT REQUEST received or DEACTIVATE EPS BEARER CONTEXT REQUEST received or BEARER RESOURCE MODIFICATION REJECT received	Retransmission of BEARER RESOURCE MODIFICATION REQUEST
T3482	PROCEDURE TRANSACTION PENDING	An additional PDN connection is requested by the UE which is not combined in attach procedure	ACTIVE DEFAULT EPS BEARER CONTEXT REQUEST received or PDN CONNECTIVITY REJECT received	Retransmission of PDN CONNECTIVITY REQUEST
T3492	PROCEDURE TRANSACTION PENDING	PDN DISCONNECT REQUEST sent	DEACTIVATE EPS BEARER CONTEXT REQUEST received or PDN DISCONNECT REJECT received	Retransmission of PDN DISCONNECT REQUEST
NOTE 1: Typically, the procedures are aborted on the fifth expiry of the relevant timer. Exceptions are described in the corresponding procedure description.				

This command can be repeated to set each timer as needed.

The retransmission of all type of NAS messages can be configured through **nas-max-retransmissions** command.

Examples

The following command sets the timeout value for EPS paging procedure timer T3413 for *10* seconds.
emm t3413-timeout 10

enb-cache-timeout

Configures the amount of time that eNodeB information is stored in cache after the eNodeB terminates the connection.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description

enb-cache-timeout *min*
default enb-cache-timeout

default

Returns the command to its default value of 10.

min

Specifies the amount of time (in minutes) that the MME stores eNodeB information after the eNodeB terminates the connection. *min* is an integer value from 1 through 1440. Default: 10

Usage Guidelines

Use this command to set the amount of time the MME stores eNodeB information in cache after the eNodeB terminates the connection.

Examples

The following command sets the amount of time the MME stores eNodeB information to *15* minutes:
enb-cache-timeout 15

encryption-algorithm-lte

Configures the precedence for LTE encryption algorithms to use for security procedures through this MME service.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description **encryption-algorithm-lte priority1 { 128-eea0 | 128-eea1 | 128-eea2 } [priority2 { 128-eea0 | 128-eea1 | 128-eea2 }] [priority3 { 128-eea0 | 128-eea1 | 128-eea2 }]**
default encryption-algorithm-lte

default

Sets the default LTE encryption algorithm for security procedures with configured priority *value*. Lowest value has highest preference. Default configuration of LTE encryption algorithm is:

- priority1 with 128-eea0 encryption algorithm
- priority2 with 128-eea1 encryption algorithm
- priority3 with 128-eea2 encryption algorithm

priority1

Specifies the preference of integrity algorithm for security procedures on this MME service as priority 1.

priority2

Specifies the preference of integrity algorithm for security procedures on this MME service as priority 2.

priority3

Specifies the preference of integrity algorithm for security procedures on this MME service as priority 3.

128-eea0

Sets the Null ciphering algorithm (128-EEA0) for LTE encryption as the encryption algorithm for security procedures. Default: Enabled

128-eea1

This keyword sets the SNOW 3G synchronous stream ciphering algorithm (128-EEA1) for LTE encryption as the encryption algorithm for security procedures. SNOW 3G is a stream cipher that forms the base of the 3GPP confidentiality algorithm UEA2 and the 3GPP integrity algorithm UIA2. Default: priority2

128-eea2

Sets the Advance Encryption Standard (AES) ciphering algorithm (128-EEA2) for LTE encryption as the encryption algorithm for security procedures. Default: priority3

Usage Guidelines

Use this command to set the LTE encryption algorithms for security procedures to use with this MME service.

Caution When this command is executed, all the existing priority-to-algorithm mappings will be removed and the newly configured ones will be applicable for security procedures.

Caution Configuration of the same algorithm to multiple priorities is prohibited.

Examples

The following command sets the 128-EEA1 as the LTE encryption algorithm with priority 2 for security procedures with an MME service:
encryption-algorithm-lte priority2 128-eea1

end

Exits the current configuration mode and returns to the Exec mode.

Product All

Privilege Security Administrator, Administrator

Syntax Description **end**

Usage Guidelines Use this command to return to the Exec mode.

esm

Defines the Evolved Session Management timer parameters like timeout durations for timers and retransmission counts for the retransmission of Non-Access Stratum (NAS) messages in MME service.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description **esm { t3396-timeout** *t3396_dur* **| t3485-timeout** *t3485_dur* **| t3486-timeout** *t3486_dur* **| t3489-timeout** *t3489_dur* **| t3495-timeout** *t3495_dur* **}**
default esm { t3396-timeout | t3485-timeout | t3486-timeout | t3489-timeout | t3495-timeout }

default

Resets the specified Evolved Session Management timer timeout to the system default value.

t3396-timeout ***t3396_dur***

Sets the ESM backoff timer duration (in seconds). If an ESM request is rejected because of congestion, the reject will have ESM cause "Insufficient resources" and will include a back-off timer IE (T3396). This back-off timer is chosen randomly and will be 10% below or above the configured T3396 timer value.

t3396_dur is an integer from 0 through 11160 (0-186 minutes). Default: 1500 seconds (25 minutes).

The MME will not start any timer for SM back-off, nor store the SM back-off timer expiry time. If an SM request is received and if congestion exists, the request would be rejected based and a new random value will be sent as the ESM back-off timer value.

The MME will reject any subsequent requests from the UE targeting to the same APN based on the presence of congestion at that time and not based on the SM back-off time previously sent to the UE.

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

t3485-timeout *t3485_dur*

Sets the timeout duration (in seconds) for the T3485 timer. This timer is used by the default EPS bearer context activation procedure.

This timer starts when the MME sends an ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST message to UE and stops when receives ACTIVATE DEFAULT EPS BEARER CONTEXT ACCEPT or ACTIVATE DEFAULT EPS BEARER CONTEXT REJECT message from UE.

t3485_dur is an integer from 1 through 60. Default: 8

t3486-timeout *t3486_dur*

Sets the timeout duration (in seconds) for theT3486 timer. This timer is used by the default EPS bearer context modification procedure.

This timer starts when the MME sends a MODIFY EPS BEARER CONTEXT REQUEST message to the UE and stops when it receives a MODIFY EPS BEARER CONTEXT ACCEPT received or a MODIFY EPS BEARER CONTEXT REJECT message from UE.

t3485_dur is an integer from 1 through 60. Default: 8

t3489-timeout *t3489_dur*

Sets the timeout duration (in seconds) for the T3489 timer. This timer is used for the default EPS bearer context deactivation procedure.

This timer starts when the MME sends an ESM INFORMATION REQUEST message to the UE and stops when receives a ESM INFORMATION RESPONSE message from the UE.

t3495_dur is an integer from 1 through 60. Default: 4

t3495-timeout *t3495_dur*

Sets the timeout duration (in seconds) for the T3495 timer. This timer is used for default EPS bearer context deactivation procedure.

This timer starts when the MME sends a DEACTIVATE EPS BEARER CONTEXT REQUEST message to UE and stops when receives DEACTIVATE EPS BEARER CONTEXT ACCEPT or DEACTIVATE EPS BEARER CONTEXT REJECT message from UE.

t3495_dur is tan integer from 1 through 60. Default: 8

Usage Guidelines

Use this command to set Evolved Session Management timers.

The following tables describe the triggers and states for timers:

Table 4: EPS Session Management Timers – Network Side

Timer	State	Cause of Start	Normal Stop	On Expiry1st, 2nd, 3rd, 4th EXPIRY (NOTE 1)
T3485	BEARER CONTEXT ACTIVE PENDING	• ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST sent • ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST sent	• ACTIVATE DEFAULT EPS BEARER CONTEXT ACCEPT received or • ACTIVATE DEFAULT EPS BEARER CONTEXT REJECT received or • ACTIVATE DEDICATED EPS BEARER CONTEXT ACCEPT received or • ACTIVATE DEDICATED EPS BEARER CONTEXT REJECT received	Retransmission of the same message
T3486	BEARER CONTEXT MODIFY PENDING	MODIFY EPS BEARER CONTEXT REQUEST sent	• MODIFY EPS BEARER CONTEXT ACCEPT received or • MODIFY EPS BEARER CONTEXT REJECT received	Retransmission of MODIFY EPS BEARER CONTEXT REQUEST
T3489	PROCEDURE TRANSACTION PENDING	ESM INFORMATION REQUEST sent	ESM INFORMATION RESPONSE received	Retransmission of ESM INFORMATION REQUEST on 1st and 2nd expiry only
T3495	BEARER CONTEXT INACTIVE PENDING	DEACTIVATE EPS BEARER CONTEXT REQUEST sent	DEACTIVATE EPS BEARER CONTEXT ACCEPT received	Retransmission of DEACTIVATE EPS BEARER CONTEXT REQUEST
NOTE 1: Typically, the procedures are aborted on the fifth expiry of the relevant timer. Exceptions are described in the corresponding procedure description.				

This command can be repeated to set each timer as needed.

The retransmission of all type of NAS messages can be configured through **nas-max-retransmissions** command.

Examples

The following command sets the timeout value for the default EPS bearer context activation procedure timer (T3485) for 10 seconds.
esm t3485-timeout 10

exit

Exits the current mode and returns to the parent configuration mode.

Product All

Privilege Security Administrator, Administrator

Syntax Description **exit**

Usage Guidelines Use this command to return to the parent configuration mode.

gtpv2

Configures GTPv2 piggybacking support from the MME to the P-GW. A piggybacking flag is sent by the MME to a P-GW in the S11 "Create Session Request" message and determines whether dedicated bearer creation (Create Bearer Request) is piggybacked onto the "Create Session Response" message or not.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description

[default | no] gtpv2 piggybacking

default

Returns the command to its default setting of enabled.

no

Disables the feature.

piggybacking

Specifies that piggybacking is to be performed by the P-GW.

Usage Guidelines

Use this command to enable the sending of a piggybacking flag to the P-GW over the S11 interface requesting that the Create Bearer Request message is piggybacked on the Create Session Response message (sent from the P-GW to the MME.

Examples

The following command disables this feature:
no gtpv2 piggybacking

heuristic-paging

Enables or disables the heuristic or optimized paging feature for the service.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description **[default | no] heuristic-paging [paging-map** *paging_map_name* **]**

default

Returns the command to its default setting of disabled.

no

Disables the feature.

paging-map ***paging_map_name***

Specifies the paging-map to be associated with this MME service. This keyword is only supported in Release 14.0 and higher.

Usage Guidelin

Caution The paging profiles need to be configured prior to configuring TAI management objects (tai-mgmt-db and tai-mgmt-obj). Otherwise, the configuration would lead to high paging load in the MME node, at peak traffic time, causing service outage

Use this command to enable or disable the heuristic paging feature for the service. Also known as idle-mode paging, enabling this feature prompts the MME service to keep track of the eNodeBs to which the access terminal (AT) most commonly attaches, thus reducing the signalling otherwise associated with continuous paging.

If no paging-map is associated when this command is issued, the default heuristic paging behavior is used (as opposed to intelligent paging behavior).

Refer to the *Heuristic and Intelligent Paging* chapter in the *MME Administration Guide* for more information about this command.

Important Heuristic (optimized) Paging is a licensed feature and will not appear as a command option unless the proper licensed is installed.

ho-resource-release-timeout

Configures the timer that is started when the source MME initiates a handover.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description **ho-resource-release-timeout** *timeout*
default ho-resource-release-timeout

default

Returns the command to the default setting of 5000 milliseconds.

timeout

Specifies the time in milliseconds that the MME will hold on to bearers and E-RABs after an S1-based handover has been initiated.

timeout must be an integer from 500 through 15000.

Default: 5000.

Usage Guidelines Use this command to configure the amount of time in milliseconds that the MME will hold on to bearers and E-RABs after an S1-based handover has been initiated. When this timer expires, the source MME will send a UE Context Release to the source eNodeB. Refer to 3GPP TS 23.401 Section 5.5.1.2.2 for additional information about the use of this timer.

Examples The following command configures the timer for 10000 milliseconds (10 seconds).
ho-resource-release-timeout 10000

integrity-algorithm-lte

Configures the precedence of LTE integrity algorithms to use for security procedures through this MME service. By default the integrity algorithm is enabled on MME service and cannot be disabled.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description **integrity-algorithm-lte priority1 { 128-eia1 | 128-eia2 } [priority2 { 128-eia1 | 128-eia2 }]**
default integrity-algorithm-lte

default

Removes the preconfigured integrity algorithm and sets the default LTE integrity algorithm for security procedures. Default configuration of LTE integrity algorithm is:

- priority1 with 128-eia1 integrity algorithm
- priority2 with 128-eia2 integrity algorithm

priority1

Specifies the preference of integrity algorithm for security procedures on this MME service as priority 1.

This is the mandatory and default priority keyword.

priority2

Specifies the preference of integrity algorithm for security procedures on this MME service as priority 2.

128-eia1

This keyword sets the SNOW 3G synchronous stream ciphering algorithm (128-EIA1) for LTE integrity as the integrity algorithm for security procedures. SNOW 3G is a stream cipher that forms the base of the 3GPP confidentiality algorithm UEA2 and the 3GPP integrity algorithm UIA2. Default: priority1

128-eia2

Sets the Advance Encryption Standard (AES) ciphering algorithm (128-EIA2) for LTE integrity as the integrity algorithm for security procedures. Default: Enabled

Usage Guidelines

Use this command to set the LTE integrity algorithms for security procedures to use with this MME service.

Caution Integrity algorithm is a mandatory aspect and can not be disabled in MME service.

Caution When this command is executed, all the existing priority to algorithm mappings will be removed and the newly configured ones will be applicable for security procedures.

Caution Configuration of same algorithm to multiple priorities is prohibited.

Examples

The following command sets the AES ciphering algorithms (128-EIA2) as the LTE integrity algorithm with priority as *1* for security procedures with an MME service:
integrity-algorithm-lte priority1 128-eia2

inter-rat-nnsf

Configures an NNSF (NAS Node Selection Functionality) entry to define a list of Served MMECs (MME codes) that is indicated to the eNodeB in the S1 Setup Response. This optional configuration is used to aid the eNodeB when selecting the MME for inter-rat handovers when the MME is co-located with an SGSN.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description **inter-rat-nnsf collocated-mme plmn-id mcc** *mcc_value* **mnc** *mnc_value* **group-id** *mme_group_id* **{ mme-codes** *mmec* **| mme-code-range** *first_mme_code* **to** *last_mme_code* **}**
no inter-rat-nnsf collocated-mme plmn-id mcc *mcc_value* **mnc** *mnc_value* **group-id** *mme_group_id*

no

Removes the specified NNSF entry.

collocated-mme

Specifies that the MME is co-located with an SGSN.

plmn-id mcc *mcc_value* mnc *mnc_value*

Specifies the PLMN-ID for this MME service.

mcc *mcc_value* : Specifies the mobile country code (MCC) portion of the PLMN identifier as an integer from 100 through 999.

mnc *mnc_value* : Specifies the mobile network code (MNC) portion of the PLMN identifier as a 2- or 3-digit integer from 00 through 999.

group-id *mme_group_id*

Configures the group id for this MME service.

mme_group_id must be an integer value from 0 through 65536.

mme-codes *mmec*

Configures a list of MMEC (MME codes) to be used.

mmec: must be entered as a series of codes, each separated by a space, such as: 10 25 102 103 105. Each code must be an integer from 0 through 255.

A maximum of 16 MME Codes are allowed to be configured per inter-rat-nnsf entry.

mme-code-range *first_mme_code* to *last_mme_code*

Configures a range of MMEC (MME codes) to be used. Identify an unlimited number of MME codes, for a particular PLMN-ID and Group-ID combination, as part of a range of MME codes.

first_mme_code: must be the first MME code in the range and it must be an integer from 0 through 255.

last_mme_code: must be the last MME code in the range and it must be an integer from 0 through 255 and it must be an integer greater than the value entered for the *first_mme_code*.

Usage Guidelines

Use this command to indicate a list of served MMECs, in addition to the one assigned to the MME service. The complete list shall be notified to the eNodeB as Served MMECs in the S1 Setup Response. This would aid the eNodeB in selecting a co-located MME during 2G/3G to 4G handovers.

When a UE moves from 2G/3G to 4G, selecting a co-located MME is not possible without some explicit configuration. In this scenario, the entire second Most-Significant-Byte of P-TMSI is copied into the MME-Code (MMEC) field. Depending on the NRI length, this could result in 'n' different MMEC values for the same NRI value. For example:

- NRI length = 6 bits
- NRI value = 5 (Binary 00 0101)
- Possible MMECs: Binary 00 0101 xx -> {20, 21, 22, 23}

Selecting a co-located MME is only possible if the eNodeB knows that any UE meant for the above set of MMECs should be directed to a given MME. This command enables the operator to specify MMECs that can possibly be mapped from a given NRI value.

A maximum of 16 MME Codes are allowed to be configured per inter-rat-nnsf entry. This allows 4 SGSNs with NRI length of 6, or 2 SGSNs with NRI length of 5. If more than 16 MMECs are required, an alternative is to pick a dummy MME-Group-ID value and create a new nnsf-entry. The Serving MME-Group-ID could also be used for this purpose as MME-Group-Id has no significance during MME node selection.

A Maximum of 32 inter-rat-nnsf entries are allowed. Regardless of the maximum entries configured, the maximum limits placed by S1AP stack take precedence. For example, if the number of plmns configured under 'network-sharing' and 'inter-rat-nnsf' exceeds the maxnoofPLMNsPerMME(32) limit set by S1AP-S1-Setup-Response, then inter-rat-nnsf entries that exceed the limit(32) do not get included in the S1 Setup Response message.

Examples

For NRI length = 6; NRI Value = 10 (Binary: 00 1010), when a UE moves from 2G/3G to 4G and maps MME Code (8 bits) from P-TMSI, the MME Code value could be:

- Binary: 00 1010 xx, where xx can be binary 10 or 01 or 00 or 11
- Decimal: 40 or 41 or 42 or 43

So, all of the above values should be configured as MMECs as part of **inter-rat-nnsf**, as follows:

inter-rat-nnsf collocated-mme plmn-id mcc 121 mnc 102 mme-id group-id 32000 mme-codes 40 41 42 43

When updating an existing NNSF entry, any new MMECs must be included with the existing MMECs. For example, to add additional MMECs (48 49 50 51) to the above command, enter the entire command again as follows:

inter-rat-nnsf collocated-mme plmn-id mcc 121 mnc 102 mme-id group-id 32000 mme-codes 40 41 42 43 48 49 50 51

isda-guard-timeout

Sets the number of seconds for the Insert Subscription Data Answer (ISDA) guard timer. The time the MME waits for current location information for the UE. If the current location is not learned before expiry, because there is no paging response or location reporting control from the eNB, then the MME sends the ISDA with the last-known location upon expiry of this timer.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description

[no] isda-guard-timeout *seconds*

no

Disables any configuration for this timer and resets the wait time to the default of 25 seconds.

seconds

Enter an integer from 1 to 100.

Usage Guidelines

With this command, the operator can configure the ISDA guard timer to any value from 1 to 100 seconds. Upon expiry of this wait timer, the MME sends the ISDA with the last-known location of the UE if the MME receives the Insert Subscriber Data Response (ISDR) with both the location flags set (current and last-known locations). Only when the ISDR is received, with both flags set, is the ISDA guard timer started. In situations where the MME receives the ISDR with only the last-known location flag set, then the MME immediately sends the ISDA with location information - no delay and this timer is not started even if configured.

When the ISDA guard timer expires, the paging procedure does not stop until the page timer expires but the MME ignores the paging timer and sends the ISDA with the last-known location if the ISDR was received with both location flags set and the UE is in EMM-idle mode.

While the MME is serving the ISDR (where both location flags are set) from the HSS, if the HSS tries to send another similar request then the MME responds to the HSS with DIAMETER_UNABLE_TO_COMPLY.

This timer is separate from the paging timer and configuration of the ISDA guard timer can reduce the overall delay before sending the ISDA.

Examples

Instruct the MME to wait *10* seconds before sending the ISDA with the last-known location of the UE:
isda-guard-timeout 10

isr-capability

Enables or disables the Idle-mode Signaling Reduction (ISR) feature on the MME service.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description **[no | default] isr-capability**

default

Sets the ISR feature to the default setting (disabled) on MME service.

no

Disables the ISR feature on MME service.

Usage Guidelines Use this command to enable or disable the ISR feature on the MME service. When enabled, the MME can perform ISR functions with a peer SGSN which also supports ISR.

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

Important This functionality is a license-controlled feature. A valid feature license must be installed to enable Idle-mode Signaling Reduction.

legacy-tai-list-encoding

Using this command instructs the MME to override the default behavior (described in *Usage* section below) and enables the MME to use "010" encoding value for the Tracking Area Identity (TAI) list IE for TAIs belonging to different PLMNs.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description

[no] legacy-tai-list-encoding

no

Disables the use of "010" encoding value for the TAI list IE for TAIs belonging to different PLMNs and returns the MME to using the TAI list value encoding based on PLMN and TAC values of TAI entries, the default behavior.

Usage Guidelines

The operator can use this command to configure the encoding of TAI list values to "010" irrespective of PLMN and TAI values, which overrides the default behavior (for releases 17.4 and forward). This commnd ensures backward compatibility with previous releases.

If this command is not used, or the **no** command prefix is used, then the MME uses the default function and encodes the TAI list IE value per the 3GPP TS 24.301. The default behavior has the MME automatically encode "000", "001", or "010" depending upon the TAC values and PLMN configuration so that the TAI list value for the IE is based on the list of Tics belonging to one PLMN, with consecutive or non-consecutive TAC values configured in the TAI entries.

Examples

Use the following command to override the MME's default behavior and to encode TAI list values to "010":
legacy-tai-list-encoding

local-cause-code-mapping apn-mismatch

Configures the reject cause code to send to a UE when an APN mismatch occurs.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description **local-cause-code-mapping apn-mismatch emm-cause-code { eps-service-not-allowed-in-this-plmn | esm-failure esm-cause-code unknown-apn | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }**
default local-cause-code-mapping apn-mismatch

default local-cause-code-mapping apn-mismatch

Returns the cause code mapping to its default value: **esm-failure esm-cause-code unknown-apn**.

apn-mismatch emm-cause-code { eps-service-not-allowed-in-this-plmn | esm-failure esm-cause-code unknown-apn | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }

Specifies the EPS Mobility Management (EMM) cause code to return when an APN mismatch occurs.

- **eps-service-not-allowed-in-this-plmn**
- **esm-failure esm-cause-code unknown-apn** - Default.

  For the **esm-failure** cause code only, the **unknown-apn** ESM code is also reported to the UE.
- **no-suitable-cell-in-tracking-area**
- **plmn-not-allowed**
- **roaming-not-allowed-in-this-tracking-area**
- **tracking-area-not-allowed**

Use this command to configure the cause code returned to a UE when an APN mismatch occurs, such as when an APN is present in the HSS subscription but the HSS subscription for this IMSI has other APNs present in the subscription. By default, the MME sends the UE the **#23 - ESM Failure** cause code for this condition.

If a condition is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the **local-cause-code-mapping** command in the call-control-profile configuration mode. This command is described in the *Call Control Profile Configuration Mode Commands* chapter.

Examples

The following command maps the "PLMN not allowed" cause code to the APN mismatch condition:
local-cause-code-mapping apn-mismatch emm-cause-code plmn-not-allowed

local-cause-code-mapping apn-not-subscribed

Gives the operator the option to specify the local cause-code mapping when the UE-requested APN is not subscribed.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description

local-cause-code-mapping apn-not-subscribed esm-cause-code requested-service-option-not-subscribed default local-cause-code-mapping apn-not-subscribed

default

Returns the local cause code mapping to the default of #27 (Unknown or Missing APN).

Usage Guidelines

The operator can specify "Requested-Option-Not-Subscribed" cause code value #33 will be sent in the Reject message when the PDN Connectivity Request is rejected because no subscription is found. If the command option is not configured, then by default the MME uses the cause code value #27 (Unknown or Missing APN) in standalone PDN Connectivity Reject message when the UE-requested APN is not subscribed.

Examples

The following instructs the MME to use cause code #33 ("Requested-Option-Not-Subscribed") in place of the default #27 (Unknown or Missing APN):.
local-cause-code-mapping apn-not-subscribed esm-cause-code requested-service-option-not-subscribed

local-cause-code-mapping apn-not-supported-in-plmn-rat

This command maps the operator-preferred ESM/EMM cause code to be sent in Activation Reject messages in place of the standard 3GPP Release 11 rejection cause #66 when activation of the requested APN is not supported in current RAT and PLMN combination.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description **local-cause-code-mapping apn-not-supported-in-plmn-rat { { emm-cause-code** *emm_cause_number* **esm-cause-code** *esm_cause_number* **[attach] [tau] } | esm-cause** *esm_cause_code* **esm-proc }**
default local-cause-code-mapping apn-not-supported-in-plmn-rat [attach | esm-proc | tau]

default

Returns the cause code mapping to its default values. The default cause code values for Attach procedures are emm-cause-code 19 and esm-cause-code 66. The default cause code values for TAU procedures are emm-cause-code 15 and esm-cause-code 66 respectively. The default cause code for ESM procedure is 66.

apn-not-supported-in-plmn-rat

The keyword **apn-not-supported-in-plmn-rat** specifies that the cause codes to be used for a rejection due to the requested APN not being supported in the current RAT and PLMN combination are those that are mapped in the configuration.

emm-cause-code ***emm_cause_number*** **esm-cause-code** ***esm_cause_number*** **[attach] [tau]**

MME only.

The keyword **emm-cause-code** configures the operator-preferred EMM cause code to be used if a NAS Request is rejected due to this configuration.

- *emm_cause_number* specifies the EMM code replacement integer. The system accepts a value in the range 0 through 255, however, the standards-compliant valid values are in the range 2 through 111.

- **esm-cause-code** configures the operator-preferred ESM cause code to be used if a NAS Request is rejected due to this configuration.
- *esm_cause_number* specifies the ESM code replacement integer. The system accepts a value in the range 0 through 255, however, the standards-compliant valid values are in the range 8 through 112.
- The **attach** keyword filter instructs the MME to use the mapped replacement cause code if an Attach procedure is rejected due to the noted APN not supported error condition.
- The **tau** keyword filter instructs the MME to use the mapped replacement cause code if an TAU procedure is rejected due to the noted APN not supported error condition.

esm-cause-code *esm_cause_number* esm-proc

MME only.

esm-cause-code configures the operator-preferred ESM cause code to be used if a bearer management Request is rejected due to this configuration.

- *esm_cause_number* specifies the ESM cause code replacement integer in the range 0 through 255.
- The **esm-proc** keyword filter instructs the MME to use the mapped replacement cause code if an ESM procedure is rejected due to the noted APN not supported error condition.

Usage Guidelines

This command is used to remap the ESM and EMM cause codes sent in activate rejections (due to APN not supported) to operator desired ESM or EMM cause codes. The default cause code values for Attach procedures are emm-cause-code 19 and esm-cause-code 66. The default cause code values for TAU procedures are emm-cause-code 15 and esm-cause-code 66. The default cause code for esm-proc is 66.

Examples

The following command is used to remap cause code #66 to cause code #20, this cause code will be sent if a bearer management request is rejected.
local-cause-code-mapping apn-not-supported-in-plmn-rat esm-cause-code 20 esm-proc

local-cause-code-mapping auth-failure

Configures the reject cause code to send to a UE when an authentication failure occurs.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description **local-cause-code-mapping auth-failure emm-cause-code { eps-service-not-allowed-in-this-plmn | illegal-ms | network-failure | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }**
default local-cause-code-mapping auth-failure

default local-cause-code-mapping auth-failure

Returns the cause code mapping to its default value: **illegal-ms**.

auth-failure emm-cause-code { eps-service-not-allowed-in-this-plmn | network-failure | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }

Specifies the EPS Mobility Management (EMM) cause code to return when an authentication failure occurs.

- **eps-service-not-allowed-in-this-plmn**
- **illegal-ms**
- **network-failure**
- **no-suitable-cell-in-tracking-area**
- **plmn-not-allowed**
- **roaming-not-allowed-in-this-tracking-area**
- **tracking-area-not-allowed**

Use this command to configure the cause code returned to a UE when an authentication failure occurs. By default, the MME sends the UE the **#3 - Illegal MS** cause code when encountering a context transfer failure from an MME.

This condition occurs for TAU and ATTACH procedures in the following cases:

- The Authentication response from the UE does not match the expected value in the MME.
- Security Mode Reject is send by the UE.
- The UE responds to any identity request with a different type of identity (ie, the MME could query for IMSI and the UE responds with IMEI).

The following are not considered for the authentication failure condition:

- HSS returning a result code other than SUCCESS.
- HSS not available.
- EIR failures.
- UE not responding to requests.

If a cause code mapping is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the **local-cause-code-mapping** command in the call-control-profile configuration mode. This command is described in the *Call Control Profile Configuration Mode Commands* chapter.

Examples

The following command maps the "network-failure" cause code to the authentication failure condition:

local-cause-code-mapping auth-failure emm-cause-code network-failure

local-cause-code-mapping congestion

Configures the reject cause code to send to a UE when a procedure fails due to a congestion condition.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description **local-cause-code-mapping congestion emm-cause-code { congestion [esm-cause-code { congestion | insufficient-resources | service-option-temporarily-out-of-order }] | eps-service-not-allowed-in-this-plmn | network failure | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }**
default local-cause-code-mapping congestion

default local-cause-code-mapping congestion

Returns the cause code mapping to its default value: **emm-cause congestion esm-cause congestion**.

congestion emm-cause { congestion [esm-cause-code { congestion | insufficient-resources | service-option-temporarily-out-of-order }] | eps-service-not-allowed-in-this-plmn | network failure | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }

Specifies the EPS Mobility Management (EMM) cause code to return when a UE requests access when the system is exceeding any of its congestion control thresholds.

- **congestion** - Default
- **eps-service-not-allowed-in-this-plmn**
- **network-failure**
- **no-suitable-cell-in-tracking-area**
- **plmn-not-allowed**
- **roaming-not-allowed-in-this-tracking-area**
- **tracking-area-not-allowed**

esm-cause-code { congestion | insufficient-resources | service-option-temporarily-out-of-order }

Specifies the EPS Session Management (ESM) cause code to return when a UE requests access when the system is exceeding any of its congestion control thresholds.

- **congestion** - Default
- **insufficient-resources**
- **service-option-temporarily-out-of-order**

Use this command to configure the cause code returned to a UE when a UE procedure fails due to a congestion condition on the MME. By default, the MME sends the UE the **#22 - Congestion**EMM cause code and ESM cause code when encountering congestion.

If a condition is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the **local-cause-code-mapping** command in the call-control-profile configuration mode. This command is described in the *Call Control Profile Configuration Mode Commands* chapter.

Examples

The following command maps the "network failure" cause code to the congestion event:
local-cause-code-mapping congestion emm-cause-code network-failure

local-cause-code-mapping ctxt-xfer-fail-mme

Configures the reject cause code to send to a UE when a UE context transfer failure from a peer MME occurs.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description **local-cause-code-mapping ctxt-xfer-fail-mme emm-cause-code { eps-service-not-allowed-in-this-plmn | network-failure | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed | unknown-ue-context }**
default local-cause-code-mapping ctxt-xfer-fail-mme

default local-cause-code-mapping ctxt-xfer-fail-mme

Returns the cause code mapping to its default value:**unknown-ue-context**.

ctxt-xfer-fail-mme emm-cause-code { eps-service-not-allowed-in-this-plmn | network-failure | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed | unknown-ue-context }

Specifies the EPS Mobility Management (EMM) cause code to return when a UE context transfer failure from an old MME occurs.

- **eps-service-not-allowed-in-this-plmn**
- **network-failure**
- **no-suitable-cell-in-tracking-area**
- **plmn-not-allowed**
- **roaming-not-allowed-in-this-tracking-area**
- **tracking-area-not-allowed**
- **unknown-ue-context** - Default

Use this command to configure the cause code returned to a UE when a UE context transfer failure from a peer MME occurs. By default, the MME sends the UE the **#9 - MS identity cannot be derived by the network** cause code for this condition.

After the peer node has been identified, the MME sends a Context Request to the peer node. If the peer node is an MME, and if the context transfer procedure fails, this condition is detected.

If a cause code mapping is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the **local-cause-code-mapping** command in the call-control-profile configuration mode. This command is described in the *Call Control Profile Configuration Mode Commands* chapter.

Examples

The following command maps the "network-failure" cause code to the context transfer failure from MME condition:

local-cause-code-mapping ctxt-xfer-fail-mme emm-cause-code network-failure

local-cause-code-mapping ctxt-xfer-fail-sgsn

Configures the reject cause code to send to a UE when a UE context transfer failure from a peer SGSN occurs.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description **local-cause-code-mapping ctxt-xfer-fail-sgsn emm-cause-code { eps-service-not-allowed-in-this-plmn | network-failure | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed | unknown-ue-context } default local-cause-code-mapping ctxt-xfer-fail-sgsn**

default local-cause-code-mapping ctxt-xfer-fail-sgsn

Returns the cause code mapping to its default value:**unknown-ue-context**.

ctxt-xfer-fail-sgsn emm-cause-code { eps-service-not-allowed-in-this-plmn | network-failure | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed | unknown-ue-context }

Specifies the EPS Mobility Management (EMM) cause code to return when a UE context transfer failure from an old SGSN occurs.

- **eps-service-not-allowed-in-this-plmn**
- **network-failure**
- **no-suitable-cell-in-tracking-area**
- **plmn-not-allowed**
- **roaming-not-allowed-in-this-tracking-area**
- **tracking-area-not-allowed**
- **unknown-ue-context** - Default

Use this command to configure the cause code returned to a UE when a UE context transfer failure from a peer SGSN occurs. By default, the MME sends the UE the **#9 - MS identity cannot be derived by the network** cause code when encountering this condition.

After the peer node has been identified, the MME sends a Context Request to the peer node. If the peer node is an SGSN, and if the context transfer procedure fails, this condition is detected.

If a cause code mapping is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the **local-cause-code-mapping** command in the call-control-profile configuration mode. This command is described in the *Call Control Profile Configuration Mode Commands* chapter.

Examples

The following command maps the "network-failure" cause code to the context transfer failure from SGSN condition:

local-cause-code-mapping ctxt-xfer-fail-sgsn emm-cause-code network-failure

local-cause-code-mapping gw-unreachable

Configures the reject cause code to send to a UE when a gateway (S-GW or P-GW) does not respond during an EMM procedure.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description **local-cause-code-mapping gw-unreachable emm-cause-code { eps-service-not-allowed-in-this-plmn | network-failure | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed } [attach [tau] | tau [attach]] | { no-bearers-active tau }**
default local-cause-code-mapping gw-unreachable [attach | tau]

default local-cause-code-mapping gw-unreachable [attach | tau]

Returns the cause code mapping to its default value: **#19 - ESM Failure** cause code for Attach procedures, and **no-bearers-active**- #40 - NO-EPS-BEARER-CONTEXT-ACTIVATED for TAU procedures.

gw-unreachable emm-cause-code { eps-service-not-allowed-in-this-plmn | network-failure | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }

Specifies the EPS Mobility Management (EMM) cause code to return when a gateway does not respond.

- **eps-service-not-allowed-in-this-plmn**
- **network-failure**
- **no-bearers-active**
- **no-suitable-cell-in-tracking-area**
- **plmn-not-allowed**
- **roaming-not-allowed-in-this-tracking-area**
- **tracking-area-not-allowed**

[attach [tau] | tau [attach]] | { no-bearers-active tau }

Optionally, the MME can return separate cause codes for Attach procedures and TAU procedures. This capability is available for any of the above EMM cause codes except **no-bearers-active**, which can only be defined for TAU procedures.

Use this command to configure the cause code returned to a UE when a gateway does not respond. By default, the MME sends the UE the **#19 - ESM Failure** cause code when encountering this condition.

Defaults:

Prior to StarOS 15.0 MR5, the MME sends the UE the **#19 - ESM Failure** cause code when encountering this condition.

In StarOS 15.0 MR5 and higher releases, the MME sends the UE the **#19 - ESM Failure** cause code for Attach procedures, and **#40 - NO-EPS-BEARER-CONTEXT-ACTIVATED** for TAU procedures.

If a cause code mapping is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the **local-cause-code-mapping** command in the call-control-profile configuration mode. This command is described in the *Call Control Profile Configuration Mode Commands* chapter.

Examples

The following command maps the "network-failure" cause code to the gateway unreachable condition:

local-cause-code-mapping gw-unreachable emm-cause-code network-failure

local-cause-code-mapping hss-unavailable

Configures the reject cause code to send to a UE when the HSS does not respond.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description **local-cause-code-mapping hss-unavailable emm-cause-code { eps-service-not-allowed-in-this-plmn | network-failure | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }**
default local-cause-code-mapping hss-unavailable

default local-cause-code-mapping hss-unavailable

Returns the cause code mapping to its default value:

hss-unavailable emm-cause-code { eps-service-not-allowed-in-this-plmn | network-failure | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }

Specifies the EPS Mobility Management (EMM) cause code to return when the HSS does not respond.

- **eps-service-not-allowed-in-this-plmn**
- **network-failure** - Default
- **no-suitable-cell-in-tracking-area**
- **plmn-not-allowed**
- **roaming-not-allowed-in-this-tracking-area**
- **tracking-area-not-allowed**

Use this command to configure the cause code returned to a UE when the HSS does not respond. By default, the MME sends the UE the **#17 - Network failure** cause code when encountering this condition.

This condition is detected in the following cases:

- HSS resolution fails in the MME.
- HSS does not respond in time.

The cause code configured for this condition will be signaled in TAU and ATTACH REJECT messages.

If a cause code mapping is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the **local-cause-code-mapping** command in the call-control-profile configuration mode. This command is described in the *Call Control Profile Configuration Mode Commands* chapter.

Examples

The following command maps the "tracking-area-not-allowed" cause code to the HSS unavailable condition:

local-cause-code-mapping hss-unavailable emm-cause-code tracking-area-not-allowed

local-cause-code-mapping newcall-policy-restrict

Configures the EPS Mobility Management (EMM) reject cause code to send to a UE when a UE requests access but the call control profile has set the call disposition to reject.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description **local-cause-code-mapping newcall-policy-restrict emm-cause-code { congestion | eps-service-not-allowed-in-this-plmn | network-failure | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed } default local-cause-code-mapping newcall-policy-restrict**

default local-cause-code-mapping newcall-policy-restrict

Returns the cause code mapping to its default value: **congestion**.

newcall-policy-restrict emm-cause-code ***emm_cause_code***

Specifies the EPS Mobility Management (EMM) cause code to return when a UE requests access but the call control profile has set the call disposition to reject.

emm_cause_code must be one of the following options:

- **congestion** - Default.
- **eps-service-not-allowed-in-this-plmn**
- **network-failure**
- **no-suitable-cell-in-tracking-area**
- **plmn-not-allowed**
- **roaming-not-allowed-in-this-tracking-area**
- **tracking-area-not-allowed**

Usage Guidelines Use this command to configure the cause code returned to a UE when a UE procedure fails, such as when the UE requests access to a restricted zone. By default, the MME sends the UE the **#22 - Congestion** cause code when encountering this condtion.

Examples The following command sets the "network-failure" cause code for newcall-policy-restrict calls:
local-cause-code-mapping newcall-policy-restrict emm-cause-code network-failure

local-cause-code-mapping no-active-bearers

Configures the reject cause code to send to a UE when the context received from a peer SGSN (during a TAU procedure) does not contain any active PDP contexts.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description **local-cause-code-mapping no-active-bearers emm-cause-code { eps-service-not-allowed-in-this-plmn | network-failure | no-bearers-active | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }**
default local-cause-code-mapping no-active-bearers

default local-cause-code-mapping no-active-bearers

Returns the cause code mapping to its default value: **no-bearers-active**.

no-active-bearers emm-cause-code { eps-service-not-allowed-in-this-plmn | network-failure | no-bearers-active | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }

Specifies the EPS Mobility Management (EMM) cause code to return when no active PDP context exists.

- **eps-service-not-allowed-in-this-plmn**
- **network-failure**
- **no-bearers-active** - Default
- **no-suitable-cell-in-tracking-area**
- **plmn-not-allowed**
- **roaming-not-allowed-in-this-tracking-area**
- **tracking-area-not-allowed**

Use this command to configure the cause code returned to a UE when the context received from a peer SGSN (during a TAU procedure) does not contain any active PDP contexts. By default, the MME sends the UE the **#40 - No PDP context activated** cause code when encountering this condition.

If a cause code mapping is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the **local-cause-code-mapping** command in the call-control-profile configuration mode. This command is described in the *Call Control Profile Configuration Mode Commands* chapter.

Examples

The following command maps the "plmn-not-allowed" cause code to the no active bearer condition:

local-cause-code-mapping no-active-bearers emm-cause-code plmn-not-allowed

local-cause-code-mapping peer-node-unknown

Configures the reject cause code to send to a UE when peer node resolution is not successful.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description **local-cause-code-mapping peer-node-unknown emm-cause-code { eps-service-not-allowed-in-this-plmn | network-failure | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }**
default local-cause-code-mapping peer-node-unknown

default local-cause-code-mapping peer-node-unknown

Returns the cause code mapping to its default value: **unknown-ue-context**

peer-node-unknown emm-cause-code { eps-service-not-allowed-in-this-plmn | network-failure | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }

Specifies the EPS Mobility Management (EMM) cause code to return when the peer node is not known.

- **eps-service-not-allowed-in-this-plmn**
- **network-failure**
- **no-suitable-cell-in-tracking-area**
- **plmn-not-allowed**
- **roaming-not-allowed-in-this-tracking-area**
- **tracking-area-not-allowed**
- **unknown-ue-context** - Default

Use this command to configure the cause code returned to a UE when peer node resolution is not successful. By default, the MME sends the UE the **#9 - MS identity cannot be derived by the network** cause code when encountering this condition.

During processing of a TAU Request, the resolution of a peer MME that had allocated the temporary identity that is signaled to the UE takes several steps in the MME. This resolution can be done based on DNS or based on local configuration. This condition occurs when all mechanisms for peer node resolution are done with no success.

If a cause code mapping is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the **local-cause-code-mapping** command in the call-control-profile configuration mode. This command is described in the *Call Control Profile Configuration Mode Commands* chapter.

Examples

The following command maps the "plmn-not-allowed" cause code to the peer node unknown condition:

local-cause-code-mapping peer-node-unknown emm-cause-code plmn-not-allowed

local-cause-code-mapping pgw-selection-failure

Configures the reject cause code to send to a UE when a failure occurs during P-GW selection.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description **local-cause-code-mapping pgw-selection-failure emm-cause-code { eps-service-not-allowed-in-this-plmn | network-failure | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }**
default local-cause-code-mapping pgw-selection-failure

default local-cause-code-mapping pgw-selection-failure

Returns the cause code mapping to its default value: **network-failure**.

pgw-selection-failure emm-cause-code { eps-service-not-allowed-in-this-plmn | network-failure | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }

Specifies the EPS Mobility Management (EMM) cause code to return when a failure occurs during P-GW selection.

- **eps-service-not-allowed-in-this-plmn**
- **network-failure** - Default
- **no-suitable-cell-in-tracking-area**
- **plmn-not-allowed**
- **roaming-not-allowed-in-this-tracking-area**
- **tracking-area-not-allowed**

Use this command to configure the cause code returned to a UE when a failure occurs during P-GW selection. By default, the MME sends the UE the **#17 - Network failure** cause code when encountering this condition.

If a cause code mapping is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the **local-cause-code-mapping** command in the call-control-profile configuration mode. This command is described in the *Call Control Profile Configuration Mode Commands* chapter.

Examples

The following command maps the "plmn-not-allowed" cause code to the P-GW selection failure condition:

local-cause-code-mapping pgw-selection-failure emm-cause-code plmn-not-allowed

local-cause-code-mapping restricted-zone-code

Configures the reject cause code to send to a UE when a procedure fails.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description **local-cause-code-mapping restricted-zone-code emm-cause-code { eps-service-not-allowed-in-this-plmn | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }**
default local-cause-code-mapping restricted-zone-code

default local-cause-code-mapping restricted-zone-code

Returns the cause code mapping to its default value: **no-suitable-cell-in-tracking-area**.

restricted-zone-code emm-cause-code *emm_cause_code*

Specifies the EPS Mobility Management (EMM) cause code to return when a UE requests access to a restricted zone.

emm_cause_code must be one of the following options:

- **eps-service-not-allowed-in-this-plmn**
- **no-suitable-cell-in-tracking-area** - Default.
- **plmn-not-allowed**
- **roaming-not-allowed-in-this-tracking-area**
- **tracking-area-not-allowed**

Use this command to configure the cause code returned to a UE when a UE procedure fails, such as when the UE requests access to a restricted zone. By default, the MME sends the UE the **#15 - No Suitable Cells in Tracking Area** cause code when encountering this condition.

If a condition is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the **local-cause-code-mapping** command in the call-control-profile configuration mode. This command is described in the *Call Control Profile Configuration Mode Commands* chapter.

Examples

The following command maps the "PLMN not allowed" cause code to the restricted zone code event:
local-cause-code-mapping restricted-zone-code emm-cause-code plmn-not-allowed

local-cause-code-mapping sgw-selection-failure

Configures the reject cause code to send to a UE when a failure occurs during S-GW selection.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description **local-cause-code-mapping sgw-selection-failure emm-cause-code { eps-service-not-allowed-in-this-plmn | network-failure | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }**
default local-cause-code-mapping sgw-selection-failure

default local-cause-code-mapping sgw-selection-failure

Returns the cause code mapping to its default value: **network-failure**.

sgw-selection-failure emm-cause-code { eps-service-not-allowed-in-this-plmn | network-failure | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }

Specifies the EPS Mobility Management (EMM) cause code to return when a failure occurs during S-GW selection.

- **eps-service-not-allowed-in-this-plmn**
- **network-failure** - Default
- **no-suitable-cell-in-tracking-area**
- **plmn-not-allowed**
- **roaming-not-allowed-in-this-tracking-area**
- **tracking-area-not-allowed**

Use this command to configure the cause code returned to a UE when a failure occurs during S-GW selection. By default, the MME sends the UE the **#17 - Network failure** cause code when encountering this condition.

If a cause code mapping is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the **local-cause-code-mapping** command in the call-control-profile configuration mode. This command is described in the *Call Control Profile Configuration Mode Commands* chapter.

Examples

The following command maps the "plmn-not-allowed" cause code to the S-GW selection failure condition:

local-cause-code-mapping sgw-selection-failure emm-cause-code plmn-not-allowed

local-cause-code-mapping vlr-down

Configures the cause code to send in a ATTACH ACCEPT or TAU ACCEPT to a UE that attachment to the VLR has failed because a VLR down condition is present.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description **local-cause-code-mapping vlr-down emm-cause-code { congestion | cs-domain-unavailable | imsi-unknown-in-hlr | msc-temp-unreachable | network-failure }**
default local-cause-code-mapping vlr-down

default local-cause-code-mapping vlr-down

Returns the cause code mapping to its default value: **msc-temp-unreachable**.

vlr-down emm-cause-code *emm_cause_code*

Specifies the EPS Mobility Management (EMM) cause code to return when a VLR down condition is present.

emm_cause_code must be one of the following options:

- **congestion**
- **cs-domain-unavailable**
- **imsi-unknown-in-hlr**
- **msc-temp-unreachable**- Default.
- **network-failure**

Use this command to configure the cause code returned to a UE when a VLR down condition is present. By default, the MME sends the UE the **#16: "MSC temporarily not reachable** cause code when encountering this condition.

If a condition is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the **local-cause-code-mapping** command in the call-control-profile configuration mode. This command is described in the *Call Control Profile Configuration Mode Commands* chapter.

Examples

The following command maps the "network failure" EMM cause code to the VLR down condition:
local-cause-code-mapping vlr-down emm-cause-code network-failure

local-cause-code-mapping vlr-unreachable

Configures the cause code to send in a ATTACH ACCEPT or TAU ACCEPT to a UE that attachment to the VLR has failed because a VLR unreachable condition is present.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description **local-cause-code-mapping vlr-unreachable emm-cause-code { congestion | cs-domain-unavailable | imsi-unknown-in-hlr | msc-temp-unreachable | network-failure }**
default local-cause-code-mapping vlr-unreachable

default local-cause-code-mapping vlr-unreachable

Returns the cause code mapping to its default value: **msc-temp-unreachable**.

vlr-down emm-cause-code ***emm_cause_code***

Specifies the EPS Mobility Management (EMM) cause code to return when a VLR unreachable condition is present.

emm_cause_code must be one of the following options:

- **congestion**
- **cs-domain-unavailable**
- **imsi-unknown-in-hlr**
- **msc-temp-unreachable** - Default.
- **network-failure**

Use this command to configure the cause code returned to a UE when a VLR unreachable condition is present. By default, the MME sends the UE the **#16: "MSC temporarily not reachable** cause code when encountering this condition.

If a condition is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the **local-cause-code-mapping** command in the call-control-profile configuration mode. This command is described in the *Call Control Profile Configuration Mode Commands* chapter.

Examples

The following command maps the "network failure" EMM cause code to the VLR unreachable condition:
local-cause-code-mapping vlr-unreachable emm-cause-code network-failure

location-reporting

Enables or disables the UE location reporting function on the MME service.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description **[no | default] location-reporting**

default

Disables the location reporting feature on MME service.

no

Disables the location reporting feature on MME service.

Usage Guidelines Use this command to enable or disable the UE location reporting feature on the MME service. When enabled the MME forwards a location report request for a specific UE from the P-GW to the eNodeB.

Important Location reporting, also known as User Location Information (ULI) Reporting, is a licensed feature and requires the purchase of the ULI Reporting feature license.

Examples The following command sets the MME service to allow for location reporting for UEs:
location-reporting

mapping

Configures how the MME maps the Target RNC-ID fields to the Target eNodeB-ID and TAC fields for Inter-RAT Gn/Gp handovers.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description **mapping rncid-to-enbid { maptype-default-includes-only-enb | maptype1-includes-enb-tai }**
no mapping rncid-to-enbid

no

Sets the command to use the default value of **maptype-default-includes-only-enb**.

maptype-default-includes-only-enb

Default mapping logic

Maps the Target RNC-ID fields to Target eNodeB-ID fields as follows:

- PLMN of LAI => PLMN of MME
- LAC of LAI => MME Group ID
- RAC => Not used.
- RNC-ID (12 or 16bits) => Lowest 12 or 16 bits of eNB ID.
- TAC is picked from the list of TAIs supported by the target eNB.

maptype1-includes-enb-tai

Maps the Target RNC-ID fields to Target eNodeB-ID fields as follows:

- PLMN of LAI => PLMN of TAI and eNB
- LAC of LAI => TAC of TAI

- RAC => Lowest 8 bits of eNB ID
- RNC-ID (12bits) => Highest 12 bits of eNB ID

Usage Guidelines Use this command to configure how the MME maps the Target RNC-ID fields to the Target eNodeB-ID and TAC fields for Inter-RAT Gn/Gp handovers.

max-bearers per-subscriber

Specifies the maximum number of EPS bearers that a subscriber may simultaneously use to access this MME service.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description

max-bearers per-subscriber *max_bearer*
default max-bearers per-subscriber

default

Configures the maximum EPS bearers for a subscriber to use simultaneously to the default value of 11.

max_bearer

Specifies the maximum number of EPS bearers for a subscriber may simultaneously use to access this MME service.

max_bearer is an integer from 1 through 11. Default: 11

Usage Guidelines

Use this command to set the maximum number of EPS bearers that a subscriber may simultaneously use to access this MME service.

Examples

The following command specifies that a maximum of *6* simultaneous EPS bearers can be facilitated for a subscriber at any given time:
max-bearers per-subscriber 6

max-paging-attempts

This command configures the maximum number of paging attempts allowed for network requested service creation to a subscriber.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description

max-paging-attempts *max_paging_attempts*
default max-paging-attempts

default

Configures the maximum number of paging attempts to the default value of 3.

max_paging_attempts

Specifies the maximum number of paging attempts allowed for network requested service creation to a subscriber.

max_paging_attempts is an integer from 1 through 10. Default: 3

Usage Guidelines

Use this command to set the maximum number of paging attempts allowed for network requested service creation to a subscriber.

When Heuristic Paging is enabled, this setting applies only to messages sent to all eNodeBs in all TAIs present in the TAI list. Paging to the last known eNodeB and paging the TAI from which the UE was last heard is attempted only once. As a result, when max-paging-attempts is set to 3, a maximum of 5 paging retries are attempted with Heuristic Paging enabled.

Refer to the *Heuristic and Intelligent Paging* chapter in the *MME Administration Guide* for more information about Heuristic Paging.

Examples

The following command specifies that a maximum of *6* paging attempt retransmissions allowed for network requested service creation to a subscriber:
max-paging-attempts 6

max-pdns per-subscriber

Specifies the maximum number of Packet Data Networks (PDNs) that a subscriber may simultaneously access through this MME service.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description **max-pdns per-subscriber** *max_pdn*
default max-pdns per-subscriber

default

Configures the maximum PDNs that a subscriber can simultaneously access through this MME service to the default value of 3.

max_pdn

Specifies the maximum number of PDNs that a subscriber may simultaneously access through this MME service.

max_pdn is an integer from 1 through 11. Default: 3

Usage Guidelines Use this command to set the maximum number of PDNs that a subscriber may simultaneously access through this MME service.

Examples The following command specifies that a maximum of *2* simultaneous PDNs can be accessed by a subscriber at any given time through this MME service:
max-pdns per-subscriber 2

mme-id

Configures the MME identifier within an MME service. The MME identifier is constructed form the MME group ID and MME Code.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description

mme-id group-id *grp_id* **mme-code** *mme_code*
no mme-id

no

Removes the configured MME identifier for this MME service.

Caution Removing the MME identifier is a disruptive operation; the MME service is removed from the system.

group-id ***grp_id***

Specifies the group identifier for the group of which this MME belongs as an integer from 0 through 65535.

mme-code ***mme_code***

Specifies the unique code for this MME service as an integer from 0 through 255.

Usage Guidelines

Use this command to set the MME identifier for this MME service. This MME identifier will be the identity of this MME in network.

Caution Changing or removing the MME identifier is a disruptive operation; the MME service will be re-started or removed from service.

Examples

The following command configures the MME identifier with group id as *41025* and MME code as *101* for this MME service:
mme-id group-id 41025 mme-code 101

mmemgr-recovery

Configures the recovery action for the MME manager.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description **mmemgr-recovery { no-reset | reset-s1-peers }**
default mmemgr-recovery

default

Resets the function configuration to the MME's default value of reset S1 peers.

no-reset

Specifies that the recovery action is **not** to reset S1 peers.

reset-s1-peers

Specifies that the recovery action is to reset S1 peers. This is the default action.

Usage Guidelines Use this command to set a recovery action for the MME Manager.

Examples The following command configures the MME Manager recovery action to reset all S1 peers:
mmemgr-recovery reset-s1-peers

msc

Creates and manages an Mobile Switching Center (MSC) server configuration, for the MME service, for an MSC enhanced with Single Radio Voice Call Continuity (SRVCC). The MSC server acts as an endpoint for the Sv interface.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description

msc { *msc_name* | **[** *ipv4_address* | *ipv6_address* **]** } **[ip-address [** *ipv4_address* | *ipv6_address* **] [offline** | **online]**
no msc { *msc_name* | **[** *ipv4_address* | *ipv6_address* **]** }

no ***msc_name***

Removes the MSC configuration from the MME service.

msc_name

Specifies a name for this peer MSC server.

msc_name must be an alphanumeric string from 1 to 63 characters.

ip-address ***ipv4_address*** **|** ***ipv6_address***

Specifies the IP address of the peer MSC server in either IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

In Release 16.0 and higher, the MME supports DNS-based MSC selection. If DNS-based selection is configured, the DNS lookup is done first, then it will fall back to local ip address.

offline

Mark this MSC server offline for maintenance. Once this command is issued, the MME will no longer send future handover requests to this MSC server. No GTPv2 messages are generated when offline/online mode is changed.

Once the MSC server is set for offline, the **online** keyword must be used to return the server to online mode.

online

Mark this MSC server for online mode. Once this command is issued, the MSC server is added back into the MSC selection algorithm and normal operation is returned. By default, an MSC server is online unless the **offline** keyword is specified.

Usage Guidelines

Use this command to configure a peer MSC server used during SRVCC handovers. For details on the configuration of the MSC and the MME's usage of SRVCC, refer to the *Single Radio Voice Call Continuity* feature chapter in the *MME Administration Guide*.

Also, this command can set an MSC server offline for maintenance.

Examples

For Release 16.0 and higher, the following command defines an MSC server *msc1* that will be selected by DNS. Any MSCs configured for DNS-based selection must be defined without an IP address:
msc msc1

The following command defines a *default* MSC server with an IPv4 address of *10.2.3.20*. The MME will select the default when no other MSC selection logic (DNS selection or MSC pool areas) are configured, or when these fail to return an MSC address.
msc default ip-address 10.2.3.20

For Release 15.0 and higher:

The following command defines an MSC server *mscwest* with an IPv4 address of *10.2.3.4*:
msc mscwest ip-address 10.2.3.4

The following command marks the above MSC server offline:
msc mscwest ip-address 10.2.3.20 offline

The following command defines a *default* MSC server with an IPv4 address of *10.2.3.20*. The MME will select the default when MSC pool areas are not configured, or when an MSC address fails to be returned.
msc default ip-address 10.2.3.20

For Release 14.0 and earlier:

The following command specifies an IPv4 address for the peer MSC server as *10.2.3.4*:
msc 10.2.3.4

msc-mapping

This command creates a mapping between the MSC ISDN number and the MSC's IP-address (either IPv4 or IPv6) to ensure location continuity for SRVCC handover. This mapping is required to include the MSV ID in the target service node IE for the Emergency_Call_Handover event.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description

msc-mapping ip-address { *ipv4_address* **|** *ipv6_address* **} isdn** *isdn_number*
msc-mapping ip-address { *ipv4_address* **|** *ipv6_address*

no

Removes a specific MSC IP address mapping definition from the MME Service configuration.

ip-address

ipv4_address **|** *ipv6_address* Specifies the IP address for the MSC as an IPv4 dotted-decimal or as an IPv6 colon-separated-hexadecimal notation.

isdn

isdn_number: Enter a numeric string upto 15 digits long.

Usage Guidelines

The MME Service supports a maximum of 24 MSC IP address to ISDN mapping definitions.

Use the **show mme-service** command to see the MSC IP address to ISDN mappings created with this command.

Examples

Map the IPv4 *192.168.61.2* address of the MSC to ISDN *123456789012345*
msc-mapping ip-address 192.168.61.2 isdn 123456789012345

nas gmm-qos-ie-mapping

Configures which QOS the MME uses in NAS GMM QoS IE and GTPv1 Context response message when the subscriber comes to MME via a handover from a GN/GP SGSN.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description

nas gmm-qos-ie-mapping { gngp-imported-qos | native-eps-qos }

gngp-imported-qos

Configures the MME to send the QoS received from GN/GP SGSN (whenever applicable).

native-eps-qos

Configures the MME to send the EPS (4G) QoS received from HSS.

This is the default setting.

Usage Guidelines

When a subscriber comes to MME via a handover from Gn/Gp SGSN, this command controls whether the MME is to use the QoS received from the SGSN, or whether to use the updated EPS QoS received from the HSS. This value is then mapped to gmm-qos-ie in subsequent NAS messages and in GTPv1 Context response messages.

Examples

The following command configures the MME to use the QoS values from the Gn/Gp SGSN in gmm-qos-ie NAS messages and GTPv1 Context response messages.
nas gmm-qos-ie-mapping gngp-imported-qos

nas-max-retransmission

Sets the retransmission counter for all type of Non-Access Stratum (NAS) messages in an MME service.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description **nas-max-retransmissions** *nas_retrans_count*
default nas-max-retransmissions

default

Resets the retransmission counter to the default value of 4.

nas_retrans_count

Sets the maximum number of retransmission of NAS messages permitted during any procedure after which the activation procedure will be discarded.

nas_retrans_count is an integer from 1 through 10. Default: 4

Usage Guidelines Use this command to set maximum number of retries allowed for any type of NAS messages.

NAS Messages sent by the MME which require a response from the UE for procedure completion are retransmitted. Retransmission happens based on timer expiry. The timers are configured through the **emm** and **esm** commands. NAS messages are retransmitted per configuration, and if no response is received from the UE, the pending transaction is abandoned. If the transaction is a DETACH or PDN DISCONNECT REQUEST, the transaction is completed without further UE signaling.

The timeout duration configured through the **emm** and **esm** commands will be applicable between two retries.

Examples The following command sets the maximum number of retries allowed as *4* for all type of NAS messages in an MME service.
default nas-max-retransmissions

network-sharing

Configures additional PLMN IDs for this MME service. Refer to the **plmn-id** command to create the base PLMN identifier for an MME service. Each PLMN ID consists of the Mobile Country Code (MCC) and Mobile Network Code (MNC). A maximum of four network sharing entries can be configured per MME service. These PLMN IDs will be communicated to the eNodeBs in the S1 SETUP response and MME CFG Update messages.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description

network-sharing plmn-id mcc *number* **mnc** *number* **mme-id group-id** *id* **mme-code** *code*
no network-sharing plmn-id mcc *number* **mnc** *number*

no

Disables the network sharing mode on this MME service.

Caution Removing the PLMN identifier is a disruptive operation; the MME service will be restarted.

plmnid mcc *number* mnc *number*

Sets the mobile country code (MCC) and mobile network code (MNC) of the PLMN ID for this service.

mcc *number*: Specifies the MCC portion of the PLMN identifier as an integer from 100 through 999.

mnc *number*: Specifies the MNC portion of the PLMN identifier as a 2- or 3-digit integer from 00 through 999.

mme-id group-id *id*

Specifies the group identifier for the group to which this MME belongs as an integer from 0 through 65535.

mme-code *code*

Specifies the unique code for an MME service as an integer from 0 through 255.

Usage Guidelines

Use this command to configure additional PLMN IDs for an MME service. In a given MME service, each PLMN ID (MCC and MNC) must be unique.

Caution Changing or removing the PLMN identifier is a disruptive operation; the MME service will be restarted.

Examples

The following command configures the network sharing parameters to an MCC of *123*, an MNC of *12*, a MME-ID/Group ID of *100*, and a MME code of *50*:
network-sharing plmnid mcc 123 mnc 12 mme-id group-id 100 mme-code 50

nri

Configures the network resource identifier (NRI) length used for source SGSN discovery via NRI-FQDN (Fully Qualified Domain Name) based DNS resolution.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description

[no] nri length *length* **plmn-id mcc** *mcc_value* **mnc** *mnc_value*

no

Removes a configured NRI length.

length *length*

Specifies the number of bits to be used in the P-TMSI (bits 23 to 18) to define the NRI as an integer from 1 through 8.

plmn-id mcc *mcc_value* mnc *mnc_value*

Specifies the PLMN-ID of the SGSN pool.

mcc *mcc_value*: Specifies the mobile country code (MCC) portion of the PLMN identifier as an integer from 100 through 999.

mnc *mnc_value*: Specifies the mobile network code (MNC) portion of the PLMN identifier as a 2- or 3-digit integer from 00 through 999.

Usage Guidelines

Use this command to retrieve the NRI (identity of an SGSN) stored in bits 23 to 18 of the packet-temporary mobile subscriber identity (P-TMSI). Up to eight NRI length values can be configured.

Important In the absence of this configuration, the MME treats the NRI as invalid. The MME will use a plain RAI-based FQDN (and not an NRI-based FQDN) for DNS queries made to resolve the source SGSN.

Examples

The following command creates an NRI length of *5* and associates it with an SGSN pool with the PLMN-ID of *123*:

nri length 5 plmnid mcc 123 mnc 23

peer-mme

Configures parameters that, when matched by another MME, specifies that MME as a peer for inter-MME relocations.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description

peer-mme { gummei mcc *number* **mnc** *number* **group-id** *id* **mme-code** *code* **address** *ipv4_address* **| tai-match priority** *value* **mcc** *number* **mnc** *number* **tac {** *area_code* **| any |** *start_area_code* **to** *end_area_code* **} address** *ipv4_address* **}**
no peer-mme { gummei mcc *number* **mnc** *number* **group-id** *id* **mme-code** *code* **| tai-match priority** *value* **}**

no

Removes the configured peer Globally Unique MME Identifier (GUMMEI) or TAI match priority from this service.

gummei mcc *number* mnc *number* group-id *id* mme-code *code* address *ipv4_address*

Specifies that an MME with values matching those configured in this GUMMEI is to be considered a peer MME. This variable supports the lookup of an IP address for a peer MME based on the exact match of the supporting keyword below (which make up the GUMMEI).

mcc *number*: Sets the mobile country code (MCC) for peer match as an integer from 100 through 999.

mnc *number*: Sets the mobile network code (MNC) for this peer match as a 2- or 3-digit integer from 00 through 999.

group-id *id*: Specifies the group identifier for the group to which this MME belongs as an integer from 0 through 65535.

mme-code *code*: Specifies the unique code for an MME service as an integer from 0 through 255.

address *ipv4_address*: Specifies the IP address of the peer MME in IPv4 dotted-decimal notation.

tai-match priority *value* **mcc** *number* **mnc** *number* **tac** { *area_code* | **any** | *start_area_code* **to** *end_area_code* } **address** *ipv4_address*

Specifies that an MME with values matching those configured in this Tracking Area Identifier (TAI) match, is to be considered a peer MME. This keyword provides a priority-ordered list of TAI descriptions where the Tracking Area Code (TAC) field may be either an exact value, a range of values, or a "wildcard" value. It also provides an IP address of the peer MME corresponding to the TAI description.

priority *value*:

mcc *number*: Sets the mobile country code (MCC) for peer match as an integer from 100 through 999.

mnc *number*: Sets the mobile network code (MNC) for this peer match as an integer from 00 through 999.

tac *area_code*: Sets a specific Tracking Area Code (TAC) for the peer MME match as an integer from 1 through 65535.

tac any: Specifies that any TAC value can be considered for a peer MME.

tac *start_area_code* **to** *end_area_code*: Specifies a range of TACs. MMEs within this range and matching the rest of the criteria in this command are to be considered peer MMEs. *start_area_code* and *end_area_code* are integers from 1 through 268435455.

address *ipv4_address*: Sets a specific IP address for this TAI peer MME match in IPv4 dotted-decimal notation.

Usage Guidelines

Use this command to configure parameters that, when matched by another MME, specifies that MME as a peer for inter-MME relocations.

This command allows configuration for two relocation scenarios:

- **gummei**: an MME receives either an Attach or a TAU request with a Globally Unique Temporary Identity (GUTI) that originated from another MME.
- **tai-match**: an MME receives an S1 Handover Required message and must select a new MME based on the TAI.

Up to 32 peer-mme gummei or tai-match entries may be configured per MME service.

Examples

The following command identifies a peer MME with GUMMEI parameters:
peer-mme gummei mcc 123 mnc 12 group-id 40000 mme-code 100 address 10.2.3.4

peer-sgsn rai

Statically configures Routing Area Identity (RAI) parameters of the peer SGSN environment to facilitate MME-SGSN relocations over S3 or Gn/Gp interfaces.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description **peer-sgsn rai mcc** *mcc_value* **mnc** *mnc_value* **[nri** *value* **] rac** *value* **lac** *value* **address** *ip_address* **capability [gn] [gp] [s16] [s3]**
no peer-sgsn rai mcc *mcc_value* **mnc** *mnc_value* **[nri** *value* **] rac** *value* **lac** *value*

no

Deletes the specified peer-SGSN RAI parameter configuration from the MME Service configuration.

mcc *mcc_value*

Specifies the mobile country code (MCC) portion of the PLMN identifier as an integer from 100 through 999.

mnc *mnc_value*

Specifies the mobile network code (MNC) portion of the PLMN identifier as a 2- or 3-digit integer from 00 through 999.

nri *value*

Specifies the Network Resource Identifier (NRI) value, used as an additional identity, as an integer from 0 through 65535.

rac *value*

Specifies the Routing Area Code (RAC) used to facilitate a lookup for a specific peer SGSN as an integer from 0 through 255.

lac *value*

Specifies the Location Area Code (LAC) value, used to facilitate a lookup for a specific peer SGSN, as an integer from 0 through 65535.

address *ip_address*

Specifies an existing IP address of the peer SGSN in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

capability [gn] [gp] [s16] [s3]

Configures the GTP interface capability of the peer SGSN.

gn: Specifies that the peer SGSN is capable of communication over the Gn interface.

gp: Specifies that the peer SGSN is capable of communication over the Gp interface.

s16: Specifies that the peer SGSN is capable of communication over the S16 interface.

s3: Specifies that the peer SGSN is capable of communication over the S3 interface.

Usage Guidelines

Use this command to configure parameters to facilitate a lookup for a specific peer SGSN. These parameters, when matched by an SGSN, specifies that SGSN as a peer for inter-RAT relocations.

The **peer-sgsn** command allows configuration for two relocation scenarios:

- Routing Area Identity (RAI) configuration is used for the lookup of an IP address for a peer MME based on the exact match of the RAI (and optionally NRI).
- Radio Network Controller Identification (RNC-ID) configuration is used for the lookup of an IP address for a peer MME based on the exact match of the RNC-ID.

Up to 32 (combined total) peer-SGSN RAI and RNC-ID entries may be configured per MME service.

Examples

The following command configures an SGSN lookup using RAI parameters with Gp interface capability:
peer-sgsn rnc-id mcc 123 mnc 12 nri 1557 rac 33 lac 3542 address 10.4.3.2 capability gp

peer-sgsn rnc-id

Statically configures Radio Network Controller Identification (RNC-ID) parameters of the peer SGSN environment to facilitate MME-SGSN relocations over S3 or Gn/Gp interfaces.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description

peer-sgsn rnc-id mcc *mcc_value* **mnc** *mnc_value* **rnc** *value* **address** *ip_address* **capability [gn] [gp] [s16] [s3]**
no peer-sgsn rnc-id mcc *mcc_value* **mnc** *mnc_value* **rnc** *value*

no

Deletes the specified peer-SGSN RAI parameter configuration from the MME Service configuration.

mcc *mcc_value*

Specifies the mobile country code (MCC) portion of the PLMN identifier as an integer from 100 through 999.

mnc *mnc_value*

Specifies the mobile network code (MNC) portion of the PLMN identifier as a 2- or 3-digit integer from 00 through 999.

rnc *value*

Specifies the Radio Network Controller (RNC) identification number used to facilitate a lookup for a specific peer SGSN as an integer from 0 through 65535.

address *ip_address*

Specifies an existing IP address of the peer SGSN in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

capability [gn] [gp] [s16] [s3]

Configures the GTP interface capability of the peer SGSN.

gn: Specifies that the peer SGSN is capable of communication over the Gn interface.

gp: Specifies that the peer SGSN is capable of communication over the Gp interface.

s16: Specifies that the peer SGSN is capable of communication over the S16 interface.

s3: Specifies that the peer SGSN is capable of communication over the S3 interface.

Usage Guidelines

Use this command to configure parameters to facilitate a lookup for a specific peer SGSN. These parameters, when matched by an SGSN, specifies that SGSN as a peer for inter-RAT relocations.

The **peer-sgsn** command allows configuration for two relocation scenarios:

- Radio Network Controller Identification (RNC-ID) configuration is used for the lookup of an IP address for a peer MME based on the exact match of the RNC-ID.
- Routing Area Identity (RAI) configuration is used for the lookup of an IP address for a peer MME based on the exact match of the RAI (and optionally NRI).

Multiple peer-sgsn RNC-ID records can be configured for the same MCC/MNC/RNC, each with different IP addresses. During a handover, if the initial peer SGSN rejects the forward relocation request, the MME will step through any alternate peer SGSNs to attempt the handover.

Up to 32 (combined total) peer-SGSN RAI and RNC-ID entries may be configured per MME service.

Examples

The following command configures an SGSN lookup using RNC-ID parameters with Gn interface capability:
peer-sgsn rnc-id mcc 123 mnc 12 rnc 2000 address 10.2.3.4 capability gn

pgw-address

Configures the IPv4 or IPv6 address of the PDN Gateway (P-GW), specifies the protocol for S5 and S8 interfaces, and sets other parameters within the MME service. By default S5 and S8 use GTP protocol for this.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description **pgw-address** { *ipv4_address* | *ipv6_address* } **[s5-s8-protocol pmip] [weight** *weight* **]**
no pgw-address { *ipv4_address* | *ipv6_address* } **[s5-s8-protocol pmip]**

no

Removes a previously configured IP address for a P-GW along with the S5 and S8 interface of P-MIP protocol type, and other parameters from this MME service.

ipv4_address* | *ipv6_address

Specifies the IP address of the P-GW in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

s5-s8-protocol pmip

Specifies that Proxy-MIP is to be used for S5 and S8 interfaces with the P-GW. By default S5 and S8 interface uses GTP protocol.

pmip Sets the protocol to Proxy-MIP for S5 and S8 interface.

weight ***weight***

Specifies the weight (preference) assigned to the address P-GW for load balancing. *weight* is an integer from 1 through 100 where 1 is the least preferred and 100 is the most preferred. If no weight is specified, the P-GW address is assigned a default weight of 1.

If a weight is assigned to an address, the weights of the P-GW(s) (that are operational) are totaled, and then a weighted round-robin selection is used to distribute new primary PDP contexts among the P-GW(s) according

to their weights. As with all weighted round-robin algorithms, the distribution does not look at the current distribution, but simply uses the weights to distribute new requests. For example, two P-GWs assigned weights of 70 and 30 would distribute 70% of calls to one, and 30% to the other. The sum of all weights do not need to total 100.

Usage Guidelines

Use this command to configure the PDN Gateway (P-GW) addresses to use with MME service. This command also changes the default protocol from GTP to P-MIP for the S5 and S8 interface, and assigns a weight to use when sharing the load between associated P-GWs. A maximum of 16 P-GW addresses can be configured with this command.

This command only changes the use of protocol for the S5 and S8 interface. By default a P-GW uses GTP protocol for S5 and S8 interfaces. This command allows an operator to change the protocol to P-MIP for S5 and S8 interface.

When weight is used, the weights of the operational P-GW(s) are totaled and then weighted round-robin selection is used to distribute new default bearer contexts among P-GW(s).

Examples

The following command associates the P-GW IP address of *192.168.3.1* to the MME service with S5 and S8 protocol as P-MIP and weight as *90*:
pgw-address 192.168.3.1 s5-s8-protocol pmip weight 90

The following command removes the above configured P-GW IP address and other parameters:
no pgw-address 192.168.3.1 s5-s8-protocol pmip

plmn-id

Configures the Public Land Mobile Network (PLMN) identifier for this MME service. The PLMN identifier consists of the Mobile Country Code (MCC) and Mobile Network Code (MNC). A single PLMN ID can be configured per MME service.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description

[no] plmn-id mcc *mcc_value* **mnc** *mnc_value*

no

Removes the configured PLMN identifier for this MME service.

Caution Removing the PLMN identifier is a disruptive operation; the MME service will be restarted.

mcc *mcc_value*

Specifies the mobile country code (MCC) portion of the PLMN identifier as an integer from 100 through 999.

mnc *mnc_value*

Specifies the mobile network code (MNC) portion of the PLMN identifier as a 2- or 3-digit integer from 00 through 999.

Usage Guidelines

Use this command to set the PLMN identifier for this MME service.

Caution Changing or removing the PLMN identifier is a disruptive operation; the MME service will be restarted.

One PLMN identifier is supported per MME service.

Important To configure additional PLMN IDs for this MME service, refer to the **network-sharing** command described in this chapter.

Examples The following command configures the PLMN identifier with MCC value as *102* and MNC value as *20* for this MME service:
plmn-id mmc 102 mnc 20

policy attach

Configures parameters for the UE Attach procedure.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description **policy attach { imei-query-type { imei | imei-sv | none } [verify-equipment-identity [allow-on-eca-timeout | deny-greylisted | deny-unknown | verify-emergency]] | set-ue-time { disable | enable [prefer-mme | prefer-msc] }**
default policy attach { imei-query-type | set-ue-time }

default

Returns the command to its default setting of **none** for **imei-query-type** and **disabled** for **set-ue-time**.

imei-query-type { imei | imei-sv | none }

Configures the IMEI query type for UE attach.

- **imei**: Specifies that the MME is required to query the UE for its International Mobile Equipment Identity (IMEI).
- **imei-sv**: Specifies that the MME is required to query the UE for its International Mobile Equipment Identity - Software Version (IMEI-SV).
- **none**: Specifies that the MME does not need to query for IMEI or IMEI-SV.

verify-equipment-identity [allow-on-eca-timeout | deny-greylisted | deny-unknown | verify-emergency]

Specifies that the identification (IMEI or IMEI-SV) of the UE is to be performed by the Equipment Identity Register (EIR) over the S13 interface.

- **allow-on-eca-timeout**: Configures the MME to allow equipment that has timed-out on ECA during the attach procedure.

- **deny-greylisted**: Configures the MME to deny grey-listed equipment during the attach procedure.
- **deny-unknown**: Configures the MME to deny unknown equipment during the attach procedure.
- **verify-emergency**: Configures the MME to ignore the IMEI validation of the equipment during the attach procedure in emergency cases. This keyword is only supported in release 12.2 and higher.

set-ue-time { disable | enable [prefer-mme | prefer-msc] }

Configures the MME to set the time in the UE during the Attach procedure. Default: **disabled**.

[prefer-mme | prefer-msc]: Specifies which UE-time to use when delivering EMM messages to the UE for cases when a UE performs combined registration.

prefer-mme: The MME shall always send its UE-time information (based on the MME's own settings), and ignore any EMM Information messages sent by the MSC.

prefer-msc: In cases where a successful Location Update is performed to a MSC, the MME shall NOT send MME configured information to the UE, and shall transmit only MSC-sent information. In cases where a Location Update procedure is not required (for example, for UEs that are performing EPS only ATTACH), or in cases where the Location Update Procedure is unsuccessful, the MME shall send the MME configured information.

Usage Guidelines

Use this command to configure various MME settings used during the UE Attach procedure.

Examples

The following command configures the MME to query the UE for its IMEI and to verify the UEs equipment identity over the S13 interface with an EIR:
policy attach imei-query-type imei verify-equipment-identity

policy idle-mode

Configures the user-defined behavioral policies of session management for an LTE subscriber in an MME service.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description **policy idle-mode detach { explicit | implicit }**
default policy idle-mode detach

default

Sets the policy configuration to the default behavior for subscriber IDLE mode Detach. The default behavior is Detach implicit.

idle-mode detach

Configures the IDLE mode Detach behavior of a UE.

detach

Defines the Detach procedure while the UE is in IDLE mode.

explicit

Enables the Explicit Detach while a UE is in IDLE mode. The system will page the UE before Detach procedure is started, and then perform the Explicit Detach procedure.

implicit

Enables the Implicit Detach while a UE is in IDLE mode. The system never sends any message to the UE before Detach, and executes the Implicit Detach procedure immediately. This is the default behavior.

Usage Guidelines Use this command to set the user-defined policies for session management in this MME service.

Examples The following command sets the Idle Mode Detach policy to Implicit for a user in this MME service:
policy idle-mode detach implicit

policy inter-rat

Configures inter-RAT policy settings.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description **policy inter-rat { ignore-sgsn-context-id | indirect-forwarding-tunnels always | select-topologic-sgw }**
no policy inter-rat { ignore-sgsn-context-id | indirect-forwarding-tunnels | select-topologic-sgw }

no

Disables the function.

ignore-sgsn-context-id

Configures the MME to ignore any Context-ID mismatch between HSS and HLR and to use the Context-ID from the HSS to override the Context-ID from the source SGSN. If this option is disabled (default), the MME will drop the PDN when there is a Context-ID mismatch.

indirect-forwarding-tunnels always

Enables establishment of Indirect Data Forwarding Tunnels (IDFT) for Gn/Gp-based Serving Radio Network Subsystem (SRNS) relocations. By default, the MME is configured to never establish IDFT.

select-topologic-sgw interface gn

Configures the MME to select the S-GW based on topological closeness to the P-GW for Gn/Gp handoff scenarios. Weighted distribution will occur across node pairs in the same degree and same order. By default this functionality is disabled.

During inter-RAT Gn/Gp based handoffs, the MME does not learn the P-GW host name from the old Gn/Gp SGSN as part of UE context. Without the P-GW host name, selection of the topologically closest S-GW is not possible per 3GPP standards. This functionality enables the MME to use a proprietary mechanism for learning the P-GW host name. For S3 & S10 cases, there is no need to enable this command, as GTPv2 allows the P-GW host name to be communicated to/from S4-SGSN/MME.

This functionality requires the **gw-selection co-location** or **gw-selection topology** commands to be enabled in the call-control-profile mode.

Note: The P-GW is anchored in the inter-RAT handoff scenarios, so regardless of the preferred weight specified in **gw-selection**, the MME always considers the S-GW's weight for weighted distribution purposes.

Usage Guidelines

Use this command to enable or disable establishment of indirect data forwarding tunnels for Gn/Gp-based SRNS relocations, and to enable or disable Context-Identifier overriding, and to enable or disable learning the P-GW host name during Gn/Gp handoffs for purposes of topologically-close S-GW distribution.

Examples

The following command enables establishment of indirect data forwarding tunnels for Gn/Gp-based SRNS relocations:
policy inter-rat indirect-forwarding-tunnels always

policy network

Configures the MME to indicate to the P-GW that all peer SGSNs support dual-addressing for bearers and, subsequently, dual-addressing must be supported for all IPv4 and IPv6 PDNs. Dual-addressing on SGSNs is based on the UE's capability to support inter-RAT roaming.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description

[default | no] policy network dual-addressing-supported

default

Returns the command to its default setting of disabled.

no

Removes the ability to send dual-addressing support messaging from the MME to the P-GW.

dual-addressing-supported

Specifies that the MME shall indicate to the P-GW that dual-addressing is supported.

Usage Guidelines

Use this command to configure the MME to send messaging to the P-GW that indicate that all peer SGSNs support dual-addressing for bearers and, subsequently, dual-addressing must be supported for all IPv4 and IPv6 PDNs.

Important This command can be used for Pre-release 8 and Release 8 SGSNs.

policy overcharge-protection

Enables overcharge protection where the MME can detect and signal a Loss of Signal Contact to the S-GW which in turn informs the P-GW to stop charging.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description **policy overcharge-protection s1ap-cause-code-group** *group_name*
{ default | no } policy overcharge-protection

default

Returns the command to its default setting of disabled. This provides the same behavior as the **no** keyword option.

no

Disables overcharge protection. This provides the same behavior as the **default** keyword option.

s1ap-cause-code-group ***group_name***

group_name: Specify the name of a preconfigured S1-AP Cause Code Group.

When the received cause code from the eNodeB matches any the cause codes defined in this Cause Code Group, the MME sets the ARRL (Abnormal Release of Radio Link) bit in the Indication IE of the Release Access Bearer Request to the S-GW.

For more information about creating an S1-AP Cause Code Group, refer to the **cause-code-group** command in the *LTE Policy Configuration Mode Commands* chapter, and the **class** command in the *S1AP Cause Code Configuration Mode Commands* chapter.

Usage Guidelines

Important Overcharge protection is a license-controlled feature. A valid feature license must be installed prior to configuring this feature. Contact your Cisco account representative for more information.

Use this command to enable or disable overcharging protection for this MME service. When enabled, the MME can detect and signal a Loss of Signal Contact to the S-GW which in turn informs the P-GW to stop charging for the UE.

Refer to the *Overcharging Protection* chapter of the *MME Administration Guide* for more information about this feature.

Examples

The following command enables overcharging protection for the S1-AP cause code defined in the S1AP Cause Code Group *group1*:
policy overcharge-protection s1ap-cause-code-group group1

policy overload

Configures the traffic overload policy to control congestion in this service.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description **policy overload { drop | reject }**
default policy overload

default

Sets the traffic overload policy action to the fault behavior of Reject.

drop

Specifies that the system is to drop the incoming packets with new session requests to avoid overload on MME node. Default: Disabled

reject

Configures the system to reject the new session/call request and responds with a reject message when the threshold for allowed call sessions is crossed on the MME node. Default: Enabled

Usage Guidelines Use this command to set the user-defined policies for new call connection attempts when an MME service is overloaded.

Congestion policies at the service-level can be configured for an individual service. When congestion control functionality is enabled, these policies dictate how services respond when the system detects that a congestion condition threshold has been crossed.

Examples The following command sets the nw call connect policy to reject the new session/call request in an MME service:
policy overload reject

policy pdn-deactivate

Configures the MME to deactivate a PDN connection if the charging characteristics (CC) AVP changes in the standalone Insert Subscriber Data Request (ISDR) or the Update Location Answer (ULA).

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description

[no] policy pdn-deactivate cc-change

no

This command filter instructs the MME to disable the PDN deactivation configuration defined with this **policy** command.

pdn-deactivate

This keyword configures the MME to deactivate the PDN connection based on the AVP included to filter the keyword.

cc-change

This filter represents the charging characteristics AVP. If it is included in the command, then the MME deactivates the PDN connection when the charging characteristics (CC) AVP changes in the standalone Insert Subscriber Data Request (ISDR) or the Update Location Answer (ULA).

Usage Guidelines

With **policy pdn-deactivate cc-change** configured, the MME updates the subscriber DB with the CC information so that the MME would be able to create a PDN connection with the new CC values.

If the deactivated PDN is the last PDN, then the UE is detached from the network and during the UE's next Attach procedure the updated CC information is taken from the subscriber DB and included in a Create Session Request.

If the information is absent from the DB, and if CC IE is not present in transferred PDNs of Context Response message during 3G to 4G TAU, then the MME does not send local default CC IE in CSReq and the PDN is activated

'Disabled' is the default behavior. If deactivation for CC changes is not enabled, then the MME updates the APN's CC information in the subscriber DB and keeps the PDN active if the CC information changes in or is absent from the ISDR.

To confirm the MME's current configuration regarding PDN deactivation, use the following command. The illustration below is a partial display to indicate the current configuration, which will be either 'enabled' or 'disabled':

show mme-service name *service_name*

```
...
...
Policy S1-Reset                       : Idle-Mode-Entry
Policy PDN-Deact CC-Change            : Enabled
Policy Nas-Non-Del                    : Disabled
...
```

Examples

The following command configures the MME to deactivate the PDN connection when the CC information changes in or is absent from received ISDR:

policy pdn-deactivate cc-change

policy pdn-reconnection

Configures the action by the MME when a PDN connection request to an already connected APN is being processed by the MME service.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description **policy pdn-reconnection { multiple | reject | restart }**
default policy pdn-reconnection

default

Sets the policy for PDN reconnection to its default behavior of Reject.

multiple

Allows multiple connections to a PDN with the same APN and PDN Type. In this case, the existing connection is left unchanged, and the MME attempts to establish an additional connection to the PDN. Default: Disabled

reject

Configures the MME to deny or reject the request, by sending a PDN Connection Reject command. This is the default behavior. Default: Enabled

restart

Deletes the existing connection and initiates an attempt to establish a new connection. Default: Disabled

Usage Guidelines Use this command to set the user-defined policies for PDN reconnection attempt procedures initiated by a UE in an MME service.

While attached the UE can request connections to PDNs. The PDNs are identified by APN (Access Point Name) and PDN Type (ipv4, ipv6 or ipv4v6).

If the UE requests connection to a PDN for which a connection with the same APN name and PDN type already exists, the MME can: 1) deny or reject the request, by sending a PDN connection reject command; 2) allow multiple connections to a PDN with same APN and PDN Type; or 3) delete the existing connection, and attempt to establish a new connection.

Examples

The following command sets the PDN reconnect policy to delete the existing PDN and start the attempt to establish a new connection in an MME service:
policy pdn-reconnection restart

policy s1-reset

Configures how the MME responds to an S1 interface reset.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description **policy s1-reset { detach-ue | idle-mode-entry }**
default policy s1-reset

default

Returns the command to its default setting of **idle-mode-entry**.

detach-ue

detach-ue: Specifies that UEs are to be implicitly detached from the service upon S1 interface reset.

idle-mode-entry

idle-mode-entry: Specifies that UEs are to be placed into an idle mode condition during S1 interface reset.

Usage Guidelines Use this command to configure how the MME reacts to an S1 interface reset condition.

Examples The following command configures the MME to place UEs into an idle state while the S1 interface is being reset:
policy s1-reset idle-mode-entry

policy sctp-down

Configures how the MME responds to a failure of the Stream Control Transmission Protocol (SCTP) connection from the eNodeB.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description **policy sctp-down { detach-ue | idle-mode-entry }**
default policy sctp-down

default

Returns the command to its default setting of **idle-mode-entry**.

detach-ue

detach-ue: Specifies that UEs are to be detached from the service when the SCTP connection from the eNodeB fails.

idle-mode-entry

idle-mode-entry: Specifies that UEs are to be placed into an idle mode condition when the SCTP connection from the eNodeB fails.

Usage Guidelines Use this command to configure how the MME reacts to an SCTP connection failure condition.

Examples The following command configures the MME to place UEs into an idle state while the SCTP connection from the eNodeB fails:
policy sctp-down idle-mode-entry

policy service-request

Configure the behavior of the MME when an initial context setup failure is received during a service request or extended service request procedure.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description **policy service-request initial-context-setup-failure s1ap-cause-code-group** *group_name* **action idle-mode-entry**
default policy service-request initial-context-setup-failure

default

Returns the command to its default behavior, where it detaches the UE when an initial context setup failure is received during a service request or extended service request procdure.

initial-context-setup-failure s1ap-cause-code-group *group_name* action idle-mode-entry

Configures the behavior of the MME when an initial context failure is received from the eNodeB during a service request or extended service request. By default, the MME detaches the UE. This command configures the MME to move the UE to IDLE MODE instead.

group_name: Specify the name of a preconfigured Cause Code Group. The MME takes the configured action to move the UE to IDLE MODE when the cause code returned from the eNodeB matches any of the cause codes defined in this Cause Code Group.

Refer to the **cause-code-group** command in the *LTE Policy Configuration Mode Commands* chapter, and the **class** command in the *S1AP Cause Code Configuration Mode Commands* chapter for more information.

action idle-mode-entry : Configures the MME to move the UE to IDLE MODE when the cause code returned from the eNodeB matches any of the cause codes in the specified S1-AP cause code group.

Usage Guidelines Use this command to configure the behavior of the MME when an initial context setup failure is received during a service request or extended service request procedure.

Examples

The following command configures the MME to detach the UE when an initial context failure occurs and the eNodeB returns a cause code which matches any of the cause codes configured in the *idle* S1-AP cause code group:
policy service-request initial-context-setup-failure s1ap-cause-code-group idle action idle-mode-entry

policy srvcc

Configures the MME to initiate an HSS Purge after the SRVCC HO where the UE supports DTM. It also allows configuration of a purge timeout value in seconds.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description **policy srvcc purge-timer** *seconds*
default policy srvcc
no policy srvcc purge-timer

default

Returns the command to its default behavior, where the MME does **not** initiate a HSS Purge after the SRVCC HO.

no

Returns the command to its default behavior, where the MME does **not** initiate a HSS Purge after the SRVCC HO. This provides the same function as the **default** keyword.

purge-timer ***seconds***

Defines how long in seconds the Purge Timer will run. This is applicable only for SRVCC Handoff without PS Handoff support scenarios.

For example, if **purge-timer** is set to 20 seconds :

If the Context Transfer happens 10 seconds after SRVCC HO, the MME intiates an HSS Purge.

If the Context Transfer happens 30 seconds after SRVCC HO, the MME will NOT initiate an HSS Purge because the Purge Timer has expired.

seconds must be entered as an integer from 1 through 24000.

Usage Guidelines

Use this command to configure the MME to perform the Purge UE procedure to the HSS for UEs which support Dual Transfer Mode (DTM). When configured, the MME initiates an HSS Purge after the following two SRVCC HO scenarios:

For SRVCC Handoff with PS Handoff support, the Purge S6a message is sent immediately after successful completion of the Handoff. For this scenario, the configurable purge timer is not used.

For SRVCC Handoff without PS Handoff support, the configurable timer is initiated and the Purge S6a message is sent if a SGSN Context Request is received prior to timer expiry. If a Context Failure occurs, no HSS Purge S6a message is sent.

Examples

The following command configures the MME to perform the Purge UE procedure and sets the purge timer to 20 seconds.
policy srvcc purge-timer 20

policy tau

Configures parameters for the tracking area update (TAU) procedure.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description **policy tau { imei-query-type { imei | imei-sv | none } [verify-equipment-identity [allow-on-eca-timeout | deny-greylisted | deny-unknown | verify-emergency]] | initial-context-setup-failure s1ap-cause-code-group** *group_name* **action detach-ue | set-ue-time { disable | enable [prefer-mme | prefer-msc] }**
default policy tau { imei-query-type | initial-context-setup-failure | set-ue-time }

default

Returns the command to its default settings:

imei-query-type: **none**

initial-context-setup-failure: Returns the MME to the default behavior, where it moves the UE to IDLE MODE when an initial context setup failure is received during a TAU procedure.

set-ue-time: **disabled**

imei-query-type { imei | imei-sv | none }

Configures the IMEI query type for TAUs.

- **imei**: Specifies that the MME is required to query the UE for its International Mobile Equipment Identity (IMEI).
- **imei-sv**: Specifies that the MME is required to query the UE for its International Mobile Equipment Identity - Software Version (IMEI-SV).
- **none**: Specifies that the MME does not need to query for IMEI or IMEI-SV.

verify-equipment-identity [allow-on-eca-timeout | deny-greylisted | deny-unknown | verify-emergency]

Specifies that the identification (IMEI or IMEI-SV) of the UE is to be performed by the Equipment Identity Register (EIR) over the S13 interface.

- **allow-on-eca-timeout**: Configures the MME to allow equipment that has timed-out on ECA during the attach procedure.
- **deny-greylisted**: Configures the MME to deny grey-listed equipment during the attach procedure.
- **deny-unknown**: Configures the MME to deny unknown equipment during the attach procedure.
- **verify-emergency**: Configures the MME to ignore the IMEI validation of the equipment during the attach procedure in emergency cases. This keyword is only supported in release 12.2 and higher.

initial-context-setup-failure s1ap-cause-code-group *group_name* action detach-ue

Configures the behavior of the MME when an initial context failure is received from the eNodeB during the processing of a TAU request. By default, the MME moves the UE to IDLE MODE. This keyword configures the MME to detach the UE.

group_name: Specify a preconfigured Cause Code Group. The MME takes the configured action to detach the UE when the cause code returned from the eNodeB matches any of the cause codes defined in this Cause Code Group.

Refer to the **cause-code-map** command in the LTE Policy Configuration mode, and the **class** command in the S1AP Cause Code Configuration mode for more information.

action detach-ue : Configures the MME to detach the UE when the cause code returned from the eNodeB matches any of the cause codes in the specified S1-AP cause code group.

set-ue-time { disable | enable [prefer-mme | prefer-msc] }

Configures the MME to set the time in the UE during the TAU procedure. Default: **disabled**.

[prefer-mme | prefer-msc]: Specifies which UE-time to use when delivering EMM messages to the UE for cases when a UE performs combined registration.

prefer-mme: The MME shall always send its UE-time information (based on the MME's own settings), and ignore any EMM Information messages sent by the MSC.

prefer-msc: In cases where a successful Location Update is performed to a MSC, the MME shall NOT send MME configured information to the UE, and shall transmit only MSC-sent information. In cases where a Location Update procedure is not required (for example, for UEs that are performing EPS only ATTACH), or in cases where the Location Update Procedure is unsuccessful, the MME shall send the MME configured information.

Usage Guidelines

Use this command to configure various MME settings used during the tracking area update (TAU) procedure.

Examples

The following command configures the MME to query the UE for its IMEI and to verify the UEs equipment identity over the S13 interface with an EIR:
policy tau imei-query-type imei verify-equipment-identity

The following command configures the MME to detach the UE when an initial context failure occurs and the eNodeB returns a cause code which matches any of the cause codes configured in the "detach" S1-AP cause code group:
policy tau initial-context-setup-failure s1ap-cause-code-group detach action detach-ue

pool-area

Creates an MSC server pool area for the Sv interface or specifies an existing pool area, and enters MME MSC Server Pool Area Configuration Mode.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description **pool-area** *pool_area_name* **type { hash-value | round-robin }**
no pool-area *pool_area_name*

no

Removes the configured pool-area for this MME service.

pool_area_name

Specifies the name of the pool-area as an alphanumeric string of 1 through 63 characters.

type { hash-value | round-robin }

Defines the MSC server selection scheme, either:

hash-value: The MME selects the MSC server based on the result of the IMSI [(IMSI div 10) modulo 1000].

round-robin: The MME selects the MSC server based on the round-robin scheme.

Usage Guidelines Use this command to create an MSC server pool area for the Sv interface or specify an existing pool area configuration and enter the MME Pool Area Configuration Mode.

The command also defines the MSC server selection method for the pool area, using either the IMSI hash value, or round-robin.

This command is also used to remove an existing pool area.

A maximum of 24 pool areas can be configured per MME service.

When configured, the MME attempts to select an MSC using the following selection order:

1. Pool area that matches the PLMN and of type hash.
2. Pool area that matches the PLMN and of type round-robin.
3. Pool area that does not have PLMN associated and of type hash.
4. Pool area that does not have PLMN associated and of type round-robin .

Entering this command results in one of the following prompts, based on the pool selection method specified:

`[`*context_name*`]`*host_name*`(config-mme-pool-area-hash-value)#`

`[`*context_name*`]`*host_name*`(config-mme-pool-area-round-robin)#`

Additional commands are defined in the *MME MSC Server Pool Area Configuration Mode Commands* chapter.

Examples

The following command defines a pool area named *msc_pool_east* and configures it for the round robin selection mode.

pool-area *msc_pool_east* **type round-robin**

ps-lte

Configures the Public Safety LTE (PS-LTE) mode of operation for this MME service.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description **ps-lte sgw {** *ipv4_address* **|** *ipv6_address* **}**
no ps-lte

no

Disables PS-LTE mode of operation.

sgw { *ipv4_address* | *ipv6_address* }

Configures the IP address of the S11 interface of the S-GW to use for PS-LTE mode of operation.

ip_address specifies the IP address for the S-GW in IPv4 dotted-decimal or IPv6 colon-separated notation.

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

Use this command to enable the MME service for use in a Public Safety LTE (PS-LTE) network. In this mode, the MME is co-located with an S-GW and at least one P-GW, and the MME must always use the co-located S-GW and a co-located P-GW for all calls that it handles. This requires configuring the IP addresses of the S11 interface of the S-GW as part of the MME service configuration.

Configuration of the S5/S8 interface to the P-GW must be configured separately as part of an APN profile configuration (refer to the **pgw-address** command within the *APN Profile Configuration Mode* chapter in the *Command Line Interface Reference*).

When enabled, all other S-GW selection mechanisms are overridden. The MME will only use the S-GW configured for PS-LTE operation and the P-GW configured in the matching APN profile, regardless of any other configuration present.

Examples

The following command enables PS-LTE mode for this MME service and configures the IP address of the S11 interface for the S-GW as 192.60.60.7.

ps-lte sgw 192.60.60.7

relative-capacity

Configures a relative capacity variable that is sent to the eNodeB for use in selecting an MME in order to load balance the pool.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description **relative-capacity** *number*
default relative-capacity

default

Returns the command to its default setting of 255.

number

Specifies the relative capacity or weight of an MME compared to others in an MME pool as an integer from 0 through 255.

Default: 255

Usage Guidelines Use this command to configure the relative capacity or weight of this MME in comparison to other MMEs in a pool. This value is sent to the eNodeB in the S1AP S1 SETUP RESPONSE message.

If this value is changed after the S1 interface is initialized, the MME CONFIGURATION UPDATE message is used to update the eNodeB with the change.

Examples The following command sets this MME with a relative capacity or weight of *100*:
relative-capacity 100

s13

Enables the MME to send additional Mobile Identity check Requests (MICR) towards the EIR over the S13 interface.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description

[no] s13 additional-id-check { attach | handover | tau }

no

This command filter instructs the MME to remove and disable the specified feature configuration from the MME Service configuration.

additional-id-check { attach | handover | tau }

attach - This keyword instructs the MME to send additional MICR in response to an Attach procedure.

handover - This keyword instructs the MME to send additional MICR in response to a Handover procedure.

tau - This keyword instructs the MME to send additional MICR in response to a Tracking Area Update procedure.

Usage Guidelines

By default, this additional imei checking functionality is disabled. Use this command to configure the MME to send additional Mobile Identity check Requests (MICR) towards the EIR over the S13 interface. You must choose at least one triggering UE procedure. You may repeat the command as needed to configure multiple triggering UE procedures.

Examples

The following commands must be issued separately. They instruct the MME to send additional IMEI check Requests to the EIR during UE Attach procedures and UE Handovers :
s13 additional-id-check attach
s13 additional-id-check handover

s1-mme ip

Configures the quality of service (QoS) differentiated service code point (DSCP) used when sending packets of a particular 3GPP QoS class over the S1-MME interface.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description **s1-mme ip qos-dscp { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | cs0 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef }**
default s1-mme ip qos-dscp

qos-dscp { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | cs0 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef }

Default: **af11**

Specifies the DSCP for the specified QoS traffic pattern. **qos-dscp** can be configured to any one of the following:

af11: Assured Forwarding 11 per-hop-behavior (PHB)

af12: Assured Forwarding 12 PHB

af13: Assured Forwarding 13 PHB

af21: Assured Forwarding 21 PHB

af22: Assured Forwarding 22 PHB

af23: Assured Forwarding 23 PHB

af31: Assured Forwarding 31 PHB

af32: Assured Forwarding 32 PHB

af33: Assured Forwarding 33 PHB

af41: Assured Forwarding 41 PHB

af42: Assured Forwarding 42 PHB

af43: Assured Forwarding 43 PHB

be: Best effort forwarding PHB

cs0: Class Selector 0 PHB

cs1: Class Selector 1 PHB

cs2: Class Selector 2 PHB

cs3: Class Selector 3 PHB

cs4: Class Selector 4 PHB

cs5: Class Selector 5 PHB

cs6: Class Selector 6 PHB

cs7: Class Selector 7 PHB

ef: Expedited forwarding PHB

Usage Guidelines

DSCP levels can be assigned to specific traffic patterns to ensure that packets are delivered according to the precedence with which they are tagged. The diffserv markings are applied to the IP header of every subscriber packet transmitted over the S1-MME interface(s).

Examples

The following command sets the DSCP-level for traffic sent over the S1-MME interface to **af12**:
s1-mme ip qos-dscp af12

s1-mme sctp port

Configures the source Stream Control Transmission Protocol (SCTP) port that will be used for binding the SCTP socket to communicate with the eNodeB using S1AP with this MME service.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description

s1-mme sctp port *port_num*
default s1-mme sctp port

default

Sets the SCTP port to the default value of 36412 to communicate with the eNodeBs using S1-MME interface.

port_num

Specifies the SCTP port number to communicate with the eNodeBs using S1-MME interface as an integer from 1 through 65535. Default: 36412

Usage Guidelines Use this command to assign the SCTP port with SCTP socket to communicate with the eNodeB using S1AP.

Only one SCTP port can be associated with one MME service.

Examples The following command sets the default SCTP port number 699 for to interact with eNodeB using S1AP on S1-MME interface:
default s1-mme sctp port

s1-ue-context-release

Specifies the cause code to be sent in a UE-CONTEXT-RELEASE message initiated by the MME upon the reception of any unexpected procedure over Initial-UE from the eNodeB, such as TAU, Service Request, Extended Service Request, Attach Request..

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description

s1-ue-context-release reason init-ue-from-enodeb cause type { nas value *nas_value* **| radio value** *radio_value* **}**
default s1-ue-context-release reason init-ue-from-enodeb cause

default

Resets the MME Service configuration to the system defaults.

nas value *nas_value*

nas_value must be an integer from 0 to 4.

- 0 - Normal Release (default value)
- 1 - Authentication Failure
- 2 - Detach
- 3 - Unspecified
- 4 - CSG Subscription Expiry

radio value *radio_value*

radio_value must be an integer from 0 to 38.

- 0 - Unspecified
- 1 - TX2RELOCOverall Expiry

- 2 - Successful Handover
- 3 - Release due to E-UTRAN Generated Reason
- 4 - Handover Cancelled
- 5 - Partial Handover
- 6 - Handover Failure In Target EPC/eNB Or Target System
- 7 - Handover Target not allowed
- 8 - TS1RELOCoverall Expiry
- 9 - TS1RELOCprep Expiry
- 10 - Cell not available
- 11 - Unknown Target ID
- 12 - No Radio Resources Available in Target Cell
- 13 - Unknown or already allocated MME UE S1AP ID
- 14 - Unknown or already allocated eNB UE S1AP ID
- 15 - Unknown or inconsistent pair of UE S1AP ID
- 16 - Handover desirable for radio reasons
- 17 - Time critical handover
- 18 - Resource optimisation handover
- 19 - Reduce load in serving cell
- 20 - User inactivity
- 21 - Radio Connection With UE Lost
- 22 - Load Balancing TAU Required
- 23 - CS Fallback Triggered
- 24 - UE Not Available For PS Service
- 25 - Radio resources not available
- 26 - Failure in the Radio Interface Procedure
- 27 - Invalid QoS combination
- 28 - Inter-RAT redirection
- 29 - Interaction with other procedure
- 30 - Unknown E-RAB ID
- 31 - Multiple E-RAB ID instances
- 32 - Encryption and/or integrity protection algorithms not supported
- 33 - S1 intra-system Handover triggered
- 34 - S1 inter system Handover triggered

- 35 - X2 Handover triggered ...
- 36 - Redirection towards 1xRTT
- 37 - Not supported QCI value
- 38 - invalid CSG Id

Usage Guidelines

By default, an MME initiates the UE-CONTEXT-RELEASE with cause NAS-Normal-Release whenever the MME receives any procedure Request over Initial-UE if the UE is in the connected state. This command makes it possible for the operator to configure a preferred cause code for the reason of the disconnect.

Important In earlier releases, the keyword was **init-ue-from-enodeb-for-tau**. In release 19.2, the name and behavior associated with this keyword changed. the keyword name is **init-ue-from-enodeb**. In support of backward compatibility, the MME will accept configurations with either form of the keyword. When the operator explicitly saves the configuration, the configuration will save using the new form of the keyword.

Beginning with release 19.2, the **init-ue-from-enodeb** reason instructs the MME to initiate the UE-CONTEXT-RELEASE with cause NAS-Normal-Release whenever the MME receives a request over Initial-UE not just for TAU but for all TAU and non-TAU scenarios (such as Service Request, Attach, and Extended-Service-Request) if the UE is in the connected state.

Examples

Include 'Authentication Failure' as the cause included in the UE-CONTEXT-RELEASE:
s1-ue-context-release reason init-ue-from-enodeb cause type nas value 1

setup-timeout

Configures the timeout duration for setting up MME calls in this MME service.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description **setup-timeout** *dur*
default setup-timeout

default

Sets the call setup timeout duration to the default value of 60 seconds.

dur

Specifies the call setup timeout duration (in seconds) for MME calls after which the attempt will be discarded.

dur is an integer from 1 through 10000. Default: 60

Usage Guidelines Use this command to configured the timeout duration for setting up an MME call with an MME service. One this timer expires, the call setup procedure will be discarded within this MME service.

Examples The following command sets the default setup timeout duration of 60 seconds for MME calls:
default setup-timeout

sgw-retry-max

Sets the maximum number of SGW selection retries to be attempted during Attach/HO/TAU. By default, this functionality is not enabled.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Command Modes

Exec > Global Configuration > MME Service Configuration

configure > mme-service *profile_name*

Entering the above command sequence results in the following prompt:

`[local]`*host_name*`(config-mme-service`*profile_name*`)#`

Syntax Description

sgw-retry-max *max_number*
no sgw-retry-max

no

Disables the configuration for the maximum number of retries.

max_number

Sets the maximum number of retries possible. Enter an integer from 0 to 5. If 0 (zero) is configured, then the MME sends Create-Session-Request to the 1st SGW and if that SGW does not reply, the MME does not select any further SGW to retry. The MME then rejects the ongoing procedure (Attach/HO/TAU) and sends a Reject message.

Usage Guidelines

Using the this command sets a limit to the maximum number of SGW selection retries to be attempted during Attach/HO/TAU. This means, the total number of tries would be 1 (the initial try) + the sgw-retry-max value (the maximum number of retries).

Entering a value with this command overrides the default behavior. If no value is configured, then the MME uses or falls back to the default behavior which is in compliance with 3GPP TS 29.274, Section 7.6. The MME sends Create-Session-Request message to one SGW in the pool. If the SGW node is not available, the MME picks the next SGW from the pool and again sends a Create-Session-Request message. The MME repeats this process. For an Attach procedure, the MME tries up to five (1 + 4 retries) different SGWs from the pool. In the case of a HO procedure, the MME will try every SGW in the entire pool of SGWs sent by the DNS. If there are no further SGW nodes available in the DNS pool or if the guard timer expires, then MME stops trying and sends a Reject with cause "Network-Failure" towards the UE and the UE must restart the Attach/Handover procedure.

Benefits of this configuration -- The amount of signaling at Attach or Handover can be reduced and the amount of time to find an available SGW can be reduced.

If the **sgw-retry-max** command is configured under both the MME service and the Call-Control Profile, then the configuration under Call-Control Profile takes precedence.

Examples

Use this command to enable the functionality for limiting the number of SGWs tried during Attach/HO/TAU to 2 retries:

sgw-retry-max 2

snmp trap

Enables or disables the SNMP trap for S1 interface connection establishment.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description **[default | no] snmp trap { s1-initial-establishment | s1-path-establishment }**

default

Returns the command to its default setting of disabled.

no

Disables the SNMP trap.

s1-initial-establishment

Specifies that the SNMP trap for the initial S1 interface connection establishment is to be enabled or disabled.

s1-path-establishment

Specifies that the SNMP trap for the S1 path establishment is to be enabled or disabled.

Usage Guidelines Use this command to enable or disabled the SNMP trap for S1 interface connection establishment.

statistics

Configures the statistics collection mode for the MME service.

Product MME

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description **statistics collection-mode { enodeb | tai } [-noconfirm]**
default statistics collection-mode [-noconfirm]

default

Configures the command to its default setting, where statistics are collected per eNodeB.

collection mode { enodeb | tai }

Configures the collection mode for statistics.

enodeb: Default - Collect statistics per eNodeB.

tai: Collect statistics per TAI.

-noconfirm

Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage Guidelines Use this command to collect statistics for this MME service at the eNodeB level (default), or at the TAI level.

⚠

Caution Changing this collection mode **will restart the MME service** and will clear all statistics at the MME service and eNodeB level.

When configured to collect statistics per TAI, the MME will collect statistics only for the TAIs that are configured in the LTE TAI Management Database that is associated with the MME service.

If a specific TAI is configured within multiple TAI Management Databases, the records collected for that TAI will be a sum of all counters for all TAI Management Databases to which it belongs.

Refer to the *TAI Schema* chapter in the *Statistics and Counters Reference* for a listing of all bulk statistics impacted by this command.

Refer also to the **show mme-service statistics** command to display TAI statistics.

Examples

The following command configures this MME service to collect statistics per TAI, instead of per eNodeB.
statistics collection-mode tai -noconfirm

ue-db

Configures the UE database that is maintained by the MME as a cache of EPS contexts per UE keyed by IMSI/GUTI to allow the UE to attach by a Globally Unique Temporary Identity (GUTI) and reuse previously established security parameters. This cache will be maintained in each session manager where the first attach occurred for the UE.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

configure > context *context_name* **> mme-service** *service_name*

Entering the above command sequence results in the following prompt:

`[`*context_name*`]`*host_name*`(config-mme-service)#`

Syntax Description

ue-db purge-timeout *dur_mins*
default ue-db purge-timeout

default

Resets the UE database purge timer timeout to the default value of 10080 minutes.

purge-timeout ***dur_mins***

Sets the timeout duration (in minutes) for MME to store the UE database in cache memory. This timer starts when the UE goes dormant.

dur_mins is an integer from 1 through 20160. Default: 10080

Usage Guidelines

Use this command to set timeout duration for MME to hold UE database information in cache memory.

The MME DB acts as a cache for storing subscriber related information. This subscriber related information helps reduce signaling traffic. The MME DB is a part of the Session Manager and interfaces between the Session Manager Application and Evolved Mobility Management Manager to provide access to the cached data.

Examples

The following command configures the MME database cache timer to hold the UE information up to 7 days (10080 minutes) in the MME Database:
default ue-db purge-timeout