Call Control Profile Configuration Mode

The MME and SGSN each support a maximum of 1,000 call control profiles; only one profile can be associated with an operator policy.

By configuring a call control profile, the operator fine tunes any desired restrictions or limitations needed to control call handling per subscriber or for a group of callers across IMSI (International Mobile Subscriber Identity) ranges.

Command Modes

Call Control Profile configuration mode defines call-handling rules which can be combined with other profiles – such as an APN profile (see the *APN Profile Configuration Mode Commands* chapter) – when using the Operator Policy feature. The call control profile is a key element in the Operator Policy feature and the profile is not valid until it is associated with an operator policy (see the **associate** command in the *Operator Policy Configuration Mode Commands* chapter).

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

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

a-msisdn

Enables the MME to advertise support for Additional Mobile Station ISDN number (A-MSISDN) functionality to the HSS.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-call-control-profile-`*`profile_name`*`)#`

Syntax Description

`[ remove ] a-msisdn`

remove

Disables support for A-MSISDN functionality on the MME. Disabled is the default behavior.

Usage Guidelines

This command enables the MME to notify the HSS of support for Additional-MSISDN for the PLMN associated with this call-control profile in Update Location Request (ULR) messages. Complete the MME configuration to fully support A-MSISDN functionality by instructing the MME to support the AVPs as defined in 3GPP 29.274 Release 11. This is done by using the **3gpp-r11** keyword with the **diameter update-dictionary-avps** command in the HSS Peer Service configuration mode.

With A-MSISDN functionality configured, the MME informs the HSS of A-MSISDN support so the MME sends Feature-List AVP, with an A-MSISDN flag set and the MSISDN, in Update Location Request (ULR) messages over the S6a interface to the HSS at the time a UE Attaches.

If the the MSISDN (A-MSISDN) is available in the subscription data, the HSS sends the provisioned Additional-MSISDN together with the MSISDN in the Update Location Answer (ULA)or the Insert-Subscriber-Data-Request (ISDR). The MME uses the received A-MSISDN as a Correlation-MSISDN (C-MSISDN) in "SRVCC PS to CS Request" and/or in "Forward Relocation Request" messages.

Example

After the **a-msisdn** command has been used to enable support, disable A-MSISDN support with the following command:

```
remove a-msisdn
```

access-restriction-data

Enables the operator to assign a failure code to be included in reject messages if the attach rejection is due to access restriction data (ARD) checking in the incoming subscriber data (ISD) messages. The operator can also disable the ARD checking behavior.

Product

MME

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

access-restriction-data { eutran-not-allowed | failure-code *cause_code* **| no-check | target-access-restriction }**
remove access-restriction-data { failure-code | eutran-not-allowed | no-check | target-access-restriction }

remove

Removes the failure code setting or eutran-not-allowed override setting.

eutran-not-allowed

Overrides the eutran-not-allowed flag received in ISD/ULA messages from the HLR/HSS received during the Attach process. The overridden value will be sent to the RNC during PDP context activation (in RAB Assignment Request messages) so that the RNC subsequently avoids performing a handover to E-UTRAN. Configuration of the **eutran-not-allowed** parameter is valid only if SRNS relocation first has been configured in *Call Control Profile Configuration Mode* via the **srns-inter** and/or **srns-intra** commands. The call-control-profile then must be associated with an operator policy in *Operator Policy Configuration Mode* using the **associate** command. Once the operator policy is associated with the call-control-profile, inclusion of the E-UTRAN Service Handover Information Element in RAB Assignment Request and Relocation Request RANAP messages must be enabled. This is done by executing the **ranap eutran-service-handover-ie** command in *RNC Configuration Mode*.

failure-code *cause_code*

cause_code: Enter an integer from 2 through 111; default code is 13 (roaming not allowed in this location area [LA]).

Refer to the GMM failure cause codes listed below (from section 10.5.5.14 of the 3GPP TS 124.008 v7.2.0 R7):

- 2 - IMSI unknown in HLR
- 3 - Illegal MS
- 6 - Illegal ME
- 7 - GPRS services not allowed
- 8 - GPRS services and non-GPRS services not allowed
- 9 - MSID cannot be derived by the network
- 10 - Implicitly detached
- 11 - PLMN not allowed
- 12 - Location Area not allowed
- 13 - Roaming not allowed in this location area
- 14 - GPRS services not allowed in this PLMN
- 15 - No Suitable Cells In Location Area
- 16 -MSC temporarily not reachable
- 17 - Network failure
- 20 - MAC failure
- 21 - Synch failure
- 22 - Congestion
- 23 - GSM authentication unacceptable
- 40 - No PDP context activated
- 48 to 63 - retry upon entry into a new cell
- 95 - Semantically incorrect message
- 96 - Invalid mandatory information
- 97 - Message type non-existent or not implemented
- 98 - Message type not compatible with state
- 99 - Information element non-existent or not implemented
- 100 - Conditional IE error
- 101 - Message not compatible with the protocol state
- 111 - Protocol error, unspecified

no-check

Including this keyword with the command disables the ARD checking behavior.

target-access-restriction

Including this keyword with the command enables the target access restriction functionality. This functionality works a bit differently for the MME and SGSN:

- MME - No Rejection: if "target-access-restriction" is *not enabled*, then the source-MME *will not* reject the outbound RAU Request based on the ARD profile of the subscriber per the Access-Restriction-Data received in ULA/ULR using the RAT Type IE received in the Context Request.
- MME - Rejection: if "target-access-restriction" is *enabled*, then the source-MME *will* reject the outbound RAU Request based on the ARD profile of the subscriber per the Access-Restriction-Data received in ULA/ULR using the RAT Type IE received in the Context Request.
- SGSN - No Rejection: if "target-access-restriction" is *enabled*, and if "access-restriction-data no-check" is *enabled*, then the source-SGSN *will not* reject the outbound RAU Request based on the ARD profile of the subscriber per the Access-Restriction-Data received in ULA/ULR using the RAT Type IE received in the Context Request.
- SGSN - Rejection: if "target-access-restriction" is *enabled*, and if "access-restriction-data no-check" is *not enabled*, then the source-SGSN will ignore the "target-access-restriction enabled" configuration and the source-SGSN *will* reject the outbound RAU Request based on the ARD profile of the subscriber per the Access-Restriction-Data received in ULA/ULR using the RAT Type IE received in the Context Request.

Usage Guidelines

The only feature available to the MME for access-restriction-data is the target access restriction; all others are exclusive to the SGSN.

By default, the SGSN checks access restriction data (ARD) within incoming insert subscriber data (ISD) messages. This enables operator to selectively restrict subscribers in either 3G (UTRAN) or 2G (GERAN). The SGSN ARD checking behavior occurs during the attach procedure and if a reject occurs, the SGSN sends the subscriber an Attach Reject message with a configurable failure cause code.

With the target access restriction feature enabled, including the **no-check** keyword with the command instructs the source-SGSN not to reject the outbound RAU Request based on the ARD profile of the subscriber per the Access-Restriction-Data received in ULA/ULR using the RAT Type IE received in the Context Request.

With the target access restriction feature enabled, including the **remove** command filter with the **no-check** keyword instructs the SGSN to reject the outbound RAU Reject based on the ARD profile of the subscriber per the Access-Restriction-Data received in ULA/ULR using the RAT Type IE received in the Context Request.

Example

For this call control profile, the following command disables the ARD checking function:

```
access-restriction-data no-check
```

accounting context

Defines the name of the accounting context and optionally associates a GTPP group with this call control profile.

Product

ePDG

S-GW

SAEGW

SGSN

SaMOG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

`accounting context` *`ctxt_name`* **`[ aaa-group`** *`grp_name`* **`] [ gtpp group`** *`grp_name`* **`]`**
`remove accounting context [ aaa-group | gtpp ]`

remove

Removes the accounting configuration from this profile's configuration.

ctxt_name

Specifies the accounting context as an alphanumeric string of 1 through 79 characters.

aaa-group *grp_name*

Configures AAA Group for MRME.

*grp_name*is a string of 1 to 63 characters (any combination of letters and digits) to identify the aaa-group created with the **aaa-group** command in the Context configuration mode.

gtpp group *grp_name*

Identifies the GTPP group, where the GTPP related parameters have been configured in the GTPP Group Configuration mode, to associate with this call control profile.

*grp_name*is a string of 1 to 63 characters (any combination of letters and digits) to identify the GTPP group created with the **gtpp group** command in the Context configuration mode.

Usage Guidelines

This command can be used to associate a predefined GTPP server group - including all its associated configuration - with a specific call control profile. The GTPP group would have been defined with the **gtpp group** command (see the *Context Configuration Mode Commands* chapter).

If the GTPP group is not specified, then a default GTPP group in the accounting context will be used.

If this command is not specified, use the name of the accounting context configured in the SGSN service configuration mode (for 3G) or the GPRS service configuration mode (for 2G), either will automatically use a "default" GTPP group generated in that accounting context.

If the accounting context is specified in the GPRS service or SGSN service and in a call control profile, the priority is given to the accounting context of the call control profile.

Example

For this call control profile, the following command identifies an accounting context called *acctng1* and associates a GTPP server group named *roamers* with defined charging gateway accounting functionality.

```
accounting context acctng1 gtpp group roamers
```

accounting mode

Configures the mode to be used for accounting – GTPP (default), RADIUS/Diameter or None.

Product

ePDG

S-GW

SAEGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
accounting mode { gtpp | none | radius-diameter }
remove accounting mode
```

remove

Removes the accounting mode.

gtpp

Specifies that GTPP accounting is performed. This is the default method.

none

Specifies that no accounting will be performed for the call control profile.

radius-diameter

Specifies that RADIUS/Diameter will be performed for the call control profile.

Usage Guidelines

Use this command to specify the accounting mode for a call control profile. For additional information on accounting mode and its relationship to operator policy, refer to the *System Administration Guide*.

Example

The following command specifies that RADIUS/Diameter accounting will be used for the call control profile:

```
accounting mode radius-diameter
```

accounting stop-trigger

Configures the trigger point for accounting stop CDR. Default is on session deletion request.

Product

S-GW

SAEGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
accounting stop-trigger custom
default accounting stop-trigger
```

default

Accounting stop CDR triggered once Delete Session/Delete Bearer Request is received at S-GW.

custom

Accounting stop CDR triggered once Delete Session/Delete Bearer Response is received at S-GW.

Usage Guidelines

Use this command to specify the trigger point for accounting stop CDR for a call control profile.

Example

The following command specifies that accounting stop trigger would be at response of session deletion:

```
accounting stop-trigger custom
```

allocate-ptmsi-signature

Enables or disables the allocation of a P-TMSI (Packet Temporary Mobile Subscriber Identity) signature.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

`[ no | default ] allocate-ptmsi-signature`

no

Disables the allocation of the P-TMSI signature.

default

Resets the configuration value to the default, which is to allocate the P-TMSI signature.

Usage Guidelines

Use this command to enable or disable the allocation of the P-TMSI signature.

Example

`allocate-ptmsi-signature`

apn-restriction

Enables the APN restriction feature and configures the instruction for the SGSN on the action to take when an APN restriction value is received from the GGSN during an Update PDP Context procedure.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

`apn-restriction update-policy deactivate` *`restriction`*
`default apn-restriction`

default

Creates a default APN restriction configuration.

update-policy deactivate *restriction*

Specifies one of the two restriction types to define the appropriate action if the APN restriction value received conflicts with the stored value:

- **least-restrictive** set the least restrictive value applicable when there are no already active PDP context(s).
- **most-restrictive** sets the most stringent restriction required by any already active PDP context(s).

Usage Guidelines

When this feature is enabled, the SGSN will send the maximum APN restriction value in every CPC Request message sent to the GGSN. The SGSN expects to receive an APN restriction value in each PDP Context received from the GGSN. The SGSN stores and compares received APN restriction values to check for conflicts. In the case of a conflict, the SGSN rejects the PDP Context with appropriate messages and error codes to the MS.

If an APN restriction value is not assigned by the GGSN, the SGSN assumes the value of "1" (least restrictive) to allow APN restriction rules will be possible when valid values are assigned for new PDP Context(s) from the same MS.

The least or most restrictive values of the APN restriction are applicable only for the Gn SGSN, as the APN restriction can be present in UPCQ/UPCR for Gn SGSN and this configuration is required to determine the PDN to be de-activated when an APN restriction violation occurs during modification procedures in the Gn SGSN. In the case of S4-SGSN, the APN restriction arrives at the S4-SGSN only in Create Session Response during activation. During activation in S4-SGSN, a PDN connection that violates the current Maximum APN restriction is always de-activated. Therefore in the case of S4-SGSN, this CLI is used only for enabling or disabling APN restriction.

Example

The following command applies the lowest level of APN restrictions:

```
apn-restriction update-policy deactivate least-restrictive
```

associate

Associates various MME -specific lists and databases with this call control profile. On an SGSN, this command can be used to associate some of these MME-related items to GPRS and/or SGSN services in support of S4 functionality. For SaMOG, this command can be used to associate various SGW and SGSN CDR triggers for the call control profile.

Product

ePDG

MME

SGSN

SaMOG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
associate { access-policy policy_name | accounting-policy policy_name |
decor-profile profile_name access-type { all | eutran | nb-iot } |
ho-restrict-list list_name | hss-peer-service service_name [ s13-interface |
 s6a-interface | s13-prime-interface | s6d-interface ] | scef-service
service_name | tai-mgmt-db tai-db_name }
remove associate { access-policy | accounting-policy | decor-profile
profile_name access-type { all | eutran | nb-iot } | ho-restrict-list |
hss-peer-service [ s13-interface | s6a-interface | s13-prime-interface |
 s6d-interface ] | tai-mgmt-db }
```

remove

Remove the specified association definition from the call control profile.

access-policy *policy_name*

Specifies the access-policy to be associated with the call-control-profile.

policy_name must be an alphanumber string of 1 through 64 characters.

accounting-policy *policy_name*

SaMOG only.

Important With SaMOG mixed license, SaMOG supports both SGSN and SGW CDRs. With SaMOG 3G license, SaMOG supports only SGSN CDRs.

Associates the APN with specific pre-configured policies configured in the same context for SaMOG charging.

policy_name must be an alphanumber string of 1 through 63 characters.

decor-profile *profile_name* access-type { all | eutran | nb-iot }

Specifies the DECOR profile that is associated with the call-control-profile. *profile_name* must be an alphanumerric string of 1 through 63 characters.

A maximum number of 16 decor-profile associations can be configured for the call-control-profile.

access-type: Configures the type of network access for the decor-profile.

- **all** : Specifies allows all access types.
- **eutran**: Specifies the access type as E-UTRAN.
- **nb-iot**: Specifies the access-type as NB-IoT.

ho-restrict-list *list_name*

MME only.

Identifies the handover restriction list that should be associated with this call control profile.

list_name is a string of 1 to 64 characters (any combination of letters and digits).

hss-peer-service *service_name*

Associates a home subscriber server (HSS) peer service with this call control profile.

service_name is an existing HSS peer service expressed as a string of 1 to 63 characters (any combination of letters and digits).

[s13-interface | s6a-interface | s13-prime-interface | s6d-interface]

Optionally, identify the interface to be associated with the HSS service in this call control profile.

The **s13-interface** and the **s6a-interface** options apply to the MME only.

The **s13-prime-interface** and **s6d-interface** options apply to the SGSN only.

The **s6d-interface** is used by the SGSN to communicate with the HSS. It is a Diameter-based interface which supports location management, subscriber data handling , authentication , and fault recovery procedures.

The **s13-prime-interface** is used by the SGSN to communicate with the equiprement identity register (EIR). It is a Diameter-based interface which performs the mobile equipment (ME) identity check procedure.

Important The **s13-prime-interface** can only be used if an **s6d-interface** is configured.

tai-mgmt-db *tai-db_name*

Identifies the tracking area identifier (TAI) database that should be associated with this call control profile.

tai-db_name is a string of 1 to 64 characters (any combination of letters and digits).

This configuration overrides the S-GW selection and TAI list assignment functionality for a call that uses an operator policy associated with this call control profile. The TAI management object provides a TAI list for calls and provides S-GW selection functionality if a DNS is not configured for S-GW discovery for this operator policy or if a DNS discovery fails.

If a TAI management database is associated with a call-control-profile, and if DNS is used for S-GW lookups, then the DNS configuration for S-GW lookups must also be configured within the same call-control-profile using the **dns-sgw** command in the call-control-profile configuration mode.

On the S4-SGSN, use this option to associate a locally configured S-GW address for the RAI address for selection if operators wish to bypass DNS resolution of RAI FQDN. This option is valid only after the following commands have been executed on the S4-SGSN:

- The **tai-mgmt-db** command in *LTE Policy Configuration Mode*
- The **tai-mgmt-obj** command in *LTE TAI Management Database Configuration Mode*.
- The **tai** and **sgw-address** commands in *LTE TAI Management Object Configuration Mode*.

Usage Guidelines

Use this command to associate handover restriction lists, HSS service (and interfaces), and a TAI database with the call control profile. This ensures that the information is available for application when a Request is received.

For SaMOG, use this command to associate the SaMOG call control profile with an accounting policy configured in this context to provide triggers to generate CDRs. If no policy is configured, triggers based on

the call control profile will not be generated, and the accounting policy in the SaMOG service context will be used. Even if an accounting policy is also specified in a call control profile, the priority is given to the accounting policy of the APN profile.

Repeat the command as needed to associate each feature.

Example

Link HO restriction list named *HOrestrict1* with this call control profile:

```
associate ho-restrict-list HOrestrict1
```

The following command associates this SaMOG call control profile with an accounting policy called *acct1*:

```
associate accounting-policy acct1
```

attach access-type

Defines attach-related configuration parameters for this call control profile based on the access-type (GPRS, UMTS, or both) and location area list.

Important SGSN only: Before using this command, ensure that the appropriate location area code (LAC) information has been defined via the **location-area-list** command.

Product

MME

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
attach access-type { gprs | umts } { all | location-area-list instance
list_id } { failure-code code | user-device-release { before-r99 failure
code code | r99-or-later failure code code } }
default attach access-type { eps | gprs | umts } { all | location-area-list
 instance list_id } { failure-code | user-device-release { before-r99
failure code | r99-or-later failure code }
```

default

Restores the default values for the for the specified parameter.

access-type *type*

Defines the type of access to be allowed or restricted.

- **gprs**
- **umts**

all

Instructs the SGSN or MME to apply the command action to all location area lists. Location area lists should already have been created with the **location-area-list** command. The location area list consists of one or more LACs, location area codes, where the MS is when placing the call.

location-area-list instance *list_id*

Instructs the SGSN to apply the command action to a specific location area list. Location area lists should already have been created with the **location-area-list** command. The location area list consists of one or more LACs, location area codes, where the MS is when placing the call.

Using this keyword with either the **allow** or **restrict** keywords enables you to configure with more granularity.

list_id: Enter an integer between 1 and 5.

failure-code *fail_code*

Specify a GMM failure cause code to identify the reason an attach did not occur. This GMM cause code will be sent in the reject message to the MS.

Default: 14.

fail_code: Enter an integer from 2 to 111. Refer to the GMM failure cause codes listed below (from section 10.5.5.14 of the 3GPP TS 124.008 v7.2.0 R7):

- 2 - IMSI unknown in HLR
- 3 - Illegal MS
- 6 - Illegal ME
- 7 - GPRS services not allowed
- 8 - GPRS services and non-GPRS services not allowed
- 9 - MSID cannot be derived by the network
- 10 - Implicitly detached
- 11 - PLMN not allowed
- 12 - Location Area not allowed
- 13 - Roaming not allowed in this location area
- 14 - GPRS services not allowed in this PLMN
- 15 - No Suitable Cells In Location Area
- 16 -MSC temporarily not reachable

- 17 - Network failure
- 20 - MAC failure
- 21 - Synch failure
- 22 - Congestion
- 23 - GSM authentication unacceptable
- 40 - No PDP context activated
- 48 to 63 - retry upon entry into a new cell
- 95 - Semantically incorrect message
- 96 - Invalid mandatory information
- 97 - Message type non-existent or not implemented
- 98 - Message type not compatible with state
- 99 - Information element non-existent or not implemented
- 100 - Conditional IE error
- 101 - Message not compatible with the protocol state
- 111 - Protocol error, unspecified

Note It is mandatory to enable the command **attach restrict access-type gprs all** so that the failure code is saved after a re-boot. The **attach access-type gprs all failure-code < code >** command and the attach restrict access-type gprs all command work together and have to be enabled together.

user-device-release { before-r99 | r99-or-later } failure-code *code*

Default: disabled

Enables the SGSN to reject an Attach procedure based on the detected 3GPP release version of the MS equipment and selectively send a failure cause code in the reject message. The SGSN uses the following procedure to implement this configuration:

1. When Attach Request is received, the SGSN checks the subscriber's IMSI and current location information.
2. Based on the IMSI, an operator policy and call control profile are found that relate to this Attach Request.
3. Profile is checked for access limitations.
4. Attach Request is checked to see if the revision indicator bit is set
   - if not, then the configured common failure code for reject is sent;
   - if set, then the 3GPP release level is verified and action is taken based on the configuration of this parameter

One of the following options must be selected and completed:

- **before-r99**: Indicates the MS would be a 3GPP release prior to R99 and an appropriate failure code should be defined.

  failure-code *code*: Enter an integer from 2 to 111.

- **r99-or-later** : Indicates the MS would be a 3GPP Release 99 or later and an appropriate failure code should be defined.

  failure-code *code*: Enter an integer from 2 to 111.

Usage Guidelines

Once the IMSI of an incoming call is known and matched with a specific operator policy, according to the filter definition of the **mcc** command, then the associated call control profile is selected to determine how the incoming call is handled.

By default, all attaches are allowed. If no access limitations are needed, do not use the **attach** command.

Important Before using this command, ensure that the appropriate LAC information has been defined with the **location-area-list** command.

Use this command to define attach limitations for the call control profile.

Use this command to fine-tune the attach configuration specifying which calls/subscribers can attach and which calls are restricted from attaching and what failure code is included in the Reject message.

Attachment restrictions can be based on any one or combination of the options, such as location area code or access type. It is even possible to restrict all attaches.

The command can be repeated using different keyword values to further fine-tune the attachment configuration.

Related Commands

- Use the **attach restrict** command to restrict attaches.
- Use the **attach allow** command to re-enable restrictions after an **attach restrict** command has been used.

Example

The following example sets all restrictions for access-type gprs and specified release version to the default setting.

```
default attach access-type gprs all user-device-release before-r99
failure-code
```

attach allow

Configures the system to re-enable attaches that were previously restricted using the **attach restrict** command.

Important SGSN only: Before using this command, ensure that the appropriate location area code (LAC) information has been defined via the **location-area-list** command.

Product

MME

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

`[ no ] attach allow access-type { eps | gprs | umts } location-area-list instance` *instance_id* **`| routing-area-list instance`** *instance_id*

no

Deletes the specified attach configuration.

allow

Enables attaches in the configuration after an **attach restrict** command has been used.

access-type *type*

Defines the type of access to be allowed.

- **eps**
- **gprs**
- **umts**

location-area-list instance *instance_id*

Instructs the SGSN to apply the command action to a specific location area list. Location area lists should already have been created with the **location-area-list** command. The location area list consists of one or more LACs, location area codes, where the MS is when placing the call.

instance_id must be an integer from 1 to 5.

routing-area-list instance *instance_id*

Instructs the SGSN to apply the command action to a specific routing area list. Routing area lists should already have been created with the **routing-area-list** command.

instance_id must be an integer from 1 to 5.

Usage Guidelines

Once the IMSI of an incoming call is known and matched with a specific operator policy, according to the filter definition of the **mcc** command, then the associated call control profile is selected to determine how the incoming call is handled.

By default, all attaches are allowed. If no access limitations are needed, then do not use the **attach** command.

Important Before using this command, ensure that the appropriate LAC information has been defined with the **location-area-list** command.

Use this command to define attach limitations for the call control profile.

Use this command to fine-tune the attach configuration specifying which calls/subscribers can attach and which calls are restricted from attaching and what failure code is included in the Reject message.

Attachment restrictions can be based on any one or combination of the options, such as location area code or access type or routing area code. It is even possible to restrict all attaches.

The command can be repeated using different keyword values to further fine-tune the attachment configuration.

Related Commands

- Use the **attach access-type** command to define the type of access to restrict or allow.
- Use the **attach restrict** command to restrict attaches.

Example

For calls under the purview of this call control profile, the following command allows attaches of **all** subscribers using the GPRS access type.

```
attach allow access-type gprs all
```

attach imei-query-type

Defines device Attach limitations for this call control profile if an IMEI is not already present in the Attach Request.

Product

MME

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
attach imei-query-type { imei | imei-sv | none } [
verify-equipment-identity [ allow-on-eca-timeout | deny-greylisted |
deny-unknown | verify-emergency ] + ]
remove attach imei-query-type
```

remove

Deletes the specified attach configuration.

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

Configures system behavior during Attach procedures if an IMEI is not already present in the Attach Request.

- **imei**: Specifies that the system is required to query the UE for its International Mobile Equipment Identity (IMEI).
- **imei-sv**: Specifies that the system is required to query the UE for its International Mobile Equipment Identity - Software Version (IMEI-SV).
- **none**: Specifies that the system 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.

Usage Guidelines

Configures system settings related to the UE Attach procedure for the specified call control profile

The command can be repeated using different keyword values to further fine-tune the attachment configuration.

Example

The following command configures the system to query the UE for its IMEI and to verify the UE equipment identity with an Equipment

```
attach imei-query-type imei verify-equipment-identity
```

attach implicit-ulr

Configures the implicit sending of ULR during local GUTI attach.

Product

MME

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description **`attach implicit-ulr`**

Example

The following command configures the implicit sending of ULR during local GUTI attach

`attach implicit-ulr`

attach restrict

Configures the system to restrict attaches based on access type, routing areas, and location areas (either all or specified location area list) for this call control profile.

Important SGSN only: Before using this command, ensure that the appropriate location area code (LAC) information has been defined via the **location-area-list** command.

Product MME

SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description **`[ no ] attach restrict access-type { eps [ emm-cause-code`** *`code`* **| imsi-attach-fail [emm-cause-code`** *`code`* **] | voice-unsupported [ emm-cause-code`** *`code`* **]] | gprs | umts } { all | location-area-list instance`** *`instance_id`* **| routing-area-list instance`** *`instance_id`* **}**

no

Deletes the specified attach configuration.

access-type *type*

Defines the type of access to be allowed or restricted.

- **eps**
- **gprs**

- **umts**

emm-cause-code *code*

Specifies the EPS Mobility Management (EMM) cause code to return to the UE:

- **eps-service-disallowed**
- **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**

The default cause code is **no-suitable-cell-in-tracking-area**.

Important The **tracking-area-not-allowed** cause code is not supported for the MME.

Important The **roaming-not-allowed-in-this-tracking-area** and **tracking-area-not-allowed** cause codes are not applicable for use with the **imsi-attach-fail** or **voice-unsupported** keywords.

imsi-attach-fail

Directs the MME to restrict EPS attach when IMSI attach fails. If the policy is configured, all IMSI failures will result in a EPS restriction.

The default cause code for calls rejected for imsi-attach-fail is **no-suitable-cell-in-tracking-area**.

voice-unsupported

Directs the MME to restrict EPS attach when voice is not supported, such as when Voice over IMS is not supported and the UE does not support Circuit Switched Fall Back (CSFB).

This setting is applicable when all of the following conditions apply:

- The UE is voice-centric as determined in the UE usage setting of the Voice Domain and UE Settings IE sent in the request.
- The UE does not support CSFB as determined in the EMM Combined procedures Capability bit of the MS Network Capability IE sent in the request, OR if CSFB is not supported on the MME as determined by the SGs service not being associated with the MME service.
- Voice over IMS is not supported in the network as defined by the **network-feature-support-ie ims-voice-over-ps** command.

The default cause code for calls rejected for voice-unsupported is **no-suitable-cell-in-tracking-area**.

all

Instructs the system to apply the command action to all location area lists. Location area lists should already have been created with the **location-area-list** command. The location area list consists of one or more LACs, location area codes, where the MS is when placing the call.

location-area-list instance *instance_id*

Instructs the SGSN to apply the command action to a specific location area list. Location area lists should already have been created with the **location-area-list** command. The location area list consists of one or more LACs, location area codes, where the MS is when placing the call.

Using this keyword with either the **allow** or **restrict** keywords enables you to configure with more granularity.

instance_id must be an integer from 1 to 5.

Important This keyword only applies to the SGSN.

routing-area-list instance *instance_id*

Instructs the SGSN to apply the command action to a specific routing area list. Routing area lists should already have been created with the **routing-area-list** command.

instance_id must be an integer from 1 to 5.

Usage Guidelines

Once the IMSI of an incoming call is known and matched with a specific operator policy, according to the filter definition of the **mcc** command, then the associated call control profile is selected to determine how the incoming call is handled.

By default, all attaches are allowed. If no access limitations are needed, then do not use the **attach** command.

Important Before using this command, ensure that the appropriate LAC information has been defined with the **location-area-list** command.

Use this command to restrict attaches for the call control profile.

Use this command to fine-tune the attach configuration specifying which calls/subscribers can attach and which calls are restricted from attaching and what failure code is included in the Reject message.

Attachment restrictions can be based on any one or combination of the options, such as location area code or access type or routing area code. It is even possible to restrict all attaches.

The command can be repeated using different keyword values to further fine-tune the attachment configuration.

Related Commands

- Use the **attach access-type** command to define the type of access to restrict or allow. The command attach restrict **access-type gprs all** has to be enabled , if the command attach **access-type gprs all failure-code < code >** is used to define a failure code. The failure code is saved after a re-boot only when the command attach restrict access-type gprs all is enabled.
- Use the **attach allow** command to re-enable restrictions after an **attach restrict** command has been used.

Example

For calls under the purview of this call control profile, the following command restricts the attaches of **all** subscribers using the GPRS access type.

```
attach restrict access-type gprs all
```

To change the attach restriction to only restrict attaches of GPRS subscribers from specified LACs included in location area list #2 and include failure-code 45 as the reject cause. This configuration requires two CLI commands:

```
attach restrict access-type gprs location-area-list instance 2
attach access-type gprs location-area-list instance 2 failure-code 45
```

In the case of a dual-access SGSN, it is possible to also add a second definition to restrict attaches of UMTS subscribers within the LACs included in location area list #3.

```
attach restrict access-type UMTS location-area-list instance 3
```

Change the configuration to allow attaches for GPRS access for all previously restricted LACs - note that GPRS attaches would still be limited:

```
no attach restrict access-type gprs all
```

Restrict (deny) all GPRS attach requests (coming from any location area) and assign a single failure code for the reject messages. This is a two command process:

```
attach restrict access-type
gprs all
attach access-type grps
all failure-code 22
```

authenticate all-events

Allows the operator to quickly define authentication procedures, based on limited parameters, for all types of events.

Product

MME

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
authenticate all-events [ access-type { gprs | umts } | frequency frequency
 [ access-type { gprs | umts } ] | periodicity duration [ access-type {
gprs | umts } ] ]
 no authenticate all-events [ access-type { gprs | umts } ]
```

```
remove authenticate all-events [ access-type { gprs | umts } | frequency
 [ access-type { gprs | umts } ] | periodicity [ access-type { gprs |
umts } ]
```

no

Disables the specified authentication configuration in the call control profile.

remove

Removes the specified authentication configuration from the call control profile configuration file.

access-type *type*

One of the following must be selected to identify the type of network access if the **access-type** keyword is included in the command:

- **gprs**
- **umts**

The **access-type** keyword can be included with any of the other three keywords available with the **authenticate all-events** command.

frequency *frequency*

This keyword defines 1-in-N selective authentication for all types of subscriber events. If the frequency is set for 12, then the service skips authentication for the first 11 events and authenticates on the 12th event.

In releases prior to 21.2, the *frequency* is an integer value from 1 up to 16.

From release 21.2 onwards the *frequency* is an integer value from 1 up to 256.

periodicity *duration*

The periodicity configured specifies authentication periodicity. The periodicity is an integer with a range "1" up to "10800" minutes. For example, if the configured periodicity is "20" minutes, the UE is authenticated at every "20" minutes.

Usage Guidelines

By default, authentication is not performed for any subscriber events. Use this command to enable authentication for all types of events at one time, such as but not limited to: Activate Requests, Attach Requests, Detach Requests, Service-Requests.

Important For the SGSN, in releases 15.0 and forward, the authentication on activation functionality has been removed so the SGSN will not authenticate on Activate Requests.

Example

The following command configures all authentication for all subscriber events to occur every tenth time a specific type of event occurs (for example every tenth time an Attach Request is received):

```
authenticate all-events frequency 10
```

The following command configures authentication for all Detach Requests and RAUs to occur if the UE access-type is UMTS:

authenticate all-events access-type umts

authenticate attach

Allows the operator to define authentication for Attach procedures.

Product

MME

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

authenticate attach access-type { gprs | umts }
authenticate attach attach-type { combined | gprs-only } [access-type { gprs | umts } | frequency *frequency* **]**
authenticate attach frequency *frequency* **[access-type { gprs | umts }]**
authenticate attach inter-rat [access-type { gprs | umts } | attach-type { combined | gprs-only } [access-type { gprs | umts } | frequency *frequency* **] | frequency** *frequency* **[access-type { gprs | umts }] | periodicity** *duration* **[access-type { gprs | umts }]]**
authenticate attach periodicity *duration* **[access-type { gprs | umts }]**
{ no | remove } authenticate attach [access-type { gprs | umts } | attach-type { combined | gprs-only } | inter-rat | attach-type { combined | gprs-only }] [access-type { gprs | umts }]]

no

Disables the defined authentication procedures configured for Attach Requests from the call control profile.

remove

Deletes the defined authentication procedures for Attach Requests from the call control profile configuration file.

access-type *type*

One of the following must be selected to identify the type of network access if the **access-type** keyword is included in the command:

- **gprs**
- **umts**

attach-type

This keyword configures the Attach authentication based on the type of attach requested. The **attach-type** must be one of the following options:

- **combined**: Authenticates combined GPRS/IMSI Attaches.
- **gprs-only**: Authenticates GRPS Attaches only.

frequency *frequency*

This keyword defines 1-in-N selective authentication for this type of subscriber event - Attach Request. If the frequency is set for 12, then the service skips authentication for the first 11 events and authenticates on the twelfth event.

In releases prior to 21.2, the *frequency* is an integer value from 1 up to 16.

From release 21.2 onwards the *frequency* is an integer value from 1 up to 256.

inter-rat

Enables/disables authentication for Inter-RAT Attaches.

periodicity *duration*

The periodicity configured specifies authentication periodicity. For example, if the configured periodicity is "20" minutes, the UE is authenticated at every "20" minutes.

The *duration*is an integer with a range "1" up to "10800" minutes.

Usage Guidelines

Authentication for Attach is disabled by default. This command enables/disables authentication for an Attach with a local P-TMSI or Attaches with an IMSI, which will be authenticated to acquire the CK (cipher key) and the IK (integrity key).

Example

The following command configures authentication to occur after every tenth attach event for GPRS access.

```
authenticate attach frequency 10 access-type gprs
```

The following command disables authentication for Inter-RAT Attaches, use:

```
no authenticate attach inter-rat
```

authenticate context

This command allows you to specify the authentication group, authentication method, context, and type of authentication for the AAA server.

Product

SaMOG

ePDG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

`authenticate context` *`context_name`* **`[ aaa-group`** *`aaa_group_name`* **`] [ auth-type { diameter | radius } ] [ auth-method { [ eap ] [non-eap] } ]`**
`remove authenticate context [ aaa-group ]`

remove

Sets the authentication type to its default value:

Default (SaMOG 3G license): radius

Default (SaMOG Mixed Mode license): diameter

context_name

Specified the name of the context for authentication.

context_name must be an alphanumeric string of 1 through 79 characters.

aaa-group *aaa_group_name*

Optionally, specifies the AAA group for MRME. *aaa_group_name* must be an alphanumeric string of 1 through 63 characters.

auth-method { [eap] [non-eap] }

Optionally, specifies the authentication method for the call control profile.

If this configuration is not used, the default value is EAP based authentication method.

Important The SaMOG Web Authorization feature is license dependent. Contact your Cisco account representative for more information on license requirements.

Usage Guidelines

Use this command to specify the authentication group, context, and type of authentication for the AAA server. Also specify an authentication method of EAP or non-EAP or both for the call control profile in the operator policy.

Example

The following command configures authentication of a context named *cxtSaMOG*, specifies AAA group named *AAASaMOG*, and sets the authentication to a DIAMETER-based authentication:

`authenticate context cxtSAMOG aaa-group AAASaMOG auth-type diameter`

authenticate detach

Allows the operator to enable and define authentication for Detach procedures.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

`authenticate detach [ access-type umts ]`
`[ no | remove ] authenticate detach [ access-type umts ]`

no

Disables the defined authentication procedures configured for Detach Requests from the call control profile.

remove

Deletes the defined authentication procedures for Detach Requests from the call control profile configuration file.

access-type umts

Optionally, identifies the type of network access if the **access-type umts** keywords are included in the command. By default, access-type UMTS is assumed.

Usage Guidelines

Authentication for Detach procedures is disabled by default. This command enables/disables authentication for a Detach Request and allows the operator to limit authentication based on the MS/UE access-type.

Example

The following command configures detach authentication to occur only for UMTS attached subscribers:

`authenticate detach access-type umts`

The following command disables authentication for all Detach Requests, use:

`no authenticate detach`

authenticate on-first-vector

Allows the operator to enable the SGSN to begin MS authentication immediately after receiving the first vector from the HLR.

Product SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

```
authenticate on-first-vector
remove authenticate on-first-vector
```

remove

Removes the authenticate on-first-vector definition from the configuration file and resets the default behavior so that the SGSN waits to receive all vectors before beginning authentication towards the MS.

Usage Guidelines After an initial attach request, some end devices restart themselves after waiting for the PDP to be established. In such cases, the SGSN restarts and a large number of end devices repeat their attempts to attach. The attach requests flood the radio network, and if the devices timeout before the PDP is established then they continue to retry, thus even more traffic is generated.

To avoid the high traffic levels during PDP establishment, the SGSN has been modified to reduce the attach time, as much as possible, so that the devices can attach and discontinue sending requests. The current enhancement is intended to reduce the time needed to retrieve vectors over the GR interface by allowing the operator to configure the SGSN to start authentication towards the MS as soon as it receives the first vector from the AuC/HLR. With the new command included in the configuration, the SGSN begins the MS authentication process immediately after receiving the first vector from the HLR while the SAI continues in parallel.

Example

Use the following command to configure the SGSN to begin MS authentication immediately after receiving the first vector from the AuC/HLR:

```
authenticate on-first-vector
```

Use the following command to reset the default behavior, so that the SGSN waits to receive all vectors requested in the SAI from the AuC/HLR before begining authentication towards the MS:

```
remove authenticate on-first-vector
```

authenticate rau

Enables or disables and fine tunes authentication procedures for routing area updates (RAUs)

Product SGSN

Privilege Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

authenticate rau [access-type { gprs | umts } | frequency *frequency* **[access { gprs | umts }] | periodicity** *duration* **[access { gprs | umts }] | update-type { combined-update | imsi-combined-update | periodic | ra-update } [access-type { gprs | umts } | frequency** *frequency* **| periodicity** *duration* **| with { foreign-ptmsi | inter-rat-local-ptmsi | local-ptmsi } [access-type { gprs | umts } | frequency** *frequency* **| periodicity** *duration* **]**

no authenticate rau [access-type { grps | umts } | update-type { combined-update | imsi-combined-update | periodic | ra-update } [access-type { gprs | umts } | with { foreign-ptmsi | inter-rat-local-ptmsi | local-ptmsi } [access-type { gprs | umts }]
remove authenticate rau [access-type { gprs | umts } | periodicity [access { gprs | umts }] | update-type { combined-update | imsi-combined-update | periodic | ra-update } [access-type { gprs | umts } | periodicity | with { foreign-ptmsi | inter-rat-local-ptmsi | local-ptmsi } [access-type { gprs | umts } | periodicity]]

no

Disables authentication for the RAUs specified in the configuration for the call control profile.

remove

Deletes the authentication configuration for the RAUs from the call control profile in the configuration file.

access-type *type*

One of the following must be selected to identify the type of network access if the **access-type** keyword is included in the command:

- **gprs**
- **umts**

The **access-type** keyword can be included with any of the other keywords available with the **authenticate rau** command.

frequency *frequency*

Defines 1-in-N selective authentication for RAU events. If the frequency is set for 12, then the SGSN skips authentication for the first 11 events and authenticates on the twelfth event.

In releases prior to 21.2, the *frequency* is an integer value from 1 up to 16.

From release 21.2 onwards the *frequency* is an integer value from 1 up to 256.

periodicity *duration*

Defines the length of time (number of minutes) that authentication can be skipped.

duration: Must be an integer from 1 to 10800.

update-type

Defines the type of RAU Request. Select one of the following:

- **combined-update [access-type | with inter-rat-local-ptmsi]**
- **imsi-combined-update [access-type | with inter-rat-local-ptmsi]**
- **periodic [access-type | frequency | periodicity]**
- **ra-update [access-type | with inter-rat-local-ptmsi]**

Usage Guidelines

By default, authentication is not performed for routing area updates (RAUs). Use this command to enable/disable authentication and to fine tune the authentication procedure based on frequency, periods for skipping authentication and the various types of routing area updates.

Example

The following command configures RAU authentication to occur after every tenth event for GPRS access.

```
authenticate rau frequency 10 access-type gprs
```

The following command disables authentication for RAUs based on the combined IMSI with foreign P-TMSIs, use:

```
no authenticate rau imsi-combined-update with foreign-ptmsi
```

The following command deletes all authentication configuration from the call control profile for all RAUs using GPRS access-type:

```
remove authenticate rau access-type gprs
```

authenticate service-request

Enables or disables and fine-tunes authentication procedures for Service Requests.

Product

MME

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
authenticate service-request [ frequency frequency | periodicity duration |
 service-type { data | page-response | signaling } [ frequency frequency |
 periodicity  duration ] ]
no authenticate service-request [ service-type { data | page-response |
signaling } ]
remove authenticate service-request [ frequency | periodicity  |
service-type { data | page-response | signaling } [ frequency | periodicity
 ] ]
```

no

Disables authentication for the Service Requests specified in the configuration for the call control profile.

remove

Deletes the authentication configuration for Service Requests from the call control profile in the configuration file.

frequency *frequency*

Defines 1-in-N selective authentication for this type of subscriber event - Service Request. If the frequency is set for 12, then the service skips authentication for the first 11 events and authenticates on the twelfth event.

In releases prior to 21.2, the *frequency* is an integer value from 1 up to 16.

From release 21.2 onwards the *frequency* is an integer value from 1 up to 256.

periodicity *duration*

Defines the length of time (number of minutes) that authentication can be skipped.

duration: Must be an integer from 1 to 10800.

signaling-type

Defines the type of service being requested by the Service Request. Select one of the following:

- **data**
- **page-response**
- **signaling**

Usage Guidelines

By default, authentication is not performed for Service Requests. Use this command to enable/disable authentication and to fine-tune the authentication procedure based on frequency and periods for skipping authentication and the various types of service. Repeat the commands as needed to configure criteria for all service types.

Example

The following command configures authentication Service Requests for data service to only occur every 5 minutes:

```
authenticate service-request service-type data periodicity 5
```

authenticate sms

Enables or disables and fine tunes authentication procedures for Short Message Service (SMS).

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
authenticate sms [ access-type { gprs | umts } | frequency frequency [
access-type { gprs umts } ] | sms-type { mo-sms | mt-sms } [ access-type
 { gprs | umts } | frequency frequency ] ]
[ no | remove ] authenticate sms [ access-type { gprs | umts } | sms-type
 { mo-sms | mt-sms } [ access-type { gprs umts } ] ]
```

no

Disables authentication for the SMS Requests specified in the configuration for the call control profile.

remove

Deletes the authentication configuration for SMS Requests from the call control profile in the configuration file.

access-type *type*

One of the following must be selected to identify the type of network access if the **access-type** keyword is included in the command:

- **gprs**
- **umts**

The **access-type** keyword can be included with any of the other keywords available with the **authenticate sms** command.

frequency *frequency*

Defines 1-in-N selective authentication for SMS Requests. If the frequency is set for 12, then the SGSN skips authentication for the first 11 events and authenticates on the twelfth event.

In releases prior to 21.2, the *frequency* is an integer value from 1 up to 16.

From release 21.2 onwards the *frequency* is an integer value from 1 up to 256.

sms-type

Enables authentication for the following SMS types:

- **mo-sms**: mobile-originated SMS
- **mt-sms**: mobile-terminated SMS

Usage Guidelines

By default, authentication is not performed for short message service (SMS). Use this command to enable/disable authentication and to fine-tune the authentication procedure based on MS/UE access type and the frequency for the selected SMS type. Repeat the commands as needed to configure criteria for all service types.

Example

The following command configures MO-SMS authentication to occur every fifth request:

```
authenticate sms sms-type mo-sms frequency 5
```

authenticate tau

Allows the operator to enable/disable and fine-tune authentication for the tracking area update (TAU) procedures.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
authenticate tau [ freqency frequency | inter-rat | periodicity interval ]
authenticate tau frequency frequency
authenticate tau inter-rat [ frequency frequency | periodicity duration ]
authenticate tau intra-rat [ frequency frequency | periodicity duration ]
authenticate tau normal [ frequency frequency | periodicity duration ]
authenticate tau periodic [ frequency frequency | periodicity duration ]
authenticate tau periodicity duration
remove authenticate tau frequency
remove authenticate tau inter-rat [ frequency | periodicity ]
remove authenticate tau intra-rat [ frequency | periodicity ]
remove authenticate tau normal [ frequency | periodicity ]
remove authenticate tau periodic [ frequency | periodicity ]
remove authenticate tau periodicity
no authenticate tau
```

no

Disables the TAU authentication procedures specified in the call control profile configuration.

remove

This keyword removes the configured TAU authentication procedures.

frequency *frequency*

Defines 1-in-N selective authentication for this type of subscriber event - a tracking area update for an inter-RAT Attach. If the frequency is set for 12, the MME skips authentication for the first 11 events and authenticates on the twelfth event.

In releases prior to 21.2, the *frequency* is an integer value from 1 up to 16.

From release 21.2 onwards the *frequency* is an integer value from 1 up to 256.

inter-rat

Enables authentication for TAU procedures for inter-RAT Attaches.

intra-rat

This keyword specifies authentication to be applied for Intra-RAT TAU.

normal

This keyword specifies authentication to be applied for normal (TA/LA update) TAU.

periodic

This keyword specifies authentication to be applied for periodic TAU.

periodicity *duration*

Defines the length of time (number of minutes) that authentication can be skipped.

duration: Must be an integer from 1 to 10800.

Usage Guidelines

Authentication for TAU procedures is disabled by default. This command enables/disables authentication for a inter-RAT TAU procedures and allows the operator to limit authentication based on the frequency of the events or elapsed intervals between the events.

Example

The following command configures TAU authentication to occur when there is 15 minutes between inter-RAT Attaches:

```
authenticate tau periodicity 15
```

The following command disables authentication for all TAU Inter-RAT Attaches, use:

```
no authenticate tau
```

cc

Defines the charging characteristics to be applied for CDR generation when the handling rules are applied via the Operator Policy feature.

Product

ePDG

MME

SAEGW

S-GW

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

```
cc { behavior-bit no-records bit_value | gen-cdr-for-profile { [ 0 ] [ 1 ]
 [ 10 ] [ 11 ] [ 12 ] [ 13 ] [ 14 ] [ 15 ] [ 2 ] [ 3 ] [ 4 ] [ 5 ] [ 6 ]
 [ 7 ] [ 8 ] [ 9 ] } | local-value behavior bit_value profile index_bit |
prefer { hlr-hss-value | local-value } }
no cc { behavior-bit no-records | gen-cdr-for-profile }
remove cc { behavior-bit no-records | local-value | prefer }
```

no

Disables the no records generation behavior-bit configuration for this call control profile.

In 21.7 and later releases, use the **no cc gen-cdr-for-profile** CLI command to disable the Controlled SGWCDR Generation feature. In other words, the SGWCDR generation will happen as before.

Important The Controlled SGWCDR Generation feature is not fully qualified in release 21.7. It is available only for testing purposes. For more information, contact your Cisco Accounts representative.

remove

Removes the specified charging characteristic configuration from this profile.

behavior-bit no-records *bit_value*

Default: disabled

Specifies the charging characteristic behavior bit. **no-records** instructs the system not to generate any accounting records regardless of what may be configured elsewhere.

bit_value is an integer from 1 through 12.

gen-cdr-for-profile { [0] [1] [10] [11] [12] [13] [14] [15] [2] [3] [4] [5] [6] [7] [8] [9] }

Important The Controlled SGWCDR Generation feature is not fully qualified in release 21.7. It is available only for testing purposes. For more information, contact your Cisco Accounts representative.

Use this CLI command to generate SGWCDR based on certain Charging-Characteristics profile value received in Charging-Characteristics IE inside CSReq.

- **0 … 15**: Configures CC-profile number 0 for SGWCDR generation ... Configures CC-profile number 15 for SGWCDR generation.

Existing CLI commands for SGWCDR generation are not impacted:

- The **cc gen-cdr-for-profile** CLI command takes effect only if the existing **cc behavior-bit no-records** CLI command has no impact based on Charging-Characteristics profile value received.
- The existing **accounting-mode gtpp** CLI command is still required for SGWCDR generation.

The Controlled SGWCDR Generation feature will not work if the **cc prefer local-value** CLI command is configured.

Subsequent configuration of **cc gen-cdr-for-profile** CLI command results in earlier values being discarded.

The values of **cc gen-cdr-for-profile** CLI command are applicable only for new subscribers connected after the CLI is configured.

local-value behavior *bit_value* profile *index_bit*

Defaults: bit_value = 0x0, index_bit = 8

Sets the local value of the behavior bits and profile index for the charging characteristics when the HLR/HSS does not provide values for these parameters.

bit_value is a hexadecimal value between 0x0 and 0xFFF.

index_bit is an integer value from 1 through 15.

Setting the profile index bis selects different charging trigger profiles to be used with the call control profile. Some of the index values are predefined according to 3GPP standard:

- **1** for hot billing
- **2** for flat billing
- **4** for prepaid billing
- **8** for normal billing

If the HLR/HSS provides the charging characteristics with behavior bits and profile index and the operator prefers to ignore the HLR/HSS values, then *also* configure the **prefer local-value** keyword.

prefer { hlr-hss-value | local-value }

Default: **hlr-hss-value**

Specifies a preference for using charging characteristics settings received from HLR or HSS, or those set by the SGSN or MME locally with the **local-value behavior** command.

- **hlr-hss-value** sets the call control profile to use charging characteristics settings received from HLR or HSS. This is the default preference.
- **local-value** sets the call control profile to use charging characteristics settings from the SGSN or MME only. If no charging characteristics are received from the HLR/HSS then local values will be applied.

Usage Guidelines

Use this command to set the behavior for charging characteristic comings from either an HLR/HSS or locally from an MME/SGSN.

These charging characteristics parameters can also be set within an APN profile with the commands of the APN Profile configuration mode. For generation of M-CDRs, the parameters configured in this mode, Call Control Profile configuration mode, will prevail but for generation of S-CDRs the parameters configured in the APN Profile configuration mode will prevail.

The 12 behavior bits (of the **local-value behavior** keyword) can be used to enable or disable CDR generation.

Example

The following command specifies a rule not to generate charging records (CDRs) and sets the charging characteristics behavior bit to *2*:

```
cc behavior-bit no-records 2
```

check-zone-code

Enables or disables the zone code checking mechanism.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

[no | remove] check-zone-code

no

Included with the command, this keyword disables the mechanism.

remove

Included with the command, this keyword causes the removal of the current **check-zone-code** configuration and returns to the SGSN to the default where zone-code checking is enabled.

Usage Guidelines Use this command to enable/disable the zone-code checking function.

Example

Disable checking of the zone code:

```
no check-zone-code
```

ciot-optimisation

This command is used to configure Control Plane (CP) CIoT optimization for an UE.

Product MME

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
ciot-optimisation { cp-optimisation { access-type { all | nb-iot |
wb-eutran } |  ciot-capable-ue } | eps-attach-wo-pdn access-type { all |
 nb- iot | wb-eutran } }
remove ciot-optimisation cp-optimisation  ciot-capable-ue
remove ciot-optimisation eps-attach-wo-pdn access-type { all | nb-iot |
wb-eutran }
```

remove

The keyword remove deletes the existing configuration.

cp-optimisation

Use this keyword to enable Control Plane optimization for an UE.

access-type

Use this keyword to specify the access type extension on which control plane optimization should be enabled. Control plane optimization and EPS attach without PDN can be enabled on both NB-IoT and WB-EUTRAN RATs or on either of them.

ciot-capable-ue

Uses only the ue-nw-capability to determine whether CP optimization or not.

all

Use this keyword to enable control plane optimization on both RAT types WB-EUTRAN and NB-IOT. This keyword is provided to the operator for the ease of configuring. Both NB-IoT and WB-EUTRAN will be considered as two independent access types for all functions.

nb-iot

Use this keyword to enable control plane optimization on the RAT type NB-IoT.

wb-eutran

Use this keyword to enable control plane optimization on the RAT type WB-EUTRAN.

eps-attach-wo-pdn

Use this keyword to enable EPS attach without PDN support for an UE.

Usage Guidelines

Use this command to configure the control plane optimization on the RAT type and to configure EPS attach without PDN support for UE. This command is not enabled by default. The call-control-profile can be associated with the operator-policy or with IME-TAC group, therefore it is possible to either enable or disable CIoT optimization on a per subscriber (IMSI) basis or on a group of subscribers or on per group of IMEI basis. CIoT optimization can be enabled on both NB-IoT and WB-EUTRAN RATs or on either of them. Enabling one RAT type does not disable the other RAT type.

Example

Use the following command to configure control plane optimization by specifying the access type as NB-IoT:

```
ciot-optimisation cp-optimisation access-type nb-iot
```

Use the following command to configure EPS attach without PDN support for UE, specify the access type as WB-EUTRAN:

```
ciot-optimisation eps-attach-wo-pdn access-type wb-eutran
```

ciphering-algorithm-gprs

Defines the order of preference of the ciphering algorithms.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-call-control-profile-`*`profile_name`*`)#`

Syntax Description

ciphering-algorithm-gprs priority *priority algorithm*
remove ciphering-algorithm-gprs priority *priority*

remove

Delete the priority definition.

priority *priority*

Sets the order in which the algorithm will be selected for use.

priority is an integer from 1 to 4.

algorithm

Identifies the ciphering algorithm to be used.

algorithm is one of the following: gea0, gea1, gea2, gea3.

Usage Guidelines

Define the order in which the ciphering algorithms are chosen for use. The command can be repeated to provide multiple definitions -- multiple priorities.

Example

Define gea1 as the third priority algorithm:

```
ciphering-algorithm-gprs priority 3 gea1
```

csfb

Configures circuit-switched fallback options. CSFB is the mechanism to move a subscriber from LTE to a legacy technology to obtain circuit switched voice or short message.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

csfb { policy { ho-restriction | not-allowed | not-preferred | sms-only | suppress-call-reject } | sms-only }
remove csfb { policy | sms-only }

remove csfb { policy | sms-only }

sms-only: Removes the SMS-only restriction allowing the UE to request voice and short message service (SMS) support for circuit-switched fallback (CSFB).

policy: Removes the configured policy.

policy { ho-restriction | not-allowed | not-preferred | sms-only | suppress-call-reject }

ho-restriction: This keyword enables ho-restriction support for CSFB MO Emergency Calls. If this keyword is enabled the MME sets the "Additional CS Fallback Indicator IE" in S1AP UE Context Setup/Modification as "restriction".

not-allowed: Specifies that the CSFB function is not allowed for both voice and SMS.

not-preferred: Specifies that the MME returns a "not-preferred" response for CSFB services. The MME does not enforce this and a voice centric is allowed to make CSFB calls on a not-preferred case if it chooses to do so.

sms-only: Specifies that the CSFB function only supports SMS.

suppress-call-reject: Configures the MME to ignore a paging request for an SMS-only CS call for an attached UE and suppress the paging reject. This allows the MME to process SGs CS call SMS-only paging requests for Ultra Card users where the same MSISDN is allocated to different IMSIs. By default the MME will reject the paging request with a cause: SGSAP_SGS_CAUSE_MOBILE_TERMINATING_CSFB_REJECTED_BY_USER

sms-only

Specifies that the circuit-switched fallback function only supports SMS.

Important This is a legacy keyword that remains to support earlier versions of the code. It operates identically to the **policy sms-only** keyword.

Usage Guidelines Use this command to restrict the circuit-switched fallback function to SMS only or no support for either voice or SMS.

Example

The following command enforces the SMS-only functionality for UEs requesting circuit-switched fallback:

```
csfb policy sms-only
```

dcnr

Enables Dual Connectivity with New Radio (DCNR) to support 5G Non Standalone (NSA).

Product MME, SGSN

Privilege Administrator

Command Modes Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

`[ no | remove ] dcnr`

no

Disables the DCNR configuration.

remove

Removes the configured values for DCNR.

Usage Guidelines

Use this command to enable DCNR for 5G NSA support.

decor

This command allows you to locally configure the UE Usage Type for UEs that complies with the Call Control Profile match criteria.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

`decor { s6a ue-usage-type [ suppress ] | send-ue-usage-type-in-csr | ue-usage-type` *`usage_type_value`* **`}`**
`remove decor { s6a ue-usage-type | send-ue-usage-type-in-csr | ue-usage-type }`

remove

Removes the specified DECOR configuration from the Call Control Profile.

decor

Specifies the Dedicated Core Network configuration.

s6a ue-usage-type [suppress]

Configures the S6a interface for DECOR configuration.

ue-usage-type: Specifies the UE usage type that needs to be sent in the Authentication-Information-Request message over the S6a interface.

suppress: Suppresses sending the UE usage type in S6a Authentication-Information-Request message.

send-ue-usage-type-in-csr

Enables the sending of ue-usage-type in create-session-request to SPGW.

ue-usage-type *usage_type_value*

Configures the UE Usage Type locally. *usage_type_value* must be an integer from 0 to 255.

Usage Guidelines

Use this command to locally configure the UE Usage Type for UEs that complies with the Call Control Profile match criteria.

Example

The following command configures the UE usage type with value set to *100*:

```
decor ue-usage-type 100
```

description

Allows you to enter a relevant descriptive string.

Product

MME

SAEGW

S-GW

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
description description
no description
```

description

Enter an alphanumeric string of 1 to 100 characters. The string may include spaces, punctuation, and case-sensitive letters if the string is enclosed in double quotation marks (").

no

Removes the description from the call control profile.

Usage Guidelines

Define information that identifies this particularly call control profile.

Example

```
description "call-control-profile handling incoming from CallTell"
```

diameter-result-code-mapping

Maps an EMM (EPS Mobility Management) NAS (Network Access Server) cause code to a Diameter result code.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

diameter-result-code-mapping s6a *diameter_result_code* **mme-emm-cause** *mme_emm_error_code*
remove diameter-result-code-mapping s6a *diameter_result_code*

remove diameter-result-code-mapping s6a *diameter_result_code*

Removes the mapping for the specified Diameter result code.

s6a *diameter_result_code*

Specifies the Diameter result code to which the EMM NAS cause code is mapped.

diameter_result_code: Specify one of the supported Diameter result codes:

- **diameter-authorization-rejected** - s6a result code 5003. Default mapped EMM code: "No suitable cells in tracking area."
- **diameter-error-other** - miscellaneous s6a error result code. Default mapped EMM code: "Network failure."
- **diameter-error-rat-not-allowed** - s6a result code 5421. Default mapped EMM code: "No suitable cells in tracking area."
- **diameter-error-roaming-not-allowed** - s6a result code 5004. Default mapped EMM code: "PLMN not allowed."
- **diameter-error-user-unknown** - s6a result code 5001/5030. Default mapped EMM code: "EPS Service and non-EPS services not allowed."
- **diameter-invalid-avp-value** - s6a result code 5004. Default mapped EMM code: "Network failure."
- **diameter-unable-to-comply** - s6a result code 5012. Default mapped EMM code: "Network failure."
- **diameter-unknown-eps-subscription** - s6a result code 5420. Default mapped EMM code: "No suitable cells in tracking area."
- **diameter-unsupported-feature** - s6a result code 5011. Default mapped EMM code: "Network failure."

mme-emm-cause *mme_emm_error_code*

Specifies the EMM NAS cause code to be mapped to the Diameter result code.

mme_emm_error_code: Specify one of the supported EMM NAS error codes:

- **eps-non-eps-not-allowed**: Specifies that the EMM NAS cause code #8 "EPS services and non-EPS services not allowed" is to be mapped to the specified Diameter result code.
- **network-failure**: Specifies that the EMM NAS cause code #17 "Network failure" is to be mapped to the specified Diameter result code.
- **no-suitable-cell-in-tracking-area**: Specifies that the EMM NAS cause code #15 "No suitable cells in tracking area" is to be mapped to the specified Diameter result code.
- **plmn-not-allowed**: Specifies that the EMM NAS cause code #11 "PLMN not allowed" is to be mapped to the specified Diameter result code.
- **roaming-not-allowed-in-this-tracking-area**: Specifies that the EMM NAS cause code #13 "Roaming not allowed in this tracking area" is to be mapped to the specified Diameter result code.
- **severe-network-failure**: Specifies that the EMM NAS cause code #42 "Severe network failure" is to be mapped to the specified Diameter result code.
- **tracking-area-not-allowed**: Specifies that the EMM NAS cause code #12 "Tracking area not allowed" is to be mapped to the specified Diameter result code.

Usage Guidelines

Use this command to map a selected EMM NAS cause code to a specific Diameter result code.

Example

The following command maps the EMM NAS cause code "Roaming not allowed in this tracking area" to the Diameter result code "S6a Diameter error RAT not allowed":

```
diameter-result-code-mapping s6a diameter-error-rat-not-allowed
mme-emm-cause roaming-not-allowed-in-this-tracking-area
```

direct-tunnel

Enables setup of a direct tunnel if direct tunneling is supported by the destination node.

Important Direct tunneling must be enabled at both of these two points to allow direct tunneling for the MS/UE.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

direct-tunnel attempt-when-permitted [to-ggsn | to-sgw]

remove direct-tunnel [to-ggsn | to-sgw]

remove

Removes the configured setting from the call control profile. An existing configuration to enable direct tunneling must be removed before creating a new direct tunnel enabling configuration.

attempt-when-permitted

Enables direct tunneling if the destination node allows it. Default: disabled.

[to-ggsn | to-sgw]

Beginning with Release 19.3.5, including one of these keyword filters allows the operator to select the interface for the direct tunnel.

- **to-ggsn** enables only the GTP-U interface between the RNC and the GGSN for the direct tunnel.
- **to-sgw** enables only the S4's S12 interface between the RNC and the SGW for the direct tunnel.

Usage Guidelines

By default, the direct tunnel feature is not enabled. Use this command to enable the direct tunnel feature.

To ensure that direct tunnel is fully configured for support by the SGSN, check the settings for **direct-tunnel** in

- the APN profile -- from the Exec mode, use command: **show apn-profile** <*profile_name*> **all**
- the RNC (radio network controller) configuration -- from the Exec mode, use command: **iups-service** <*service_name*> **all**

There are three optional configurations:

1. **attempt-when-permitted** enables both the GTP-U interface towards the GGSN and the S12 interface towards the SGW.
2. **attempt-when-permitted to-ggsn** enables only the GTP-U interface towards the GGSN.
3. **attempt-when-permitted to-sgw** enables only the S12 interface towards the SGW.

Important All three forms of the CLI function independently. This means that the configuration created with one command (for example: **direct-tunnel attempt-when-permitted to-ggsn** is not overwritten by the entry of one of the other commands (for example: **direct-tunnel attempt-when-permitted**). The existing configuration must be removed to disable the configuration and then the next configuration must be added.

Example

The following command sets the configuration to instruct the SGSN to attempt to setup a direct tunnel if permitted at the destination node:

direct-tunnel attempt-when-permitted

The following command allows the operator to select the direct tunnel interface and sets the configuration to instruct the S4-SGSN to attempt to setup a direct tunnel using an S12 interface to the destination SGW if the SGW permits direct tunnels:

direct-tunnel attempt-when-permitted to-sgw

dns-ggsn

Defines the context to be used to do DNS lookup for GGSNs.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

dns-ggsn context *ctxt_name*
no dns-ggsn context *ctxt_name*

no

Removes the dns-ggsn configuration from this call control profile.

context *ctxt_name*

Specifies the context to be used to do DNS lookup for GGSNs as an alphanumeric string of 1 through 64 characters.

Usage Guidelines

Use this command to define the context to be used to do DNS lookup to find the GGSN address.

Example

dns-ggsn context sgsn1

dns-mrme

This command is used to configure the DNS client context and DNS query type used for the PGW/GGSN resolution for MRME.

Product

SaMOG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

```
dns-mrme { context context_name [ query-type { a-aaa | snaptr } ] | query-type
 { a-aaa | snaptr } }
no dns-mrme context
default dns-mrme query-type
```

no

Removes the dns-mrme configuration from this call control profile.

default

Sets the default value for the query-type and context will not be modified.

Default (SaMOG 3G license): a-aaa

Default (SaMOG Mixed Mode license): snaptr

Important The **default dns-mrme query-type** command is available only when the SaMOG Mixed Mode license (supporting both 3G and 4G) is configured.

context_name

Specifies the DNS client context to be used for DNS lookup. *context_name* must be an alphanumeric string of 1 through 79 characters.

query-type { a-aaa | snaptr }

Specifies the the type of DNS query used for the PGW/GGSN resolution for MRME.

a-aaa: Specifies to use A-AAA queries using pre-release 8 DNS procedures.

snaptr: Specifies to use SNAPTR queries using post-release 7 DNS procedures. This is the default value when SaMOG Mixed Mode license is configured.

Important This keyword is available only when the SaMOG Mixed Mode license (supporting both 3G and 4G) is configured. However, when an SaMOG 3G license is configured, the query type for the DNS query is set to use A-AAA queries using pre-release 8 DNS procedures.

Usage Guidelines

Use this command to configure the DNS client context and DNS query type used for the PGW/GGSN resolution for MRME. The DNS context configuration is used to provide the context name where the DNS client for this AAA server is configured. The default dns-context is configured under the MRME Service Configuration Mode. If no DNS context is configured under the MRME Service Configuration Mode, the DNS context will be used as the context for the MRME service.

Example

```
dns-mrme context mrme1 query-type snaptr
```

dns-msc

Defines the context to be used to do DNS lookup for Mobile Switching Centers (MSCs).

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

dns-msc context *ctxt_name*
remove dns-msc

remove

Deletes this definition from the call control profile.

context *ctxt_name*

Specifies the context to be used to do DNS lookup for MSCs as an alphanumeric string of 1 through 64 characters.

This specifies the name of the context where the DNS client is configured that will be used for DNS resolution of MSCs for Single Radio Voice Call Continuity (SRVCC).

Usage Guidelines

This feature requires that a valid SRVCC license key be installed.

Use this command to configure the context ID for the DNS lookup.

MSC selection using DNS takes precedence over locally configured MSCs. If DNS lookup fails, the MME will select the MSC from local configuration.

DNS based MSC selection can be defined for an MME service, or for a Call Control Profile. Both configuration options specify the context in which a DNS client configuration has been defined. Configuration via Call Control Profile takes precedence in cases where DNS selection is also configured in the MME service

Example

The following command associates a pre-configured context *dns_ctx1* where a DNS client service is configured for DNS query to MSC for this Call Control Profile.

```
dns-msc context dns_ctx1
```

dns-sgsn

Identifies the context to be used to do DNS to find an SGSN address.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

`[ no ] dns-sgsn context` *`ctxt_name`*

no

Removes the dns-sgsn configuration from this call control profile.

context *ctxt_name*

Identify the context where the DNS client is configured to send the DNS query to get the peer SGSN address.

context_name: Enter a string of 1 to 79 alphanumeric characters to identify the context.

This configuration would override any similar configuration for **dns-sgsn context** in the SGTP service configuration.

Usage Guidelines

Use this command to configure the context ID for the SGSN address that will be used to do the DNS lookup.

Example

Configure context *sgsn1* for DNS lookup:

```
dns-sgsn context sgsn1
```

dns-pgw

Defines the context to be used to do DNS lookup for P-GWs.

Product

MME

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

[remove] dns-pgw context *ctxt_name*

remove

Deletes this definition from the call control profile.

context *ctxt_name*

Specifies the context to be used to do DNS lookup for P-GWs as an alphanumeric string of 1 through 64 characters.

On the S4-SGSN, if the interface selected for a UE is S4 and if there is no DNS-PGW context configured under a call control profile, then by default the system will look for the DNS client in the context where the eGTP service is defined. If the interface selected for a UE is Gn-Gp and if there is no **dns-pgw context** configured in a call control profile, then by default the S4-SGSN will look for the DNS client in the context where the SGTP service is configured for selecting a co-located PGW/GGSN if:

- the UE is EPC capable and,
- **apn-resolve-dns-query snaptr** is configured in an APN profile using *APN Profile Configuration Mode*.

If the **dns-pgw context** is deleted with the **remove** option, the S4-SGSN chooses the DNS client from the context where the eGTP service is configured.

Usage Guidelines

Use this command to configure the context ID for the DNS lookup.

Important It is recommended to execute the S4 SGSN configuration commands during the maintenance window. After configuring the node, re-start the node to activate the configuration commands. This will ensure that the node is in a consistent state and S4 SGSN service instability scenarios are avoided.

Example

```
dns-pgw context pgw1
```

dns-sgw

Defines the context to be used to do DNS lookup for S-GWs.

Product

MME

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
[ remove ] dns-sgw context ctxt_name
```

remove

Deletes this definition from the call control profile.

context *ctxt_name*

Specifies the context to be used to do DNS lookup for S-GWs as an alphanumeric string of 1 through 64 characters.

This command must be used to configure DNS client settings when using dynamic S-GW selection where the tai-mgmt-db has been associated with a call-control-profile.

On the S4-SGSN, this specifies the name of the context where the DNS client is configured that will be used for DNS resolution of S-GWs. If **dns-sgw context** is not specified, the S4-SGSN uses the DNS client configured in the context where the eGTP service is configured to query the S-GW DNS address.

Usage Guidelines

Use this command to configure the context ID for the DNS lookup.

Important It is recommended to execute the S4 SGSN configuration commands during the maintenance window. After configuring the node, re-start the node to activate the configuration commands. This will ensure that the node is in a consistent state and S4 SGSN service instability scenarios are avoided.

Example

```
dns-sgw context sgw1
```

ecn

This command enables explicit congestion notification (ECN) in normal mode or compatible mode for the GTP tunnel over S2b interface.

Product

ePDG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
ecn gtp mode normal
remove ecn gtp mode
```

ecn

Specifies ECN over GTP tunnel in normal mode.

gtp

Enables ECN handling over GTP tunnel.

mode

Specifies the tunnel ingress encapsulation mode.

normal

Specifies the normal mode of encapsulation.

remove

Enables ECN in compatible mode for GTP tunnel over the S2b interface. The default mode is the compatible mode, supported for backward compatibility.

Usage Guidelines

Use this command to enable ECN in normal mode or compatible mode for the GTP tunnel over S2b interface.

Example

The following command enables ECN in normal mode for the GTP tunnel:

```
ecn gtp mode normal
```

edrx

This command enables Extended Discontinuous Reception (eDRX) and configures its respective parameters, on the MME.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax

```
edrx { ptw ptw_value edrx-cycle cycle_length_value | ue-requested } [
dl-buf-duration [ packet-count packet_count_value ] ]
remove edrx
```

remove

The keyword **remove**disables the eDRX configuration on the MME.

ptw *ptw_value*

This keyword is used to configure the PTW value.

In releases prior to 21.2: The *ptw_value* is an integer ranging from "0" up to "20".

In 21.2 and later releases: The *ptw_value* is an integer ranging from "0" up to "15".

ue-requested

The keyword **ue-requested**specifies the UE requested values of the Paging Time Window (PTW) and the eDRX cycle length received from the UE in the Attach Request/TAU Request message be accepted.

edrx-cycle *cycle_length_value*

The keyword **edrx-cycle**is used to configure the eDRX cycle length. The *cycle_length_value* is an integer value from " 512" up to "262144". It is a multiple of 2 starting from 512 up to 262144 (for example: 512, 1024, 2048, and so on).

dl-buf-duration

The keyword **dl-buf-duration** is used to send downlink buffer duration in DDN ACK when unable to page UE.

packet-count*packet_count_value*

The keyword **packet-count** is used to send 'DL Buffering Suggested Packet Count' in DDN ACK when unable to page UE. The *packet_count_value* is an integer value from "0" up to "65535". If the *packet_count_value* is not configured locally, the subscription provided value for the *packet_count_value* is used. The subscription value can be "0" in which case packet count IE will not be sent for that subscriber even if it is configured locally.

Usage Guidelines

Use this command to enable eDRX on the MME. This command is configured as part of the eDRX feature for MME - it allows UEs to connect to the network on a need basis. With eDRX, a device can remain inactive or in sleep mode for minutes, hours or even days based on the H-SFN synchronization time (UTC Time). The H-SFN synchronization time for eDRX is configured at an MME-Service level. See *MME Service Configuration Mode Commands* chapter for configuration information on H-SFN synchronization. This command is not enabled by default.

Example

The following command is used to configure the PTW and eDRX cycle length. The command is also used to send the downlink buffer duration in the DDN ACK along with a suggested packet count:

```
edrx ptw 10 edrx-cycle 512 dl-buf-duration packet-count 10
```

egtp

Configures the type of PLMN sent in either the user location information (ULI) IE or the Serving Network IE.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

```
egtp network-sharing-plmn { serving-network { use-common-plmn |
use-selected-plmn | use-ue-plmn } | uli { use-common-plmn |
use-selected-plmn | use-ue-plmn } }
remove egtp network-sharing-plmn { serving-network | uli }
```

remove

Erases the IE choice from the call control profile configuration.

use-common-plmn

Instructs the SGSN to identify the Common PLMN for the shared network.

use-selected-plmn

Instructs the SGSN to identify the Selected PLMN for the shared network.

use-ue-plmn

Instructs the SGSN to identify the UE selected PLMN that is available in the shared network.

Usage Guidelines

The SGSN supports location change reporting on the S4 interface, when requested by the P-GW, using a ULI IE in GTPv2 messages. When the network sharing feature is enabled the operator can determine which PLMN to send to the P-GWin the ULI IE and Serving Network IE. The command can be issued multiple times to configure the PLMN type for each IE.

The selections made for this configuration must match those configured for the call control profile's GTP configuration.

This command can only be used if network sharing is enabled and the appropriate "Location-reporting in connected-mode" feature license is installed. For details, check with your Cisco Representative.

Example

Configure the ue-plmn type PLMN to be sent in the Serving Network IE:

```
egtp network-sharing-plmn serving-network ue-plmn
```

eir-profile

Identifies and associates an EIR profile to be used by the SGSN for EIR selection.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

`[ no ] eir-profile` *`profile_name`*

no

Disassociates the EIR profile with the call control profile.

Usage Guidelines

The equipment identify register (EIR) profile contains all the parameters needed to identify and work with an EIR to perform check IMEI procedures and to address multiple EIR through a single EIR address. The configuration in the EIR profile associated with the call control profile take precedence over the EIR parameters configured in the MAP service.

Example

Associate the EIR profile called *LondonEIR1*:

```
eir-profile LondonEIR1
```

encryption-algorithm-lte

Defines the priorities for using the encryption algorithms.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

```
encryption-algorithm-lte priority1 { 128-eea0 | 128-eea1 | 128-eea2 |
128-eea3 } [ priority2 { 128-eea0 | 128-eea1 | 128-eea2 | 128-eea3 } ] [
 priority3 { 128-eea0 | 128-eea1 | 128-eea2 | 128-eea3 } ] [ priority4 {
```

```
 128-eea0 | 128-eea1 | 128-eea2 | 128-eea3 } ]
remove encryption-algorithm-lte
```

remove

Deletes the priorities definition from the call control profile configuration.

priority1

Specifies the preference of integrity algorithm for security procedures on this call control profile as priority 1.

priority2

Specifies the preference of integrity algorithm for security procedures on this call control profile as priority 2.

priority3

Specifies the preference of integrity algorithm for security procedures on this call control profile as priority 3.

priority4

Specifies the preference of integrity algorithm for security procedures on this call control profile as priority 4.

128-eea0

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

Default: priority1

128-eea1

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

128-eea3

Sets the ZUC algorithm (128-EEA3) for LTE encryption as the encryption algorithm for security procedures.

Default: priority4

Usage Guidelines Set the order or priority in which the MME will select an encryption algorithm for use. All three priorities must be set or the definition is invalid. The command can be re-entered to change the priorities without removing the configuration.

Example

The following command sets the 128-EEA2 as the LTE encryption algorithm with priority 3 for security procedures with the call control profile:

```
encryption-algorithm-lte priority1 128-eea2 priority3
```

encryption-algorithm-umts

Defines the priorities for using the encryption algorithms.

Product SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
encryption-algorithm-umts { uea0 | uea1 | uea2 } [ then-uea# | then-uea# ]
no encryption-algorithm-lte
```

no

Deletes the priorities definition from the call control profile configuration.

{ *uea0* | *uea1* | *uea2* }

Enter one of the three options to define the first priority algorithm.

[then-uea# | then-uea#]

If a second algorithm is to be included as an option, give it second priority. Enter 0, 1, or 2 at the end of **then-uea** to define the algorithm being given second priority.

then-uea#

If a third algorithm is to be included as an option, give it third priority. Enter 0, 1, or 2 at the end of **then-uea** to define the algorithm being given third priority.

Usage Guidelines Set the order or priority in which the SGSN will select a UEA algorithm for use. It is not necessary to define priorities for all three priority levels. The command can be re-entered to change the priorities without removing the configuration.

Example

Configure algorithm UEA2 as the first priority encryption algorithm with no others to be considered:

```
encryption-algorithm-umts uea2
```

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.

epdg-s2b-gtpv2

Configures S2b GTPv2 IE Options.

Product ePDG

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
[ remove ] epdg-s2b-gtpv2 send  { aaa-server-id | message { mbr trigger
mobike } | serving-network { value uli }  | ue-local-ip-port | uli   |
wlan-location-info-timestamp }
```

remove

Using the "remove" keyword will remove the configuration and restore the default behavior. By default the inclusion of the AVPs in the Create Session Request Message will be disabled.

send

Configure the IE or message options in send direction.

aaa-server-id

This is used to send AAA origin-host and origin-realm in Node Identifier IE.

message

This is used to configure the message options to be sent.

serving-network

This is used to send serving-network IE.

ue-local-ip-port

This is used to send UE Local IP IE and UE UDP Port IE.

uli

This is used to send uli IE.

wlan-location-info-timestamp

This is used to send UE Wlan Location Information and Timestamp IE.

Usage Guidelines

Use this command to Enable/Disable the inclusion of the "UE Local IP Address" and "UE UDP Port" AVPs in the GTPv2 Create Session Request message from ePDG to PGW.

Example

Use the following command to include "UE Local IP Address" and UE UDP Port" AVPs in the GTPv2 Create Session Request message from ePDG to PGW.

```
epdg-s2b-gtpv2 send ue-local-ip-port
```

equivalent-plmn

Configures the definition for an equivalent public land mobile network identifier (PLMN ID) and the preferred radio access technology (RAT). This is a of PLMNs which should be considered by the mobile as equivalent to the visited PLMN for cell reselection and network selection. When configured, the equivalent PLMN list will be sent to the UE in NAS ATTACH ACCEPT / TAU ACCEPT messages (up to 15 PLMNs in each message).

Product

MME

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

equivalent-plmn radio-access-technology { 2G | 3g | 4g | any } plmnid mcc *mcc_number* **mnc** *mnc_number* **priority** *priority*
no equivalent-plmn radio-access-technology { 2G | 3g | any } plmnid mcc*mcc_number* **mnc** *mnc_number*

no

Removes the equivalent-PLMN configuration from this call control profile.

radio-access-technology { 2G | 3g | 4g | any }

Identify the RAT type of the equivalent PLMN:

- **2G**: 2nd generation
- **3G**: 3rd generation
- **4G**: 4th generation
- **any**: Any RAT

plmnid mcc *mcc_number* mnc *mnc_number*

- **mcc**: Specifies the mobile country code (MCC) portion of the PLMN ID. The number can be any integer between 100 and 999.
- **mnc**: Specifies the mobile network code (MNC) portion of the PLMN ID. The number can be any 2- or 3-digit integer between 00 and 999.

priority *priority*

Enter an integer between 1 and 15 with the highest priority assigned to the integer of the lowest numeric value.

Usage Guidelines

Use the command to identify an 'equivalent PLMN' and assign it a priority to define the preferred equivalent PLMN to be used. This command can be entered multiple times to set priorities of usage.

Example

The following command sets up a secondary equivalent PLMN definition that allows for any RAT with a PLMN ID of MCC121.MNC767:

```
equivalent-plmn radio_access_technology any plmnid mcc 121 mnc 767 priority
 2
```

esm t3396-timeout

This command is used to configure the ESM T3396 timer to be sent to UE in ESM reject messages.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

esm t3396-timeout *timeout_value* **cause** *cause_code_value*
remove esm t3396-timeout cause *cause_code_value*

remove

Removes the T3396 timeout configuration for the specified cause code from Call Control profile. The T3396 timeout will then be applied from the MME-service.

t3396-timeout *timeout_value*

Configures the value for ESM backoff timer (in seconds) to be sent to UE for ESM reject cause 'insufficient resources' and 'missing or unknown apn'. This value overrides the MME-service level configuration.

The *timeout_value* is an integer from 0 to 1116000.

cause *cause_code_value*

Configures the cause code value as an integer that is either 26 or 27. If the configured value is present in the ESM reject messages, the T3396 back-off timer will be included.

- The following cause values are supported:
  - 26 - Insufficient resources
  - 27 - Missing or Unknown APN
- Only one cause value can be configured with the **cause** keyword. Multiple cause values cannot be configured.

Usage Guidelines

This command configures the ESM T3396 timer to be sent to UE in ESM reject messages. There is no specified default value for T3396 timeout for a given cause code.

- To configure the T3396 timeout for different cause codes, the configuration must be done in multiple lines. For example:

  ```
  esm t3396-timeout 1100 cause 26
  esm t3396-timeout 1500 cause 27
  ```

- The new configuration for T3396 timeout for a given cause code will override the previous configuration. For example:

  ```
  esm t3396-timeout 1500 cause 26
  esm t3396-timeout 1800 cause 26
  ```

  The final T3396 timeout that will be applied for cause code 26 is 1800 seconds.

Example

The following command sets the ESM T3396 timeout value as *1860* seconds for cause code value *26*:

```
esm t3396-timeout 1860 cause 26
```

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.

gbr-bearer-preservation-timer

Configures the system to preserve GBR bearers for a configurable timer value.

Product MME

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description **gbr-bearer-preservation-timer** *timer_value*
remove gbr-bearer-preservation-timer

remove

Disables the timer configuration.

gbr-bearer-preservation-timer

The above command allows the operator to set the preservation time for the Bearer on receiving the UE Context Release with the Radio Connection With UE Lost cause code.

timer_value

Specifies the duration for preserving the bearers in seconds. *timer_value* must be an integer from 1 to 600.

Usage Guidelines MME provides a configurable timer. Operators can configure a timer value for which the GBR bearers are preserved when the subscriber is out of coverage during a VoLTE call.

Example

The following command preserves the GBR bearers for 300 seconds.

```
gbr-bearer-preservation-timer 300
```

gmm Extended-T3312-timeout

This command enables the operator to determine how the SGSN handles Extended T3312 timer values at the Call-Control Profile level.

Product SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
gmm Extended-T3312-timeout  { value exT3312_minutes | when-subscribed } [
low-priority-ind-ue ]
no gmm Extended-T3312-timeout
```

no

This command filter instructs the SGSN to remove the Extended T3312 configuration from the Call-Control Profile configuration.

value

This keyword instructs the SGSN to send the defined Extended T3312 timer value in Attach or RAU Accept messages to the MS if the subscriber has a subscription for the Extended T3312 timer (Subscribed Periodic RAU/TAU Timer in ISD) and indicates support for the extended periodic timer via the MS Network Feature Support.

exT3312_minutes : Enter an integer from 0 to 18600 to identify the number of minutes for the timeout; default is 186 minutes.

when-subcribed

This keyword instructs the SGSN to only send the Extended T3312 period RAU timer value in Attach or RAU Accept messages if the SGSN receives the timeout value in an ISD (insert subscriber data) when the MS has indicated support in "MS Network Feature Support".

low-priority-ind-ue

This keyword instructs the SGSN to include the extended T3312 timer value only if the Attach/RAU Request messages include a LAPI (low access priority indicator) in the "MS Device Properties".

Usage Guidelines

An **Extended-T3312-timeout** configuration in the Call-Control Profile will override an **Extended-T3312-timeout** configuration done for either the GPRS or SGSN services. As well, a Call-Control Profile configuration enables the operator to finetune for Homers and Roamers.

Example

Use a command similar to the following to instruct the SGSN to only send the Extended T3312 value when the Attach/RAU Request includes a LAPI and when the received "MS Network Feature Support" information indicates the the user is subscribed for this timer:

```
gmm Extended-T3312-timeout when-subscribed low-priority-ind-ue
```

Use the following command to remove the Extended T3312 timer configuration from the Call-Control Profile.

```
no gmm Extended-T3312-timeout
```

gmm information-in-messages

Provides the configuration to include the information in messages for the GPRS mobility management (GMM) parameters.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
gmm information-in-messages access-type { { gprs | umts } [ network-name
 { full-text name | short-text name } | [ send-after { attach | rau } ] }
[ default | no ] gmm { information-in-messages access-type { gprs | umts
 }
```

no

Disables the GMM configuration from this call control profile.

default

Sets up a GMM configuration with system default values.

access-type

Must select one of the following options:

- **gprs** - General Packet Radio Service network
- **umts** - Universal Mobile Telecommunications System network

After selecting the access-type, an additional parameter can be configured:

- **network-name**: identifies the network name in either short text or full text.
- **send-after**: configures the information in message to send after attachment or Routing Area Update (RAU).

network-name { full-text *name* | short-text *name* }

This keyword provides the option to add the network name to the message. The network name will in full text or short text. Possible options are:

- full-text *name*: Indicate the network name in full text
- short-text *name*: Indicate the network name in short text

send-after { attach | rau }

This keyword configures the information in message to send after attachment or RAU message. Possible options are:

- **attach**: Information sent after attachment
- **rau**: Information sent after routing area update

Usage Guidelines Use this command to configure identifying information about the network that will be included in GMM messages.

Example

Set default settings for calls coming from 2.5G networks:

```
default gmm information-in-messages access-type gprs
```

gmm rau-accept

Provides the configuration to set the Follow-On Proceed (FOP) bit in the Routing Area Update Accept (RAU) message.

Product SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

```
gmm rau-accept follow-on-proceed { on-following-nw-procedure |
only-on-ue-request }
remove gmm rau-accept follow-on-proceed
```

remove

Disables the SGSN from sending the Follow On Proceed bit in the RAU response.

follow-on-proceed

This keyword configures the SGSN to send FOP bit in RAU Accept message.

on-following-nw-procedure

This keyword configures the SGSN to send FOP bit when there is a following Network Procedure.

only-on-ue-request

This keyword configures the SGSN to send FOP bit only when UE requests for it.

Usage Guidelines

Use this command to configure the setting of Follow On Proceed bit in Routing Area Accept Message. The FOP bit can be set only when the UE requests for it by configuring the command option **only-on-ue-request** or the FOP bit can be set when there is a following network procedure by configuring the CLI option **on-following-nw-procedure**. By default, the configuration is **gmm rau-accept follow-on-proceed only-on-ue-request**.

Example

Use this command to configure the SGSN to send the Follow On Proceed bit when there is a following Network Initiated Procedure.

```
gmm rau-accept follow-on-proceed on-following-nw-procedure
```

gmm retrieve-equipment-identity

Configures the International Mobile Equipment Identity (IMEI) or software version (SV) retrieval and validation procedure.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

gmm retrieve-equipment-identity { imei | imeisv [unciphered] [then-imei] } [verify-equipment-identity [deny-greylisted] [allow-unknown]] [no | default] gmm retrieve-equipment-identity

no

Disables the equipment identity retrieval procedure configured for this call control profile.

default

Sets the default action for equipment identity retrieval (EIR) procedure:

- **retrieve-equipment-identity**: Default action is disabled - no retrieval of IMEI/IMEI-SV
- **verify-equipment-identity**: Default action is disabled - no verification with Equipment Identity Register (EIR)

equipment-identity-type

Default: disabled

Indicates the type of equipment identification, with the possible values:

- **imei**: International Mobile Equipment Identity
- **imeisv**: International Mobile Equipment Identity - Software Version

imei

Indicates the equipment identity retrieval type to International Mobile Equipment Identity (IMEI). IMEI is a unique 15-digit number consisting of a TAC (Technical Approval Code), a FAC (Final Assembly Code), an SNR (Serial Number), and a check digit.

imeisv [unciphered] [then-imei]

Indicates the equipment identity retrieval type to IMEI with software version (SV). IMEI with SV is a unique 16-digit number consisting of a TAC (Technical Approval Code), a FAC (Final Assembly Code), an SNR (Serial Number), and a 2-digit software version number.

- **unciphered**: This optional keyword enables the unciphered retrieval of IMEI-SV. If this option is enabled the retrieval procedure will get IMEISV (if auth is still pending, get as part of Authentication and Ciphering Response otherwise, via explicit Identification Request after Security Mode Complete).
- **then-imei**: This optional keyword enables the retrieval of software version number before the IMEI. If this option is enabled the equipment identity retrieval procedure will get IMEISV on secured link (after Security mode procedure via explicit GMM Identification Request), and if MS is not having IMEISV (responded with NO Identity), SGSN will try to get IMEI.

If no other keyword is provided, imeisv will get IMEISV on a secured link (after a Security mode procedure via explicit GMM Identification Request).

verify-equipment-identity [deny-greylisted] [allow-unknown]

Default: disabled

This keyword enables the equipment identity validation and validates the equipment identity against the EIR.

- **deny-greylisted**: This keyword fine-tunes the configuration and enables the restriction to the user having mobile equipment with an IMEI in the EIR grey list.
- **allow-unknown**: If this keyword is configured and EIR sends equipment status as "UNKNOWN EQUIPMENT" then the call will be allowed to continue in SGSN.

Usage Guidelines

Use this command to enable and configure the procedures for mobile equipment identity retrieval and validation from the EIR identified in the MAP Service Configuration mode.

Example

The following command enables the SGSN to send "check IMEI" messages to the EIR:

```
gmm retrieve-equipment-identity imei verify-equipment-identity
```

gmm t3346

The **gmm** command includes a new keyword to set the MM T3346 back-off timer for a Call-Control Profile.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
gmm t3346 min minimum_minutes max maximum_minutes
no gmm t3346
```

no

Including this filter with the command removes the MM back-off timer definition from the Call-Control Profile configuration.

min *minimum_minutes*

Enter an integer from 1 to 15 to identify the minimum number of minutes the timer should run; default is 15 minutes.

max *maximum_minutes*

Enter an integer from 1 to 30 to identify the maximum number of minutes the timer should run; default is 30 minutes.

Usage Guidelines

- Under congestion, the SGSN can assign the T3346 back-off timers to the UEs and request the UEs not to access the network for a given (timer value) period of time.
- If an Attach Request or RAU Request or Service Request is rejected due to congestion, then the T3346 value will be included in the reject message with GMM cause code 22 (congestion). The MM back-off timer value sent will be chosen randomly from within the configured T3346 timer value range.
- If T3346 timer value is configured in a Call-Control Profile then it will override the back-off timer values defined for either the SGSN Service or GPRS Service configurations.
- The timer will be ignored if an Attach Request or RAU Request is received after congestion has cleared.

Example

Use a command similar to the following to define a T3346 with a timeout range of *2 to 15* minutes.

```
gmm t3346 min 2 max 15
```

gs-service

Associates the context of a Gs service interface with this call control profile.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

gs-service *gs_srvc_name* **context** *ctx_name*
no gs-service *svc_name*

no

Removes/disassociates the named Gs service from the call control profile.

gs-service *gs_srvc_name*

Specifies the name of a specific Gs service for which to display information. *gs_srvc_name* is the name of a configured Gs service expressed as an alphanumeric string of 1 through 63 characters that is case sensitive.

context *ctx_name*

Specifies the specific context name where Gs service is configured. If this keyword is omitted, the named Gs service must exist in the same context as the GPRS/SGSN service.

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

Usage Guidelines

Use this command to associate a specific Gs service interface with this GPRS service instance.

Important

A Gs service can be used with multiple SGSN and/or GPRS service.

Example

The following command associates a Gs service instance named *stargs1*, which is configured in context named *star_ctx*, with a call control profile:

```
gs-service stargs1 context star_ctx
```

gtp send

Configures which information elements (IE) the SGSN sends in GTP messages. These are required by the GGSN.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
gtp send { imeisv [ derive-imeisv-from-imei ] | ms-timezone | rai [
use-local-plmn [ network-sharing { use-selected-plmn | use-ue-plmn |
use-common-plmn } ] ] | rat | uli [ use-local-plmn [ network-sharing {
use-selected-plmn | use-ue-plmn | use-common-plmn } ] ] }
remove gtp send { imeisv | ms-timezone | rai | rat | uli }
no gtp send
```

remove

Removes the specified GTP send definition from the system configuration.

no

Disables the specified GTP send configuration.

imeisv

Instructs the SGSN to include the IMEISV (International Mobile Equipment Identity with Software Version) of the mobile when sending GTP messages of the type Create PDP Context Request.

By default, this function is disabled.

derive-imeisv-from-imei

This is a filter for the **imeisv** keyword. It allows the operator to configure the SGSN to send IMEI to the GGSN as IMEI-SV.

This filter instructs the SGSN to add four 1s (1111) to the final semi-octet of the CPCQ (Create PDP Context Request) message which enables the SGSN to deduce the IMEI-SV value from the IMEI. If this filter is used, then IMEI is also sent as IMEI-SV when the **gmm retrieve-equipment-identity** command is configured.

ms-timezone

Instructs the SGSN to include this IE in GTP messages of the type Create PDP Request and Update PDP Context Request. This IE specifies the offset between universal time and local time, where the MS currently resides, in 15-minute steps.

This IE is sent by default.

rai

Configures the SGSN to include the Routing Area Identity (RAI) of the SGSN in the following situations:

- 2G new SGSN RAU
- 3G new SGSN SRNS
- 2G -> 3G HO (only if PLMN Id has changed)
- 3G -> 2G HO (only if PLMN Id has changed)
- multiple IUPS service RAU (only if PLMN Id has changed)
- multiple GPRS service RAU (only if PLMN Id has changed)
- 3G new SGSN RAU (change in behavior)
- 3G primary and secondary PDP activation (change in behavior)
- 2G primary and secondary PDP activation (change in behavior)

Optionally, this keyword can be followed with the keyword selection for the PLMN - **use-local-plmn**.

rat

Specifies which radio access technology (RAT) is being used by the MS (GERAN, UTRAN, or GAN). Including this keyword instructs the SGSN to include this IE when sending GTP messages of the type Create PDP Request and Update PDP Context Request.

This IE is sent by default.

uli

Specifies the CGI (MCC, MNC, etc.) and SAI of the MS where it is registered. Including this keyword instructs the SGSN to include the IE when sending GTP messages of the type Create PDP Request and Update PDP Context Request.

This IE is not sent by default.

Optionally, this keyword can be followed with the keyword selection for the PLMN - **use-local-plmn**.

Important Currently, the next 5 (five) keywords, are only used with parameters **rai** or **uli**.

use-local-plmn

This keyword selects the local PLMN when network is not shared.

network-sharing

This keyword is used to configure network-sharing.

use-selected-plmn

This keyword selects the Selected PLMN when network is shared.

use-ue-plmn

This keyword selects Selected PLMN for supporting UE and Common PLMN for non-supporting UE when network is shared.

use-common-plmn

This keyword selects the Common PLMN when network is shared.

Usage Guidelines

Use this command to define a preferred set of information to include when GTP messages are sent. Repeat this command multiple times to enable or disable multiple options. This instruction will be implemented when the specific operator policy and call control profile are applied.

The PLMN value in RAI/ULI can be selected if 3G network-sharing is enabled.

Example

The following command series instructs the SGSN (1) not to send MS' timezone IE, and (2) to identify the MS' radio access technology info in the GTP messages:

```
no gtp send ms-timezone
gtp send rat
```

The next set of commands provides examples indicating the usage of keywords to select PLMN values in RAI/ULI.

On executing the following command, ULI is sent and PLMN will be "use-selected-plmn" if network-sharing is enabled. If network-sharing is not enabled, PLMN will be "use-local-plmn".

```
gtp send uli
```

On executing the following command, ULI is sent and PLMN will be "use-selected-plmn" if network-sharing is enabled. If network-sharing is not enabled, PLMN will be "use-local-plmn".

```
gtp send uli use-local-plmn
```

On executing the following command, ULI is sent and PLMN will be "use-selected-plmn" if network-sharing is enabled. If network-sharing is not enabled PLMN will be "use-local-plmn".

gtp send uli use-local-plmn network-sharing use-selected-plmn

On executing the following command, ULI is sent and PLMN will be "use-common-plmn" if network-sharing is enabled. If network-sharing is not enabled PLMN will be "use-local-plmn".

gtp send uli use-local-plmn network-sharing use-common-plmn

gtpp

Enables secondary GTPP accounting for an S-GW call control profile. By default, secondary GTPP accounting is disabled.

Product

S-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

gtpp secondary-group *group_name* **[accounting context** *ctx_name* **]**
no gtpp secondary-group

no

Disables secondary GTPP accounting.

secondary-group *group_name*

Enables secondary GTPP accounting and specifies a GTPP group name.

group_name must be an alphanumeric string of 1 through 63 characters.

accounting context *ctx_name*

Specifies the specific accounting context to be used for secondary GTPP accounting. If this keyword is omitted, source context will be used for secondary GTPP accounting.

ctx_name must be an alphanumeric string of 1 through 79 characters.

Usage Guidelines

Use this command to enable or disable secondary GTPP accounting for an S-GW call control profile.

Example

The following command enables secondary GTPP accounting for an S-GW call control profile and specifies a GTPP group named *gtpp-grp1*:

gtpp secondary-group gtpp-grp1

gtpu fast-path

Enables or disables the network processing unit (NPU) Fast Path support for NPU processing of GTP-U packets of user sessions at the NPU.

Important This command is deprecated from StarOS release 16.2 onwards as the NPU FastPath feature is not supported from the StarOS 16.2 release.

Product

SAEGW

SGSN

S-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-call-control-profile-`*`profile_name`*`)#`

Syntax Description

`[ remove ] gtpu fast-path`

remove

Removes the NPU fast path functionality configuration from the call control profile.

Usage Guidelines

Use this command to enable/disable the NPU processed fast-path feature for processing of GTP-U data packets received from GGSN/RNC or P-GW/eNodeB. This feature enhances the GTP-U packet processing by adding the ability to fully process and forward the packets through the NPU itself.

Important When enabled/disabled, fast-path processing will be applicable only to new subscriber who establishes a PDP context after issuing this command (enabling GTP-U fast path). No existing subscriber session will be affected by this command.

Example

The following command enables the NPU fast path processing for all new subscribers' session established with this call control profile:

```
gtpu fast-path
```

guti

This command is used to configure the periodicity (time interval) / frequency of GUTI reallocation for a UE.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

`[ remove ] guti reallocation [ frequency` *`frequency`* **`| periodicity`** *`duration`* **`]`**

remove

The **remove** keyword is used to remove the configured GUTI reallocation frequency and periodicity specified in the call control profile configuration.

guti

The keyword **guti** identifies the Globally Unique Temporary UE Identity (GUTI).

reallocation

The keyword **reallocation** specifies reallocation of GUTI.

frequency *frequency*

The frequency configured specifies the GUTI reallocation frequency. The frequency is an integer with a range "1" up to "65535" requests. A configured frequency of "n" requests triggers GUTI Reallocation for every 'nth' ATTACH / TAU / SERVICE REQUEST received from the UE.

periodicity *duration*

The periodicity configured specifies GUTI reallocation periodicity. The periodicity is an integer with a range "1" up to "65535" minutes. A configured periodicity of "t" minutes triggers GUTI Reallocation at every "t" minutes for a UE.

Usage Guidelines

GUTI reallocation is disabled by default. Use this command to configure the periodicity (time interval) / frequency of GUTI reallocation for a UE.

Example

The following command is used to configure the frequency of GUTI reallocation for a UE as "10".

```
guti reallocation frequency 10
```

gw-selection

Configures the parameters controlling the gateway selection process.

Product

MME

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-call-control-profile-`*`profile_name`*`)#`

Syntax Description

`[ remove ] gw-selection { co-location [ weight [ prefer { sgw | pgw } ] ]| gtp-weight | pgw weight | sgw weight | topology [ weight [ prefer { sgw | pgw } ] ] }`

remove gw-selection

Deletes the gw-selection definition from the call control profile.

co-location [weight [prefer { sgw | pgw }]]

Selects "co-location" as the determining factor for gateway selection. Collocation should be configured for both P-GW and S-GW selection for collocation to function. If a collocated PGW/SGW node cannot be found, then topologically closest nodes are chosen next. Host names with both "topon" and "topoff" labels will be considered in collocation.

weight: Enables weighted selection if there are multiple co-located pairs.

prefer { pgw | sgw}: Configures which weight to be used for weighted selection.

gtp-weight

Is the weight value calculated from the Load Control Information received from the GTP peers. The option enables the MME selection of SGW and PGW based on the advertised load control information. This configuration can be applied selectively to subscribers.

pgw weight

Selects PDN-Gateway as the determining factor for gateway selection.

sgw weight

Selects Serving Gateway as the determining factor for gateway selection.

topology [weight [prefer { sgw | pgw }]]

Selects topology as the determining factor for gateway selection. Topological selection is done only during initial attach, and not used during S-GW relocation or additional-pdn-connection.

weight: Enables weighted selection if there are multiple pairs with the same degree of topological closeness.

prefer { pgw | sgw}: Configures which weight to be used for weighted selection.

Usage Guidelines

Use this command to define the criteria for gateway selection.

Selection of a co-located gateway (GW) node or a topologically closer GW node is based on string comparison of canonical node names included in two or more sets of records received in DNS S-NAPTR query result. For comparison, the canonical node names are derived from the hostnames received in the DNS records. The hostnames must adhere to the following format:

```
<topon|topoff>.<single-label-interface-name>.<canonical-node-name>;
```

Where "topon" or "topoff" is a prefix of the hostname and indicates whether or not the canonical node name can be used for topology matching.

The table below lists the behaviors with various CLI options:

Table 1: CLI Behavior Options

Option	Keyword Selected	Prefix in Hostname	Topological Match Nodes Selected	Comments
1	co-location	topon	Yes	Co-located nodes are selected if available as they are listed before topologically closer nodes in the DNS records.
2	co-location	topoff	Yes	Co-located nodes are selected if available as they are listed before topologically closer nodes in the DNS records.
3	topology	topon	Yes	Co-located nodes are selected if available as they are listed before topologically closer nodes in the DNS records.

Option	Keyword Selected	Prefix in Hostname	Topological Match Nodes Selected	Comments
4	topology	topoff	No	Nodes with prefix 'topoff' are ignored for topological matching purposes. If no nodes are present with 'topon' as prefix then nodes are selected independently based on Order/Priority mentioned in DNS Records.
5	co-location	neither	Yes	Will strip only the first label from hostname to fetch canonical node name for topology matching. Co-located nodes are selected if available as they are listed before topologically closer nodes in the DNS records.
6	topology	neither	No	No co-located node pair listing; topologically closer node listing used if available (Same behavior as defined for (4).

Example

The following command instructs the MME or SGSN to determine gateway selection on the basis of topology:

```
gw-selection topology
```

hss

This command defines the HSS message specific configurations. Using this command the operator can control GPRS Subscription Data Requests in Update Location Request (ULR) messages to the HSS.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

hss message update-location-request gprs-subscription-indicator { never | non-epc-ue }
remove hss message update-location-request gprs-subscription-indicator

remove

Use this keyword to remove the configuration to GPRS Subscription Data requests in the ULR messages to the HSS.

message

Use this keyword to define the HSS message specific configurations.

update-location-request

Use this keyword to specify Update Location Request (ULR) message configuration.

gprs-subscription-indicator

The HSS includes the GPRS Subscription data in the ULA command if **gprs-subscription-indicator** keyword is set in the ULR message. By default, GPRS Subscription Data is always requested from the HSS.

never

Use this keyword to specify that GPRS Subscription Data should never be requested from the HSS.

non-epc-ue

Use this keyword to specify that GPRS Subscription Data should be requested from the HSS when the UE is not an EPC-capable device.

Usage Guidelines

This command provides operator control over GPRS Subscription Data Requests in ULR messages to the HSS. If this command is configured, the parameter GPRS-Subscription-Data-Indicator is set in the ULR message. The HSS includes the GPRS subscription data in the ULA command. If the GPRS subscription data is available in the HSS and GPRS-Subscription-Data-Indicator bit is set in the ULR message, the HSS includes the GPRS Subscription data in the ULA command. By default, GPRS Subscription Data is always requested from the HSS.

Example

Use the following command to ensure the SGSN will not request GPRS Subscription Data from the HSS.

hss message update-location-request gprs-subscription-indicator never

Use the following command to ensure the SGSN will request GPRS Subscription Data from the HSS for Non-EPC-capable UEs.

hss message update-location-request gprs-subscription-indicator non-epc-ue

ie-override

This command is used to override the RAT type AVP value with the configured value for messages sent from MME to HSS.

Important This command ensures backward compatibility with previous releases as the HSS does not support the new NB-IoT RAT type.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-call-control-profile-`*`profile_name`*`)#`

Syntax Description

[remove] ie-override s6a rat-type wb-eutran

remove

The keyword remove deletes the existing configuration.

ie-override

This keyword allows the operator to configure IE override in messages sent from MME to HSS.

s6a

This keyword is used to specify the interface as s6a. The s6a interface used by the MME to communicate with the Home Subscriber Server (HSS).

rat-type

Use this keyword to configure the supported RAT type AVP IE.

wb-eutran

Use this keyword to specify the WB-EUTRAN AVP Value.

Usage Guidelines Use this command to override the RAT type AVP value with the configured value for messages sent from MME to HSS over the s6a interface. If the configured RAT type is NB-IoT, it is changed to wb-eutran for messages sent from the MME to HSS. This command is not enabled by default.

Example

The following command is used to enable override of the RAT type AVP value with the configured value of WB-EUTRAN:

```
ie-override s6a rat-type wb-eutran
```

ignore-ul-data-status

This command is used to enable or disable processing of Uplink Data Status IE in Service Request.

Product SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
[ remove ] ignore-ul-data-status
```

remove

Use this keyword to enable processing of Uplink Data Status IE in Service Request.

Usage Guidelines This feature is enabled by default, to disable the feature use the command **ignore-ul-data-status**. To enable this feature use the command **remove ignore-ul-data-status**. When this feature is enabled, RAB is established for NSAPIs present in the Uplink data status IE. RABs are not established if the NSAPI PDPs are not present in the SGSN. If the Uplink data Status IE contains NSAPI not known to the SGSN, the SGSN establishes all the RAB's. RAB's are not established if corresponding NSAPI is absent in the PDP-Context Status IE. When this feature is disabled, if Uplink data status IE is received in service request the SGSN ignores it and establishes RAB's for all the PDP's.

Example

Use the following command to disable processing of Uplink Data Status IE in Service Request:

```
ignore-ul-data-status
```

idle-mode-signaling-reduction

Enables or disables the Idle-Mode-Signaling-Reduction (ISR) feature on the S4-SGSN.

Product SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description **`[ remove ] idle-mode-signaling-reduction access-type [ gprs | umts ]`**

remove

Disables the ISR feature configuration from this call control profile.

idle-mode-signaling-reduction

Configures ISR for this call control profile.

access-type

Specifies the network access type for the ISR feature. Select one of the following options:

- **gprs** - General Packet Radio Service network. Specifies 2G network access support for the ISR feature. *This option is only supported for Release 15.0 and beyond.*
- **umts** - Universal Mobile Telecommunications System network. Specifies 3G network access support for the ISR feature.

Usage Guidelines Use this command to enable or disable the ISR feature on the S4-SGSN. Note that ISR is supported on the S4-SGSN only.

This command is available only if the *Idle Mode Signaling Reduction* license is enabled on the SGSN.

When 3G ISR is enabled, operators should set the ISR deactivation timer value sent by the S4-SGSN to the UE in Attach Accept and Routing Area Update Accept messages. Use the **gmm T3323-timeout** command in *SGSN Service Configuration Mode* to set the ISR deactivation timer value.

When 2G ISR is enabled, operators should set the implicit detach timeout value to use for 2G ISR. Use the **gmm implicit-detach-timeout** command in *GPRS Service Configuration Mode*.

Example

`idle-mode-signaling-reduction access-type umts`

ims-apn

Use this command to add or remove network identifier in Call Control Profile.

Product SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

ims-apn network-identifier *network_identifier_name*

remove ims-apn network-identifier

network_identifier_name

Configures the network identifier on MME. Once configured APN is considered as IMS APN and UE is allowed attempt IMS PDN connection only if it is subscribed to that APN. network_identifier_name Must be string of 1 through 63 characters. It should consist only of alphabetic characters (A-Z and a-z), digits (0-9), dot(.) and the dash (-).

remove

Removes the network identifier configured for IMS APN.

Example

Use the following command to add or remove network identifier in Call Control Profile:

ims-apn network-identifier *network_identifier_name*

integrity-algorithm-lte

Specifies the order of preference for using an Integrity Algorithm.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

```
integrity-algorithm-lte priority1 { 128-eia0 | 128-eia1 | 128-eia2 |
128-eia3 } [ priority2 { 128-eia0 | 128-eia1 | 128-eia2 | 128-eia3 } ] [
 priority3 { 128-eia0 | 128-eia1 | 128-eia2 | 128-eia3 } ] [ priority4 {
 128-eia0 | 128-eia1 | 128-eia2 | 128-eia3 } ]
remove integrity-algorithm-lte
```

remove

Deletes the priorities definition from the call control profile configuration.

priority1

Specifies the preference of integrity algorithm for security procedures on this call control profile as priority 1.

This is the mandatory and default priority keyword.

priority2

Specifies the preference of integrity algorithm for security procedures on this call control profile as priority 2.

priority3

Specifies the preference of integrity algorithm for security procedures on this call control profile as priority 3.

priority4

Specifies the preference of integrity algorithm for security procedures on this call control profile as priority 4.

128-eia0

Sets the Null ciphering algorithm (128-EIA0) for LTE integrity as the integrity algorithm for security procedures.

Default: priority1

128-eia1

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: priority2

128-eia2

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

Default: priority3

128-eia3

Sets the ZUC algorithm (128-EIA3) for LTE integrity as the integrity algorithm for security procedures.

Default: priority4

Usage Guidelines Set the order or priority in which the MME will select an integrity algorithm for use. All the priorities must be set or the definition is invalid. The command can be re-entered to change the priorities without removing the configuration.

Example

Configure 128-EIA0 as first priority integrity algorithm:

```
integrity-algorithm-lte priority1 128-eia 0 priority2 128-eia 2 priority3
 128-eia 1
```

integrity-algorithm-umts

Configures the order of preference for the Integrity Algorithm used for 3G.

Product SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-call-control-profile-`*`profile_name`*`)#`

Syntax Description

integrity-algorithm-umts *type* **then_** *type*
default integrity-algorithm-umts

default

Specifies the default preference based on system defaults.

type

Creates a configuration defining an order of preference. Enter one or more of the following options in the order of preference:

- **uia1** - uia1 Algorithm
- **uia2** - uia2 Algorithm

Usage Guidelines Use this command to determine which integrity algorithm is preferred 3G. This command is configured in tandem with the algorithm type for **encryption-algorithm-umts** command.

Example

```
default integrity-algorithm-umts
```

lcs-mo

This command enables/disables mobile-originating Location Requests by access-type when Location Services functionality is enabled.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

`lcs-mo { allow | restrict } access-type { gprs | umts }`

allow

Enables mobile-originating Location Requests. This is the default state when Location Services are enabled.

Usage Guidelines

This command ties Location Service functionality to a call-control profile by IMSI so that Location Services can optionally be determined by an operator policy for incoming calls.

Example

Use the following command to disable or disallow mobile-originating Location Requests within a GPRS network:

`lcs-mo restrict access-type gprs`

lcs-mt

This command enables/disables mobile-terminating Location Requests by access-type when Location Services functionality is enabled.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

`lcs-mt { allow | restrict } access-type { gprs | umts }`

allow

Enables mobile-terminating Location Requests. This is the default state when Location Services are enabled.

Usage Guidelines

This command ties Location Service functionality to a call-control profile by IMSI so that Location Services can optionally be determined by an operator policy for incoming calls.

Example

Use the following command to disable or disallow mobile-terminating Location Requests within a UMTS network:

```
lcs-mt restrict access-type umts
```

lcs-ni

This command enables/disables network-initiated Location Requests by access-type when Location Services functionality is enabled.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-call-control-profile-`*`profile_name`*`)#`

Syntax Description

```
lcs-ni { allow | restrict } access-type { gprs | umts }
```

allow

Enables network-initiated Location Requests . This is the default state when Location Services are enabled.

Usage Guidelines

This command ties Location Service functionality to a call-control profile by IMSI so that Location Services can optionally be determined by an operator policy for incoming calls.

Example

Use the following command to enable or allow network-initiated Location Requests within a UMTS network if this function has been restricted previously:

```
lcs-ni allow access-type umts
```

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 > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

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 } remove local-cause-code-mapping apn-mismatch`

remove local-cause-code-mapping apn-mismatch

Removes the configured 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 }

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**

Usage Guidelines

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.

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 mme-service configuration mode. This command is described in the *MME Service Configuration Mode Commands* chapter.

Example

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 > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

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

remove

Deletes the local cause code mapping from the configuration.

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.

The new keyword apn-not-subscribed is added to specify the local cause-code mapping when the UE-requested APN is not subscribed for that subscriber. If cause code mapping for apn-not-subscribed is explicitly configured with requested-service-option-not-subscribed in either the Call-Control-Profile or MME-Service configuration mode, then the new code "Requested-Option-Not-Subscribed" (cause-code #33) will be sent in the Reject message when the PDN Connectivity Request is rejected because no subscription is found.

Example

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

In support of 3GPP Release 11 EMM/ESM cause code #66, this command remaps the EMM/ESM/SM cause codes to operator-preferred codes in the Call Control Profile. These replacements codes are sent in Reject messages when the activation rejection is due to the APN not being supported in the requested PLMN/RAT.

Product

SGSN

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

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-code** *esm_cause_number* **esm-proc | sm-cause-code** *sm_cause_number* **}**
remove local-cause-code-mapping apn-not-supported-in-plmn-rat [attach | esm-proc | sm-cause-code | tau]

remove

Removes the configured cause code mapping.

apn-not-supported-in-plmn-rat

The keyword **apn-not-supported-in-plmn-rat** specifies that the MME is to use the mapped operator-preferred replacement cause codes when a call is rejected because the requested APN is not supported in current RAT and PLMN combination.

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.

sm-cause-code *sm_cause_number*

SGSN only.

The keyword **sm-cause-code** identifies the operator-preferred SM cause code to be used towards the UE. *sm_cause_number* value can be any integer in the range 0 through 255.

Usage Guidelines

This command specifies the cause codes that operator would prefer to send our in Reject messages when the cause of the call rejection is the APN not being supported in the current RAT and PLMN combination. This mapping is not done by default.

- The **emm-cause-code** keyword is used to specify the EMM cause code to be used if a NAS request is rejected due to this configuration.
- The **esm-cause-code** keyword is used to specify the ESM cause code to be used if a bearer management request is rejected due to this configuration.
- The **sm-cause-code** keyword is used to specify the SM cause code used towards UE.

Example

The following command maps cause code *20* in place of standard cause code #66 for the SGSN to send in activate rejection messages.

```
local-cause-code-mapping apn-not-supported-in-plmn-rat sm-cause-code 20
```

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 > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
local-cause-code-mapping 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 }
remove local-cause-code-mapping auth-failure
```

remove local-cause-code-mapping auth-failure

Removes the configured cause code mapping.

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**
- **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 an authentication failure occurs. By default, the MME sends the UE the **#3 - Illegal MS** cause code when encountering an authentication failure.

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 sent by the UE.
- The UE responds to any identity request with a different type of identity (for example, 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 mme-service configuration mode. This command is described in the *MME Service Configuration Mode Commands* chapter.

Example

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 > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

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 }
remove local-cause-code-mapping congestion
```

remove local-cause-code-mapping congestion

Removes the configured cause code mapping.

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**

Usage Guidelines

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.

To set the cause codes for situations where a call control profile cannot be attached to a call (for example new-call restrictions, congestion during new call attempt, etc.), use the **local-cause-code-mapping** command in the mme-service configuration mode. This command is described in the *MME Service Configuration Mode Commands* chapter.

Example

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 > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-call-control-profile-`*`profile_name`*`)#`

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 }
remove local-cause-code-mapping ctxt-xfer-fail-mme
```

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

Removes the configured 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 }

Specifies the EPS Mobility Management (EMM) cause code to return when a UE context transfer failure from a peer 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**

Usage Guidelines

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 mme-service configuration mode. This command is described in the *MME Service Configuration Mode Commands* chapter.

Example

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 > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

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 }
remove local-cause-code-mapping ctxt-xfer-fail-sgsn
```

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

Removes the configured 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 }

Specifies the EPS Mobility Management (EMM) cause code to return when a UE context transfer failure from a peer 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**

Usage Guidelines

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 mme-service configuration mode. This command is described in the *MME Service Configuration Mode Commands* chapter.

Example

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 > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

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 }
remove local-cause-code-mapping gw-unreachable [ attach | tau ]
```

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

Removes the configured 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 }

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.

Usage Guidelines

Use this command to configure the cause code returned to a UE when a gateway (S-GW or P-GW) does not respond during an EMM procedure.

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 mme-service configuration mode. This command is described in the *MME Service Configuration Mode Commands* chapter.

Example

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 > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

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 }
remove local-cause-code-mapping hss-unavailable
```

remove local-cause-code-mapping hss-unavailable

Removes the configured 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 }

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**
- **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 the HSS is unavailable. 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 mme-service configuration mode. This command is described in the *MME Service Configuration Mode Commands* chapter.

Example

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 map-cause-code

Configures the operator-preferred GMM reject cause code to send to a UE in response to some failures, such as Inbound RAU Context Transfer failure .

Product SGSN

Privilege Administrator

Command Modes Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
local-cause-code-mapping map-cause-code { roaming-not-allowed
gmm-cause-code gmm-cause | unknown-subscriber { gmm-cause-code gmm-cause |
map-diag-info { gprs-subscription-unknown gmm-cause-code gmm-cause |
imsi-unknown gmm-cause-code gmm-cause } } }
remove local-cause-code-mapping map-cause-code { roaming-not-allowed |
unknown-subscriber { gmm-cause-code  | map-diag-info {
gprs-subscription-unknown  | imsi-unknown  } } }
```

remove

Removes the specified, previously configured cause code mapping .

roaming-not-allowed

Instructs the SGSN to send a different GPRS mobility management (GMM) cause code to a UE when the UE's access request is rejected due to map cause 'roaming not allowed'. Specify one of the GMM cause codes listed below.

unknown-subscriber

Instructs the SGSN to send a different GPRS mobility management (GMM) cause code to a UE when the UE's access request is rejected due to map cause 'unknown-subscriber'. As well, the Operator is given the *option* to include MAP diagnostic information in the Reject message to provide additional details about the MAP failure.

- **gmm-cause-code** replaces the cause code. For options see below.
- **map-diag-info** instructs the SGSN to include one of two types of MAP diagnostic information in the Reject message *AND* specifies the replacement GMM cause code to use in the Reject message.
  - **gprs-subscription-unknown**
  - **imsi-unknown**

gmm-cause-code *gmm-cause*

Specifies the GPRS mobility management (GMM) cause code to return to a UE in access request Reject messages. Replacement cause code options include:

- **gprs-serv-and-non-gprs-serv-not-allowed**
- **gprs-serv-not-allowed**
- **gprs-serv-not-in-this-plmn**
- **location-area-not-allowed**
- **network-failure**

- **no-suitable-cell-in-this-la**
- **plmn-not-allowed**
- **roaming-not-allowed-in-this-la**

Usage Guidelines

This command enables the operator to configure a preferred GMM cause code to return to the UE when a UE access request is rejected due to map-cause 'roaming-not-allowed' or 'unknown-subscriber'.

As well, the operator can send additional MAP failure details in the reject message when the map-cause being replaced is 'unknown-subscriber'.

It is possible to map replacement cause codes for both 'roaming-not-allowed' and 'unknown-subscriber, but additional configurations for either would overwrite.

Example

The following command maps *network-failure* as the GMM cause code to be included in an Access Reject sent to the UE when the UE is denied due to map-cause 'roaming-not-allowed':

```
local-cause-code-mapping map-cause-code roaming-not-allowed gmm-cause-code
 network-failure
```

Use the following to change a mapping configuration of 'unknown-subscriber' replaced by 'roaming-not-allowed-in-this-la' to 'unknown-subscriber' replaced by cause code 'gprs-serv-not-in-this-plmn' and include MAP diagnostic information in the Reject message:

```
local-cause-code-mapping map-cause-code unknown-subscriber map-diag-info
 gprs-subscription-unknown gmm-cause-code gprs-serv-not-in-this-plmn
```

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 > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

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 }
remove local-cause-code-mapping no-active-bearers
```

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

Removes the configured 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 }

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**
- **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 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 mme-service configuration mode. This command is described in the *MME Service Configuration Mode Commands* chapter.

Example

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 odb packet-services

Configures the ESM and EMM cause codes to send to a UE depending on the Operator Determined Barring (ODB) condition.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
local-cause-code-mapping odb packet-services emm-cause-code cc_value [
esm-cause-code cc_value ]
remove local-cause-code-mapping odb packet-services
```

remove local-cause-code-mapping odb packet-services

Removes the configured cause code mapping.

packet-services emm-cause-code *cc_value* [esm-cause-code *cc_value*]

Specifies the EPS Mobility Management (EMM) cause code to return when ODB condition is hit.

emm-cause-code *cc_value* : Specifies the EMM cause code for ODB all packet services. The EMM cause code value is an integer from 0 to 255.

esm-cause-code *cc_value* : This is an optional keyword used to specify the ESM cause code as an integer from 0 to 255.

Usage Guidelines

Use this command to configure the cause code returned to a UE when ODB condition is hit, such as when the subscriber does not have an LTE/EPS subscription.

Related Commands:

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 signaled to the UE. See also the **local-cause-code-mapping** command in the mme-service configuration mode. This command is described in the *MME Service Configuration Mode Commands* chapter.

Example

The following command maps the EMM cause code #15 (NO_SUITABLE_CELL_IN_TRACKING_AREA) to the ODB condition:

```
local-cause-code-mapping odb packet-services emm-cause-code 15
```

local-cause-code-mapping odb roamer-to-vplmn

Configures the ESM and EMM cause codes to send to a UE depending on the Operator Determined Barring (ODB) condition.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

`local-cause-code-mapping odb roamer-to-vplmn emm-cause-code` *`cc_value`* `[ esm-cause-code` *`cc_value`* `]`
`remove local-cause-code-mapping odb roamer-to-vplmn`

remove local-cause-code-mapping odb roamer-to-vplmn

Removes the configured cause code mapping.

roamer-to-vplmn emm-cause-code *cc_value* [esm-cause-code *cc_value*]

Specifies the EPS Mobility Management (EMM) cause code to return when ODB condition is hit.

emm-cause-code *cc_value* : Specifies the EMM cause code for ODB roamer to visited PLMN. The EMM cause code value is an integer from 0 to 255.

esm-cause-code *cc_value* : This is an optional keyword used to specify the ESM cause code as an integer from 0 to 255.

Usage Guidelines

Use this command to configure the cause code returned to a UE when ODB condition is hit, such as when the subscriber does not have an LTE/EPS subscription.

Related Commands:

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 signaled to the UE. See also the **local-cause-code-mapping** command in the mme-service configuration mode. This command is described in the *MME Service Configuration Mode Commands* chapter.

Example

The following command maps the EMM cause code #15 (NO_SUITABLE_CELL_IN_TRACKING_AREA) to the ODB condition:

```
local-cause-code-mapping odb roamer-to-vplmn emm-cause-code 15
```

local-cause-code-mapping path-failure

Configures SM cause codes for SGSN to send in Deactivate PDP Request.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-call-control-profile-`*`profile_name`*`)#`

Syntax Description

`local-cause-code-mapping path-failure sm-cause-code {`
`insufficient-resources | network-failure | reactivation-requested |`

regular-deactivation }
remove local-cause-code-mapping path-failure

remove

Erases defined cause code configuration.

sm-cause-code

Defines the SM cause code to replace the default cause code sent in a Deactivate PDP Request message when a GTP-C path failure occurs. Options include:

- insufficient-resources
- network-failure
- reactivation-requested
- regular-deactivation

Usage Guidelines

This command is part of the Cause Code Mapping feature, documented in the *SGSN Administration Guide*, that provides the operator with the option to configure preferred cause codes to be sent in error or failure messages to the UE.

Example

Use the following command to replace the default cause code with SM cause *network-failure*:

local-cause-code-mapping path-failure sm-cause-code network-failure

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 > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-call-control-profile-`*`profile_name`*`)#`

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

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

Removes the configured 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 }

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

- **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 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 mme-service configuration mode. This command is described in the *MME Service Configuration Mode Commands* chapter.

Example

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 > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

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 }
remove local-cause-code-mapping pgw-selection-failure
```

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

Removes the configured 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 }

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**
- **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 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 mme-service configuration mode. This command is described in the *MME Service Configuration Mode Commands* chapter.

Example

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 UE requests access to a restricted zone.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

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 }
remove local-cause-code-mapping restricted-zone-code
```

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

Removes the configured cause code mapping.

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**

Usage Guidelines

Use this command to configure the cause code returned to a UE when a UE requests access to a restricted zone.

To set the cause codes for situations where a call control profile cannot be attached to a call (for example new-call restrictions, congestion during new call attempt, etc.), use the **local-cause-code-mapping** command in the mme-service configuration mode. This command is described in the *MME Service Configuration Mode Commands* chapter.

Example

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 > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

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 }
remove local-cause-code-mapping sgw-selection-failure
```

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

Removes the configured 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 }

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**
- **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 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 mme-service configuration mode. This command is described in the *MME Service Configuration Mode Commands* chapter.

Example

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 > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

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

remove local-cause-code-mapping vlr-down

Removes the configured cause code mapping.

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**

Usage Guidelines

Use this command to configure the cause code returned to a UE when a VLR down condition is present.

To set the cause codes for situations where a call control profile cannot be attached to a call (for example new-call restrictions, congestion during new call attempt, etc.), use the **local-cause-code-mapping** command in the mme-service configuration mode. This command is described in the *MME Service Configuration Mode* Commands chapter.

Example

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 > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

`local-cause-code-mapping vlr-unreachable emm-cause-code { congestion | cs-domain-unavailable | imsi-unknown-in-hlr | msc-temp-unreachable | network-failure }`
`remove local-cause-code-mapping vlr-unreachable`

remove local-cause-code-mapping vlr-unreachable

Removes the configured cause code mapping.

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**

Usage Guidelines

Use this command to configure the cause code returned to a UE when a VLR unreachable condition is present.

To set the cause codes for situations where a call control profile cannot be attached to a call (for example new-call restrictions, congestion during new call attempt, etc.), use the **local-cause-code-mapping** command in the mme-service configuration mode. This command is described in the *MME Service Configuration Mode* Commands chapter.

Example

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-area-list

Defines the location area list to allow or restrict services in the specified location areas identified by location area code (LAC).

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

`location-area-list instance` *`instance`* **`area-code`** *`area_code`* **`[`** *`area_code *`* **`]`**
`no location-area-list instance` *`instance`* **`[ area-code`** *`area_code`* **`]`**

no

If the **area-code** keyword is included in the command, then only the specified area code is removed from the identified list. If the **area-code** keyword is not included with the command, the entire list of LACs is removed from this call control profile.

instance *instance*

Specifies an identification for the specific location area list.

instance must be an integer between 1 and 5.

area-code *area_code **

This keyword defines the location area codes (LACs) to be used by this call control profile as a determining factor in the handling of incoming calls. Multiple LACs can be defined in a single location-area-list.

area_code: Enter an integer between 1 and 65535.

* If desired, enter multiple LACs separated by a single blank space.

Usage Guidelines

Use the command multiple times to configure multiple LAC lists or to modify the a list.

Example

The following command creates a location area list for a single area code:

```
location-area-list instance 1 area-code 514
```

This command creates a second location area list for with multiple area codes - all separated by a single blank space:

```
location-area-list instance 2 area-code 514 62552 32 1513
```

The next command corrects an area code mistake (327 not 32) made in the previous configuration:

```
location-area-list instance 1 area-code 514 62552 327 1513
```

location-reporting

Enable 3G/2G Location Change Reporting feature on the SGSN.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

`[ remove ] location-reporting access-type { gprs | umts }`

remove

If the **remove** keyword is included in the command, then the location change reporting feature is disabled.

access-type *type*

Defines the type of subscriber access which is to reported for location changes.

- **gprs** - 2G
- **umts** - 3G

Usage Guidelines

Use the command multiple times to configure both types of access types.

This command enables the 3G/2G Location Change Reporting feature which notifies the GGSN whenever one of the following changes for a UE:

- the serving cell global identity (CGI), or
- the service area identity (SAI), or
- the routing area identity (RAI).

Example

The following command enables location change reporting to a GGSN for 3G subscribers:

`location-reporting access-type umts`

This command disables location change reporting that has been enabled for 2G subscribers:

`remove location-reporting access-type gprs`

lte-zone-code

Configures the enforcement of allowed or restricted zone code lists and associates an EPS Mobility Management (EMM) cause code to rejected attach attempts.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

lte-zone-code [allow | restrict } { 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] zone-code-list *zc_id* **+**
remove lte-zone-code zone-code-list

remove

Removes the zone code list from the call control profile.

[allow | restrict]

Specifies whether the zone code list is allowed or restricted.

Important You can only create an allowed or restricted list, not both.

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]

Optionally, specify one of the following EMM cause codes to apply when a UE request is rejected:

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

zone-code-list *zc_id* +

Specifies the zone code in the allowed or restricted list of zone codes. *zone_code* must be an integer value from 0 to 65535.

Usage Guidelines

Use this command to create zone code lists that allow or restrict access to UEs managed by this call control profile.

Example

The following command restricts access to zone codes 234 and 456 and returns an EMM cause code of "tracking area not allowed":

```
lte-zone-code restrict emm-cause-code tracking-area-not-allowed
zone-code-list 234 456
```

map

Configures the optional extensions to Mobile Application Part (MAP) messages.Using this command the operator can control GPRS/EPS Subscription data requests in UGL messages to the HLR.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

`[ remove ] map message { mo-fwd-sm imsi | update-gprs-location { eps-subscription-not-needed [ always | non- epc-ue ] | exclude-gmlc | gprs-subscription-not-needed [ always | epc-ue ] | imeisv | private-extension access-type } }`
`remove map message update-gprs-location gprs-subscription-not-needed`
`remove map message update-gprs-location eps-subscription-not-needed`

remove

IMEI-SV is not included in the GLU request -- this is the default behavior. The remove option is also used to remove the configuration of GPRS subscription data or EPS subscription data requests in UGL messages to the HLR.

message mo-fwd-sm imsi

Configures the SGSN to include the IMSI of the originating subscriber in the mobile-originated SM transfer. This parameter shall be included when the sending entity (MSC or SGSN) supports mobile number portability (MNP). This IMSI IE is required in the in MAP-MO-FORWARD-SHORT-MESSAGE in countries where MNP is deployed.This keyword-set is required. The default is disabled.

update-gprs-location

Includes a GLU message.

eps-subscription-not-needed

The operator can use this keyword to control the request for EPS Subscription Data in addition to GPRS Subscription Data from the HLR. By default, EPS Subscription Data is always requested from the HLR.

Optionally include:

- **always** - Include this keyword to specify that EPS Subscription Data should never be requested from the HLR.
- **non-epc-ue** - Include this keyword to specify that EPS Subscription Data should never be requested from the HLR when the UE is not an EPC capable device.

exclude-gmlc

This keyword configures the SGSN to exclude the GMLC address in the Update-GPRS-Location (UGL) messages sent to the HLR.

gprs-subscription-not-needed

The operator can use this keyword to control the request for GPRS Subscription Data in addition to EPS Subscription Data from the HLR. By default, GPRS Subscription Data is always requested from the HLR.

Optionally include:

- **always** - Include this keyword to specify that GPRS Subscription Data should never be requested from the HLR.
- **non-epc-ue** - Include this keyword to specify that GRPS Subscription Data should never be requested from the HLR when the UE is an EPC capable device.

imeisv

Specifies the International Mobile equipment Identity-Software Version (IMEI-SV) information to include in the GPRS Location Update (GLU) request message. SGSN will include IMEI-SV in the message, if available. Default: disabled

private-extension access-type

Includes a specific access-type private extension in the message.

Usage Guidelines

This command configures optional extensions to MAP messages. The HLR should ignore these extensions if not supported by the HLR. This command allows operator control over the GPRS Subscription Data or EPS Subscription Data requests in UGL messages to the HLR.

Example

Use the following command to have the SGSN add GLU extension information to the MAP messages sent to the HLR.

```
map message update-gprs-location private-extension access-type
```

Use the following command to ensure the SGSN (or MME/ IWF) will not request GPRS Subscription Data in addition to EPS Subscription Data from the HLR.

```
 map message update-gprs-location gprs-subscription-not-needed always
```

Use the following command to ensure the SGSN (or MME/ IWF) will not request GPRS Subscription Data in addition to EPS Subscription Data from the HLR for EPC capable UEs.

```
map message update-gprs-location gprs-subscription-not-needed epc-ue
```

Use the following command to ensure the SGSN will not request EPS Subscription Data in addition to GPRS Subscription Data from the HLR.

```
map message update-gprs-location eps-subscription-not-needed always
```

Use the following command to ensure the SGSN will not request EPS Subscription Data in addition to GPRS Subscription Data from the HLR for Non-EPC capable UEs.

```
map message update-gprs-location eps-subscription-not-needed non-epc-ue
```

map-service

Identifies a Mobile Application Part (MAP) service and the context which contains it and associates both with the call control profile.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

`map-service context` *`ctxt_name`* **`service`** *`map_srvc_name`*
`no map-service context`

no

Disables use of MAP service with this call control profile.

context *ctxt_name*

Specifies the name of the context for the MAP service as an alphanumeric string of 1 through 64 characters.

service *map_srvc_name*

Specifies the MAP service name as an alphanumeric string of 1 through 64 characters.

Usage Guidelines

Use this command to enable or disable MAP service with this call control profile.

Example

```
no map-service context
```

max-bearers-per-subscriber

Defines the maximum number of bearers allowed per subscriber.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

max-bearers-per-subscriber *number*
remove max-bearers-per-subscriber

remove

Deletes the definition from the call control profile.

number

Identifies the maximum number of bearers allowed per subscriber as an integer from 1 to 11.

Usage Guidelines

Use this command to set the maximum number of bearers allowed per subscriber.

Example

Set the maximum to 3:

```
max-bearers-per-subscriber 3
```

max-pdns-per-subscriber

Defines the maximum number of PDNs allowed per subscriber.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

max-pdns-per-subscriber *number*
remove max-pdns-per-subscriber

remove

Deletes the definition from the call control profile.

number

Identifies the maximum number of PDNs allowed per subscriber as an integer from 1 to 11.

Usage Guidelines

Use this command to set the maximum number of PDNs allowed per subscriber.

Example

Set the maximum to 4:

```
max-pdns-per-subscriber 4
```

min-unused-auth-vectors

Configures a specific minimum number of unused vectors to be maintained by the SGSN.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

min-unused-auth-vectors *min#_vectors*
remove min-unused-auth-vectors

remove

Removes the definition from the configuration file and restores the default behavior, which does not use the threshold.

min#_vectors

Enables and defines a threshold for the minimum number of unused vectors that the SGSN retains to trigger the initation of a service area identity request (SAI) .

min#_vectors: Enter a digit betwen 1 and 4.

Usage Guidelines

Vectors are used by the SGSN for authentication. Use this command to enable a minimum threshold for unused vector for this call control profile. When the unused vector count falls below this configured threshold, then an SAI is initiated to fill the buffer back to 5 or to the most appropriate number based on the MAP service configuration.

Example

Enter a command similar to the following to set a threshold of *3*:

```
min-unused-auth-vectors 3
```

Use the following command to disable this function and restore the default behavior, which does not use a threshold to trigger an SAI:

```
remove min-unused-auth-vectors
```

mme s6a

This command is used to control sending the Notify Request (NOR) on the S6a interface.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

`[ no ] mme s6a send message nor trigger mnrf`

no

Disables sending the NOR on the S6a interface.

mme

Configures MME capability.

s6a

Configures MME capability on the S6a interface.

send

Configures MME capability to send on the S6a interface.

message

Configures MME capability to send message on the S6a interface.

nor

Configures MME capability to send NOR on the S6a interface.

trigger

Configures trigger to send the message.

mnrf

Sends message to trigger MNRF flag on the S6a interface (SMS in MME).

Usage Guidelines

Use this command to control sending the NOR on the S6a interface. This command is disabled by default.

The user sends the NOR on the S6a interface to HSS in the event of user availability to received SMS (if the user moved to active state from idle or the user's memory is available).

mme sgd

This command is used to control sending the Alert SC Request (ALR) on the SGd interface.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

`[ no ] mme sgd send message alr trigger mnrf`

no

Disables sending the ALR on the SGd interface.

mme

Configures MME capability.

sgd

Configures MME capability on the SGd interface.

send

Configures MME capability to send on the SGd interface.

message

Configures MME capability to send message on the SGd interface.

alr

Configures MME capability to send ALR on the SGd interface.

trigger

Configures trigger to send the message.

mnrf

Sends message to trigger MNRF flag on the SGd interface (SMS in MME).

Usage Guidelines

Use this command to control sending the ALR on the SGd interface. This command is disabled by default.

The user sends the ALR on the SGd interface to SMSC in the event of user availability to received SMS (if the user moved to active state from idle or the user's memory is available). It is also sent if the user did a handover to the new MME/SGSN and any MT SMS was pending for the user.

mobility-protocol

This command allows you to configure the default mobility protocol type to be used for setting up a call when the AAA server forwards an IP address directly.

Product

SaMOG

Privilege

Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-call-control-profile-`*`profile_name`*`)#`

Syntax Description

`mobility-protocol { GTPv1 | GTPv2 | pmip }`
`default mobility-protocol`

default

Sets the mobility-protocol configuration to its default values.

Default (SaMOG 3G license): GTPv1

Default (SaMOG Mixed Mode license): GTPv2

Usage Guidelines

Use this command to configure the default mobility protocol type to be used for setting up a call when the AAA server forwards an IP address directly. If the mobility protocol is also configured in the APN Profile Configuration Mode, the value configured here will be overridden with the configured value in the APN profile.

Example

The following command configures mobility protocol to GTPv2:

`mobility-protocol GTPv2`

mps

This command under the Call Control profile configuration mode is configured to support Multimedia Priority Service (MPS) in the CS/EPS domain.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

[remove] mps [cs-priority | eps-priority] { subscribed | none }

remove

The **remove** keyword deletes the existing configuration.

cs-priority

The keyword **cs-priority** configures support for priority service in the CS domain.

eps-priority

The keyword eps-priority configures support for MPS in the EPS domain.

subscribed

The keyword **subscribed** configures support for priority service in the CS/EPS domain.

none

The keyword **none** configures disables support for priority service in the CS/EPS domain.

Usage Guidelines

This CLI helps operator to override the MPS CS/EPS Subscription received from HSS. It allows the operator to prioritize the Mobile originating voice calls of a set of subscribers irrespective of them subscribed for MPS services or not. By default MME sets the value of "CS fallback indicator IE" as "CSFB High Priority" in the S1AP UE Context Setup/Modification if the MPS-CS-Priority bit is set in MPS-Priority AVP received from HSS.

Example

The following command is issued to set "CSFB High Priority" for "CS Fallback Indicator IE", in the S1AP UE Context Setup/Modification message:

```
[local]asr5x00(config-call-control-profile-call1)# mps cs-priority
subscribed
```

The following command is issued to set "CSFB Required" for "CS Fallback Indicator IE", in the S1AP UE Context Setup/Modification message:

```
[local]asr5000(config-call-control-profile-call1)# mps cs-priority none
```

msc-fallback-disable

Define all SRVCC causes for which the MME does not try sending PS-CS Request to a next available MSC, during an SRVCC handover, if the MME received one of the configured SRVCC causes in the PS-CS Response received from the first MSC.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

`[ remove ] msc-fallback-disable srvcc-cause` *`cause`*

remove

When added to the command, this command filter causes the MME to delete the specified SRVCC cause code definition.

srvcc-cause *cause*

This keyword configures an SRVCC cause code. If the MME receives this SRVCC cause code in a negative PS-CS Response from the first MSC tried in an SRVCC handover, then the MME sends SRVCC HO Failure and no other MSCs are tried. The *cause* must be any integer from 0 to 255, as defined in 3GPP TS 29.280.

Usage Guidelines

This command can be repeated to configure more than one SRVCC cause.

This command is only applicable for PS-CS Requests and not for PS to CS complete messages.

This command is applicable for both statically configured MSC addresses (in an MSC Pool) and for MSC addresses returned by DNS.

If this command is not used to define SRVCC causes, then the MME will use default behavior to select the next MSC to retry PS-CS Request.

To confirm the MME's current configuration of SRVCC causes, use the **show call-control-profile full** command to generate output with a list of the 'MSC fallback disabled SRVCC causes'.

Example

Use a command similar to the following to configure one or more SRVCC cause codes. The following set of commands configures three SRVCC cause codes:

```
msc-fallback-disable srvcc-cause 8
msc-fallback-disable srvcc-cause 9
msc-fallback-disable srvcc-cause 10
```

nb-iot

This command enables Extended Discontinuous Reception (eDRX) and configures the respective parameters for NB-IoT subscribers on the MME.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

```
nb-iot  {  edrx { ptw ptw_value edrx-cycle cycle_length_value | ue-requested }
 [ dl-buf-duration [ packet-count packet_count_value ] ] | mo-exception-data
 reporting-threshold-value threshold_value  }
remove nb-iot {  edrx  | mo-exception-data }
```

remove

This keyword disables the eDRX configuration on the MME for NB-IoT subscribers.

edrx

This keyword configures extended discontinuous reception parameters.

ptw *ptw_value*

This keyword configures the Paging Time Window (PTW) value. *ptw_value* must be an integer value in seconds. The allowed values are 2.56, 5.12, 7.68, 10.24, 12.80, 15.36, 17.92, 20.48, 23.04, 25.60, 28.16, 30.72, 33.28, 35.84, 38.40 and 40.96 seconds.

ue-requested

This keyword specifies the UE requested values of the Paging Time Window (PTW) and the eDRX cycle length received from the UE in the Attach Request or TAU Request message be accepted.

edrx-cycle *cycle_length_value*

This keyword configures the eDRX cycle length. *cycle_length_value* is an integer value in seconds. The allowed values are 5.12, 7.68, 10.24, 12.80, 15.36, 17.92, 20.48, 40.96, 81.92, 163.84, 327.68, 655.36, 1310.72, 2621.44, 5242.88 and 10485.76 seconds.

dl-buf-duration

This optional keyword sends downlink buffer duration in DDN ACK when unable to page UE.

packet-count *packet_count_value*

This optional keyword sends "DL Buffering Suggested Packet Count" in DDN ACK when unable to page UE. The *packet_count_value* is an integer value from 0 to 65535. If the *packet_count_value* is not configured locally, the subscription provided value for the *packet_count_value* is used. The subscription value can be 0 in which case the packet count IE will not be sent for that subscriber even if it is configured locally.

mo-exception-data

Configures NBIOT RRC Cause MO Exception Data counter.

reporting-threshold-value *value*

Specifies reporting threshold value. *value* Must be an integer from 1 to 50.

Usage Guidelines

Use this command to enable eDRX on the MME for NB-IoT subscribers. The operator can use this command for:

- Accept eDRX parameters: Paging Time Window (PTW) and eDRX cycle length value, from the UE
- Configure PTW and eDRX cycle length value
- Configure downlink buffer duration in DDN ACK when unable to page UE
- Configure "DL Buffering Suggested Packet Count" in DDN ACK when unable to page UE

When the eDRX feature is enabled on the MME, it pages the NB-IoT subscribers only at valid paging occasions. The MME sends the NB-IoT eDRX paging parameters to the eNodeB during paging. The operator can either configure the option to accept the UE requested values or configure the values using this command. This command is not enabled by default.

A similar CLI command is implemented for WB-EUTRAN subscribers. Both WB-UTRAN eDRX and NB-IoT eDRX parameters can be configured on the system for WB-UTRAN and NB-IoT subscribers.

See the *eDRX Support on the MME* feature chapter in the *MME Administration Guide* for more information.

Example

The following command configures the PTW and eDRX cycle length. The command also sends the downlink buffer duration in the DDN ACK along with a suggested packet count:

```
nb-iot edrx ptw 256 edrx-cycle 512 dl-buf-duration packet-count 10
```

network-feature-support-ie

Configures support for the IMS Voice over Packet-Switched indication and Homogenous Support of IMS Voice over PS indication.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
network-feature-support-ie ims-voice-over-ps [ not-supported | supported
 srvcc-ue-with-voice-domain-pref ]
remove network-feature-support-ie
```

remove

Disables support for Voice over PS.

ims-voice-over-ps [not-supported | supported]

Enables support for Voice over PS in all Tracking Areas.

not-supported: Configures the MME to add the "Homogenous Support of IMS Voice over PS Sessions" AVP to the S6a Update-Location-Request and Notify Request messages to the HSS, with the value set to "Not Supported". This indicates that IMS Voice over PS is **not** supported in **any** Tracking Areas.

supported: Configures the MME to add the "Homogenous Support of IMS Voice over PS Sessions" AVP to the S6a Update-Location-Request and Notify Request messages to the HSS, with the value set to "Supported". This indicates that IMS Voice over PS is supported in all Tracking Areas.

srvcc-ue-with-voice-domain-pref: IMS Voice Over PS not Supported for srvcc with cs voice preference UE only.

If the command is entered without either the **supported** or **not-supported** keywords, then MME indicates network feature support in the Attach Accept sent to the UE and includes the "Homogenous Support of IMS Voice over PS Sessions" AVP to the S6a Update-Location-Request and Notify Request messages sent to the HSS, with the value set to "Not Supported". This indicates that IMS Voice over PS is supported in all Tracking Areas.

Usage Guidelines

Use this command to include the "IMS Voice over PS" indication, thereby indicating support for IMS Voice over PS sessions for all Tracking Areas.

This command also configures whether to include the "Homogenous Support of IMS Voice over PS Sessions" indication as well as the included in the indication, either supported or not supported.

Example

The following command enables support for IMS Voice over PS on the MME:

```
network-feature-support-ie ims-voice-over-ps
```

network-initiated-pdp-activation

Configures the call control profile to perform two functions: (1) to enable or disable network-requested PDP context activation (NRPCA) for 3G attachments and (2) to define a failure cause code for inclusion in NRPCA-related reject messages.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

`[ remove ] network-initiated-pdp-activation { allow primary | restrict primary | secondary } access type { gprs | umts } { all | location-area-list instance` *<instance>* **}**
`network-initiated-pdp-activation primary access type { gprs | umts } { all | location-area-list instance` *<instance>* **} failure-code** *code*
`network-initiated-pdp-activation secondary access type { gprs | umts } { all | location-area-list instance` *<instance>* **} failure-code** *code*

remove

Including this keyword with the command, removes all configured values for the specified configuration.

allow

Allows network-initiated PDP context activation. This keyword must be followed by other parameters to indicate the limitations for allowing the NRPCA.

Allow is the default for NRPCA.

restrict

Restricts network-initiated PDP context activation. This keyword must be followed by other command parameters to indicate the limitations for restricting the NRPCA.

primary

Specifies that only network-initiated primary PDP context activations are to be allowed.

secondary

Specifies that only network-initiated secondary PDP context activations (NRSPCAs) are to be allowed.

Important The **secondary** keyword is visible and can be selected. However, NRSPCA functionality is only supported for Release 15.0 onwards.

all

Configures the SGSN to allow or to restrict NRPCA for calls within all location areas.

location-area-list instance *instance*

Selects a pre-defined list of location area codes (LACs) and allows/restricts the NRPCA procedure for calls within the listed area codes.

instance: Enter a list ID; an integer between 1 and 5.

Important Before using this keyword, ensure that the appropriate LAC information has been defined with the **location-area-list** command, also in this configuration mode.

failure-codes *code*

Enter an integer from 192 to 226 to identify the GTPP failure cause code (from 3GPP TS29.060, list below) to be included in the reject messages when NRPCA is restricted. If a failure cause code is not defined, the default value is 200 (service not supported).

- 192 - Non-existent
- 193 - Invalid message format
- 194 - IMSI not known
- 195 - MS is GPRS Detached
- 196 - MS is not GPRS Responding
- 197 - MS Refuses
- 198 - Version not supported
- 199 - No resources available
- 200 - Service not supported
- 201 - Mandatory IE incorrect
- 202 - Mandatory IE missing
- 203 - Optional IE incorrect
- 204 - System failure
- 205 - Roaming restriction
- 206 - P-TMSI Signature mismatch
- 207 - GPRS connection suspended
- 208 - Authentication failure
- 209 - User authentication failed
- 210 - Context not found
- 211 - All dynamic PDP addresses are occupied
- 212 - No memory is available
- 213 - Relocation failure

- 214 - Unknown mandatory extension header
- 215 - Semantic error in the TFT operation
- 216 - Syntactic error in the TFT operation
- 217 - Semantic errors in packet filter(s)
- 218 - Syntactic errors in packet filter(s)
- 219 - Missing or unknown APN
- 220 - Unknown PDP address or PDP type
- 221 - PDP context without TFT already activated
- 222 - APN access denied – no subscription
- 223 - APN Restriction type incompatibility with currently active PDP Contexts
- 224 - MS MBMS Capabilities Insufficient
- 225 - Invalid Correlation-ID
- 226 - MBMS Bearer Context Superseded

Usage Guidelines

Use this command to allow or restrict network-requested PDP context activation (NRPCA) based on access-type and location areas. NRPCA is used when there is downlink data at the GGSN for a subscriber, but there is no valid context for the already-established PDP address so the GGSN initiates an NRPCA procedure towards the SGSN.

This command can also be used to define the failure cause code that will be included in activation reject messages.

These commands can be repeated to define a unique set of NRPCA parameters for each access-type and each location area list.

The **T3385-timeout** and the **max-actv-retransmission** timers configure the retransmission timer and the number of retries for PDP context activation requests. Both of these timers are set in the SGSN service configuration mode.

The configuration for NRPCA can be viewed via the **show call-control-profile full name** *profile_name*. Statistics associated with NRPCA can be seen via the **show gmm-sm statistics** output and via the **show sgtpc statistics verbose** output.

Example

The following command changes the failure code for Reject messages from 200 (service not supported) to 205 (roaming restriction) for primary NRPCA for all GRPS access and all LACs:

```
network-initiated-pdp-activation primary access-type gprs all failure-code
 205
```

The following command enables network-initiated primary PDP context activation for UMTS calls from the LACs in location-area-list 1:

```
network-initiated-pdp-activation allow primary access-type umts
location-area-list instance 1
```

The following command restricts network-initiated primary PDP context activation for UMTS calls from the LACs in location-area-list 2:

```
network-initiated-pdp-activation restrict primary access-type umts
location-area-list instance 2
```

override-arp-with-ggsn-arp

Enables or disables the ability of the SGSN to override an Allocation/Retention Priority (ARP) value with one received from a GGSN. If there is no authorized Evolved ARP received from the GGSN, by default the SGSN continues to use the legacy ARP included in the Quality of Service (QoS) Profile IE.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-call-control-profile-`*`profile_name`*`)#`

Syntax Description

`[ remove ] override-arp-with-ggsn-arp`

remove

Adding the **remove** keyword to the command disables the override feature.

Usage Guidelines

Enabling this function on the SGSN will allow the ARP sent by the GGSN, in CPCR / UPCR / UPCQ, to be applicable as an overriding value.

Example

Use this command to configure the SGSN to negotiate the ARP to be used as an overriding value:

`override-arp-with-ggsn-arp`

paging-priority

This command is configured to support sending of paging-priority value in S1AP paging-request message to the eNodeB. This command supports both PS and CS traffic types.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

[remove] paging-priority cs *cs_value*

From release 20.0 onwards the paging priority command is updated to support PS traffic:

[remove] paging-priority { cs { *cs_value* **| map emlpp-priority** *emlpp_value* **s1-paging-priority** *priority_value* **} | ps map arp** *arp_value* **s1-paging-priority** *priority_value*

remove

The **remove** keyword deletes the configured value of paging-priority to be sent to eNodeB for CS /PSpaging.

cs

This keyword is used to configure the value of paging-priority to be sent to eNodeB for Circuit Switched (CS) traffic. The paging priority value can be configured or it can be used to map the received value to the paging-priority.

cs_value

The paging priority *value* is an integer in the range "0" up to "7". Configuring a value of "0" disables sending of paging priority value to eNodeB.

ps

This keyword is used to configure the value of paging-priority to be sent to eNodeB for Packet Switched (PS) traffic. The paging priority value can be configured or it can be used to map the received value to the paging-priority.

map

This keyword is used to map the received value to paging-priority.

emlpp-priority

This keyword is used to configure priority value of enhanced Multi Level Precedence and Pre-emption service

emlpp_value

The emlpp value is an integer in the range "0" up to "7".

s1-paging-priority

This keyword is used to configure the value of paging-priority to be sent to eNodeB.

priority_value

The priority_value is an integer in the range "0" up to "7". Configuring a value of "0" disables sending of paging priority value to eNodeB.

arp

This keyword is used to configure the value of allocation and retention priority.

arp_value

The arp_value is an integer in the range "1" up to "15".

Usage Guidelines

This command helps operator to map eMLPP Priority / ARP to s1 ap paging priority to be sent to eNB. By default, sending of paging priority-ie in S1AP paging-request message to eNodeBs is enabled. The priority value received from the MSC/VLR is relayed to the eNodeB. A lower value of paging priority indicates a higher priority. Older values of paging priority are overridden by configuring new values. By default no mapping is enabled. From release 20.0 onwards this command is enhanced to emlpp-priority to paging-priority. It is used to configure the priority value of enhanced Multi Level Precedence and Pre-emption service. This command is also used to configure the Allocation Retention priority value for PS paging.

Example

The following command is issued to disable sending of paging priority value to the eNodeB:

```
[local]asr5x00(config-call-control-profile-call1)# paging-priority cs 0
```

The following command enables sending of paging priority value to the eNodeB, a priority value of "5" is configured using this command:

```
[local]asr5000(config-call-control-profile-call1)# paging-priority cs 5
```

pcscf-restoration

This command enables HSS-based P-CSCF Restoration procedure.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
[ remove ] pcscf-restoration
```

remove

The remove keyword disables HSS-based P-CSCF Restoration in the MME.

pcscf-restoration

The pcscf-restoration command in the above configuration enables HSS-based P-CSCF restoration. When enabled, MME supports P-CSCF Restoration on the S6a interface towards HSS for IMS PDN.

Usage Guidelines

The command **pcscf-restoration** aids in successful establishment of MT VoLTE calls when the serving P-CSCF is unreachable. By default, the above configuration is disabled. To select the method for P-CSCF Restoration, use the **pcscf-restoration** keyword in **apn-type ims** command under APN Profile Configuration mode.

Example

The following configurations enables HSS-based P-CSCF Restoration:

```
pcscf-restoration
```

pdp-activate access-type

Configures the PDP context activation option based the type of access technology.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
pdp-activate access-type { grps | umts } { all | location-area-list
instance instance } failure-code failure_code
default pdp-activate access-type { grps | umts } { all | location-area-list
 instance instance } failure-code code
```

default

Resets the configuration to system default values for PDP context activation request.

{ grps | umts }

Specifies the access technology type for PDP context activation.

- **gprs**: Enables access type as GPRS.
- **umts**: Enables access type as UMTS.

all

Default: allow

Configures the system to allow the creation of all PDP context activation requests received from MS.

location-area-list instance *instance*

Specifies the location area instance for which to create a PDP context as an integer from 1 through 5. The value must be an already defined instance of a location area code (LAC) list created via the **location-area-list** command.

failure-code *code*

Specifies the failure code for PDP context activation as an integer from 8 through 112. Default: 8

Usage Guidelines

Use this command to configure this call control profile to allow GPRS/UMTS access through PDP context activation request from MS.

Example

The following command configures the system to create the PDP context for requests from MS for GPRS access with location area list instance *2* and failure-code *5*:

```
pdp-activate access-type gprs location-area-list 2 failure-code 5
```

pdp-activate allow

Configures the system to allow the PDP context activation based on the type of access technology.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-call-control-profile-`*`profile_name`*`)#`

Syntax Description

`[ no ] pdp-activate allow access-type { grps | umts } location-area-list instance` *`instance`*

no

Removes the configured permission to create PDP context on request of PDP context activation from MS for an access type.

access-type { grps | umts }

Specifies the access technology type for PDP context activation.

- **gprs**: Enables access type as GPRS.
- **umts**: Enables access type as UMTS.

location-area-list instance *instance*

Specifies the location area instance to create PDP context.

instance must be an integer from 1 through 5. The value must be an already defined instance of a location area code (LAC) list created via the **location-area-list** command.

Usage Guidelines

Use this command to configure this call control profile to allow GPRS/UMTS access through PDP context activation request from MS.

Example

The following command configures the system to allow the PDP context activation for GPRS access type with location area list instance *2*:

```
pdp-activate allow access-type gprs location-area-list instance 2
```

pdp-activate restrict

Configures the system to restrict the PDP context activation based on the type of access technology.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
[ no | remove ] { { access-type { gprs | umts } { all | location-area-list
 instance instance } } | { pdp-type { all | dual-ipv4v6 | ipv4 | ipv6 | ppp
 } { access-type { gprs | umts } { all | location-area-list instance
instance } } } | { secondary-activation access-type { gprs | umts } { all
| location-area-list instance instance  } } }
```

no | remove

Either of these prefixes removes the previously configured restriction on PDP context activation and returns the 'allow' default.

access-type { grps | umts }

Specifies the access technology type for which to restrict PDP context activation.

- **gprs**: Enables access type as GPRS.
- **umts**: Enables access type as UMTS.
- **all**: Configures the system to restrict all PDP context activation requests from the MS.

- **location-area-list instance** *instance*: Specifies the location area instance to restrict PDP context activation, where *list_id* must be an integer from 1 through 5. The value must be an already defined instance of a location area code (LAC) list created with the **location-area-list** command.

pdp-type

Sets the configuration to restrict PDP activation based on the requested PDP type.

To restrict more than one type of PDP, the command must be reissued for each PDP type.

- **all**: restricts activation of all types PDP.
- **dual-ipv4v6**: restricts activation when dual-IPv4v6 PDP contexts are requested.
- **ipv4**: restricts activation when IPv4 PDP contexts are requested.
- **ipv6**: restricts activation when IPv6 PDP contexts are requested.
- **ppp**: restricts activation when PPP PDP contexts are requested.

secondary-activation

Restricts the SGSN, based on the access-type, so that secondary PDP contexts are not created when receiving the PDP Context Activation Request from the MS.

Usage Guidelines

Use this command to configure this call control profile to restrict PDP context activation requests from MS.

Example

The following command configures the system to restrict the PDP context activation for request from 2G MS with location area list instance *2*:

```
pdp-activate restrict access-type gprs location-area-list instance 2
```

The following command configures the SGSN to restrict PDP context activation for requests from 3G MS if their PDP-type is IPv4. The second command restricts based on PDP-type IPv6.

```
pdp-activate restrict pdp-type ipv4 access-type umts all
pdp-activate restrict pdp-type ipv6 access-type umts location-area-list
instance 1
```

pdn-type-override

Configures the MME or the SGSN to override the requested packet data network (PDN) type based on the inbound roamer PLMN, and re-assigns the UE to an IPv4-only or IPv6-only PDN. This override can be applied based on the type of access technology.

Product

MME

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-call-control-profile-`*`profile_name`*`)#`

Syntax Description

```
pdn-type-override { ipv4-only | ipv4v6 { ipv4 | ipv6 } [ access-type {
eps | grps | umts } ] }
remove pdn-type-override [ access-type { eps | grps | umts } | ipv4-only
 ]
```

remove

Removes the configured PDN type override.

ipv4-only

Enables MME to allow only IPv4 addresses to a PDN connection.

The default behavior allows PDN to have IPv6 addresses when subscription allows it.

ipv4v6 { ipv4 | ipv6 }

Defines the PDN type (IPv4 or IPv6) to which UEs should be restricted.

access-type { eps | grps | umts }

Specifies the access technology type to which the override is applied.

- **eps**- enables PDN override for EPS access type.
- **gprs** - enables PDN override for GPRS access type.
- **umts** - enables PDN override for UMTS access type.

If this keyword is not included, then all three access types can have the PDN type overridden.

Usage Guidelines

Use this command to configure the call control profile to override the requested packet data network (PDN) type and re-assign the UE to a different PDN type. Optionally, it is possible to filter the override based on access technology.

Important This call control profile becomes valid only when it is associated with an operator policy using the **associate** command in the Operator Policy configuration mode.

Example

The following command configures the system to override the requested PDN type and assign a UE to an IPv4-only PDN if the UE's access technology is GPRS:

```
pdn-type-override ipv4v6 ipv4 access-type gprs
```

peer-mme

Configures a peer MME address. S4-SGSN operators can use this command if they wish to bypass DNS resolution to obtain the MME address.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

`peer-mme { mme-groupid` *`<lac val>`* **`mme-code`** *`<rac value>`* **`| tac`** *`tac`* **`} prefer { fallback-for-dns | local } address {`** *`<ipv4_address>`* **`|`** *`<ipv6_address>`* **`} interface { gn [ s3 ] | s3 [ gn ] }`**
`remove peer-mme { mme-groupid` *`<lac val>`* **`mme-code`** *`<rac value>`* **`| tac`** *`tac`* **`} address [`** *`<ipv4_address>`* **`|`** *`<ipv6_address>`* **`[ interface { gn [ s3 ] | s3 [ gn ] } ]`**

remove

Removes a specified peer MME from the call control profile. The **interface** keyword is optional. If it is not used, the entire interface will be deleted.

mme-groupid *<lac val>*

Specifies the location area code value of the peer MME. The MME group ID of the peer MME maps to the LAC value when GUTI is converted to P-TMSI.

<*lac val*> must be an integer from 1 to 65535.

mme-code *<rac value>*

Specifies the routing area code value of the peer MME. The MME code of the peer MME maps to the RAC value when GUTI is converted to P-TMSI.

<*rac value*> must be an integer from 0 to 255.

tac *tac*

Optional. Specifies the Tracking Area Code (TAC) of the target eNodeB that is used for UTRAN to E-UTRAN (SGSN to MME) SRNS relocation across the S3 interface. Valid entries are 1 to 65535. This setting applies only if SRNS relocation first has been configured via the **srns-inter** and/or **srns-intra** commands in *Call Control Profile Configuration Mode*.

prefer { fallback-for-dns | local }

Indicates whether to use a DNS query to obtain the address or to use a locally configured peer MME address:

- **fallback-for-dns** - Instructs the SGSN to perform a DNS query to get the IP address of the peer MME. If the DNS query fails, then the IP address configured with this command is used.
- **local** - Use the locally configured address for the MME address.

Important If the **prefer** command is used to change an existing peer-mme configuration (with the same LAC and RAC) from **fallback-for-dns** to **local**or from **local** to **fallback-for-dns**, the new setting overwrites the previously configured setting for all interfaces.

address { *ipv4_address* | *ipv6_address* }

Specifies the IP address of the peer MME. Currently, the IPv6 address option is not supported on the S4-SGSN.

ipv4 must be in standard dotted-decimal notation.

interface { gn [s3] | s3 [gn] }

Specifies the interface to use for communication between the SGSN and the peer MME:

- **gn**: Use the Gn interface between the S4-SGSN and the MME in the LTE network.
- **s3**: Use the S3 interface between the S4-SGSN and the MME in the LTE network. This is the default setting.

Usage Guidelines Use this command to instruct the S4-SGSN how to determine a peer MME address, via DNS or local configuration. For a local address, use this command to configure the peer MME address.

This command also sets the interface type to be used between the peer MME and the SGSN.

Example

The following command configures LAC/RAC *111/22* for the peer MME and instructs the SGSN to use the MME's locally configured IPv4 address of *1.1.1.1* and an S3 interface between the MME and the SGSN.

```
peer-mme mme-groupid 111 mme-code 22 prefer local address 1.1.1.1
interface s3
```

peer-msc

Enables/disables weight-based selection of a peer MSC during MSC lookup. By default, this functionality is disabled.

Product MME

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
peer-msc interface-type sv weight
remove peer-msc interface-type sv weight
```

remove

Deletes the weight-based selection for peer-MSC configuration if it has been enabled using this command and returns to the default of preference-based selection of a peer MSC.

Usage Guidelines

This command enables the operator to override the default behavior and define weight-based selection of a peer-MSC during MSC lookup to facilitate 'weight' based load balancing for the MME's Sv interface.

Example

Disable weight-based MSC selection when it has been configured:

```
remove peer-msc interface-type sv weight
```

peer-nri-length

Enables the SGSN to use NRI-FQDN-based DNS resolution for non-local RAIs when selection of the call control profile is based on the old-RAI and the PLMN Id of the RNC (for 3G subscribers) or BSC (for 2G subscribers) where the subscriber originally attached. The SGSN also supports RAI based query when NRI based query fails.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
peer-nri-length length [ rai-fqdn-fallback ] [nri-for-inter-pool-address]
remove peer-nri-length [ rai-fqdn-fallback ] [nri-for-inter-pool-address]
```

remove

Deletes the NRI length configuration for the non-local RAIs and the SGSN sends RAI-FQDN-based DNS resolution.

length

This defines the NRI length for the peer SGSN and enables use of NRI-FQDN-based DNS resolution for non-local RAIs. This variable allows for an integer from 1 to 10.

rai-fqdn-fallback

This keyword allows the operator to configure SGSN support for RAI based query when NRI based query fails. By default this keyword is disabled.

nri-for-inter-pool-address

This keyword enables NRI-only based static peer-sgsn address configuration for inter-pool. If this keyword is configured and if the NRI value derived from the PTMSI received in the RAU request matches the NRI value configured in the CLI **sgsn-address nri** *nri-value* **prefer local address ipv4** *addr* **interface** *name*, the static sgsn-address configured in the above CLI will be used to initiate the context request. Otherwise, a DNS query will be initiated to fetch the peer-sgsn address.

Usage Guidelines

Important

- This feature is supported only for 3G subscribers until Release 15.0.
- This feature is also supported for 2G subscribers from Release 16.0 onwards.

Important Fall back to RAI based query when NRI based query fails is not supported in the following scenarios:

- 2G Context Request and Identification Request are not supported.
- S4 support of this extension for all applicable scenarios are not supported.

The command enables the SGSN to perform DNS query with an NRI when RAU comes from an SGSN outside the pool. The SGSN uses NRI-FQDN-based DNS resolution for the non-local RAIs for 3G and 2G subscribers in place of RAI-FQDN-based DNS resolution.

This functionality is applicable in situations for either inter- or intra-PLMN when the SGSN has not chosen a local NRI value (configured with SGSN Service commands) other than local-pool-rai or nb-rai. This means the RAI (outside pool but intra-PLMN) NRI length configured here will be applicable even for intra-PLMN with differently configured NRI lengths (different from the local pool).

This functionality is not applicable to call control profiles with an associated MSIN range as ccprofile selection is not IMSI-based. When this feature is enabled, the selection of the ccprofile is based on the old-RAI and the PLMN Id (if configured) of the RNC (for 3G subscribers) or BSC (for 2G subscribers) where the subscriber originally attached.

When the CLI keyword **nri-for-inter-pool-address** is enabled the static SGSN address configured in the command **sgsn-address** is used for inter-pool Attaches/RAUs if the NRI value configured in the CLI **sgsn-address** matches the NRI value calculated from the PTMSI received in the attach/RAU message. If the keyword **nri-for-inter-pool-address** is not enabled, a DNS query is sent out to fetch the peer-sgsn address. This enhancement is applicable for both 2G and 3G scenarios. The primary advantage of this enhancement is that the DNS query for inter-pool 3G or 2G Attach/RAU scenarios is avoided.

Example

The following command is used to configure a peer-nri-length of *3*, with support for RAI based query when NRI based query fails:

```
peer-nri-length 3 rai-fqdn-fallback
```

plmn-protocol

Configures the protocol supported by the PLMN (Public Land Mobile Network).

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

`plmn-protocol plmnid mcc` *`mcc_num`* **`mnc`** *`mnc_num`* **`{ s5-protocol | s8-protocol } { gtp | pmip }`**
`remove plmn-protocol plmnid mcc` *`mcc_num`* **`mnc`** *`mnc_num`*

remove

Deletes the definition from the call control profile configuration.

plmn-id mcc *mcc_num* mnc *mnc_num*

Identifies the PLMN by MCC (mobile country code) and MNC (mobile network code).

mcc_num: Enter a 3-digit integer from 100-999.

mnc_num: Enter a 2- or 3-digit integer from 00 to 999.

s5-protocol | s8-protocol

Select which protocol – S5 or S8 – that controls the identified PLMN.

gtp | pmip

Select the protocol variant - GTP or PMIP - that controls functionality for the identified PLMN.

Usage Guidelines

Use this command to identify a particular PLMN and, at a higher level, its operational characteristics.

Example

The following command instructs the MME to use PLMN MCC423.MNC40.GPRS with PMIP under S8 Protocol:

```
plmn-protocol plmnid mcc 423 mnc 40 s8-protocol pmip
```

prefer subscription-interface

Selects the specified subscription interface (Gr or S6d) if both interface types are associated with a call-control-profile. Use of this command requires an S6d license. The SGSN also allows selection of S6d interface only if the UE is EPC capable. The keyword **epc-ue** supports the selection of HSS interface only for EPC capable subscribers.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

```
prefer subscription-interface { hlr | hss  [ epc-ue ] }
remove prefer subscription-interface
```

remove

Removes the preferred subscription-interface for the call control profile.

hlr

Selects the HLR Gr interface.

hss

Selects the HSS S6d interface.

epc-ue

Configure this keyword to select the HSS interface for EPC capable subscribers. For other subscribers the MAP interface will be selected. This keyword will be applicable only when both MAP and HSS interfaces are configured in the Call-control profile. If this keyword is not configured then SGSN follows existing logic for interface selection. The interface selection based on UE capability is done only at the time of Attach / new SGSN RAU / SRNS. Once the interface is selected, the subscriber remains in same interface till the UE moves out of the SGSN.

Usage Guidelines

Use of this command requires an S6d license.

The SGSN provides a mechanism to associate a MAP service with call control profile. It is possible that both MAP service and HSS peer service are associated with the call control profile. If the interface preference selected is "hlr", the MAP protocol is used to exchange messages with the HLR. If the interface preference selected is "hss", the Diameter-protocol is used to exchange messages with the HSS.

Example

The following command specifies that "hss" for S6d is selected as the subscription-interface:

```
prefer subscription-interface hss
```

psm

This command is used to configure UE Power Saving Mode parameters.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

`[remove] psm {ue-requested [dl-buf-duration [packet-count` *packet_value* **]]| t3324-timeout** *t3324_value* **t3412-extended-timeout** *t3412_ext_value* **[dl-buf-duration [packet-count** *packet_value* **]]}**

remove

The **remove** keyword deletes the existing power saving mode configuration.

ue-requested

Use this keyword when UE requested values for Active and Extended Periodic timers are to be accepted.

t3324-timeout *t3324_value*

Use this keyword to configure the T3324 active timer value.

t3324_value

The T3324 active timer is an integer value in the range 0 up to 11160 seconds.

t3412-extended-timeout *t3412_ext_value*

Use this keyword to configure the t3412 Extended timer value.

t3412_ext_value

The T3412 extended timer is an integer value in the range 0 up to 35712000 seconds.

dl-buf-duration

Use this keyword to Send Downlink Buffer Duration in DDN ACK when unable to page UE.

packet-count *packet_value*

Use this keyword to send 'DL Buffering Suggested Packet Count' in DDN ACK when unable to page UE.

packet_value

The *packet_value* is an integer value from 0 up to 65535.

Usage Guidelines

Use this CLI command to configure the T3324 active and T3412 extended timers. The CLI also provides an option to either accept UE requested values or HSS subscribed values or MME configured values for these timers. This command is used to configure either to send or not send the Downlink Buffer Duration in DDN Ack, the DDN Ack Optional IE "Downlink Suggested Packet Count". The CLI option **dl-buf-duration [packet-count** *packet_value* **]** is used to optionally configure either to send or not send the downlink buffer duration in DDN Ack, the DDN Ack Optional IE "Downlink Suggested Packet Count" can also be configured. If this option is not configured and not sent in subscription, MME does not send IE in DDN reject. If the **packet-count** value is not configured locally, the subscription value for **packet-count** is used. The subscription value can be "0", in this case the packet count IE will not be sent for that subscriber even if it is configured locally. If the T3324 active and T3412 extended timers are locally configured these values are always used. If the **psm** command is configured to use the UE requested values for Active and Extended Periodic timers the UE requested values are accepted, but in case if the UE does not request T3412 extended timer, then the value available in subscription data are used for Extended Periodic timer. If the values are not available in the subscription data then the values configured under the MME service are used .

As per latest version of 3GPP TS 24.008, the maximum value of T3412 extended timer can be "320*31" hours that is "35712000" seconds. Due to MME constraints on timer implementation the T3412 extended timer is restricted to 1050 hours that is "3780000" seconds. However, the nearest usable value of this timer as 3GPP TS 24.008 GPRS Timer 3 is 960 hours (320 * 3) that is 3456000 seconds.

Example

Use the following command to enable power saving mode and to accept UE requested values for T3324 and T3412 timers.

```
psm ue-requested
```

Use the following command enable UE power saving mode and provide operator desired values for T3324 and T3412 timers:

```
psm t3324-timeout 100 t3412-extended-timout 5000
```

Use the following command to enable PSM and accept UE requested values for T3324 and T3412 timers. This command also specifies the 'DL Buffering Suggested Packet Count' in DDN ACK when unable to page UE.

```
psm ue-requested dl-buf-duration packet-count 100
```

In the following example, PSM is enabled and values of T3324 and T3412 timers are specified along with configuring a packet count in DDN ACK:

```
psm t3324-timeout 1000 t3412-extended-timeout 5000 dl-buf-duration
packet-count 100
```

ptmsi-reallocate

Defines P-TMSI reallocation for Attach Requests, RAU Request, and Service Requests.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

ptmsi-reallocate { attach | frequency *frequency* **| interval** *interval* **| routing-area-update [update-type] | service-request [service-type] } [access-type { gprs | umts }]**
ptmsi-reallocate routing-area-update [access-type { gprs | umts } | frequency *frequency* **| update-type { combined-update | imsi-combined-update | periodic | ra-update } [access-type { gprs | umts } | frequency** *frequency* **]]**
ptmsi-reallocate service-request [frequency *frequency* **| service-type { data | page-response | signaling } [frequency** *frequency* **]]**
[no | remove] ptmsi-reallocate { attach | frequency | interval | routing-area-update [update-type { combined-update | imsi-combined-update | periodic | ra-update } [access-type { gprs | umts }]] | service-request [service-type { data | page-response | signaling }] } [access-type { gprs | umts }]

no

Disables the authentication procedures configured for the specified P-TMSI reallocation configuration in the call control profile.

remove

Deletes the defined authentication procedures for the specified P-TMSI reallocation configuration from the call control profile configuration file.

attach

Enables/disables P-TMSI reallocation for Attach with local P-TMSI.

Important IMSI or inter-SGSN Attach is not configurable and will always be reallocated.

access-type *type*

One of the following must be selected to reallocate on the basis of the type of network access:

- **gprs**
- **umts**

This keyword can be used in combination with other keywords to refine the reallocation configuration.

frequency *frequency*

Defines frequency of the reallocation based on the number of messages skipped. If the frequency is set for 1, then the SGSN skips 1 message and then reallocates on receipt of the 2nd (alternate) request message, essentially

reallocating the P-TMSI every time. If the frequency is set for 12, then the SGSN skips reallocation for 12 messages and reallocates on receipt of the 13th request message. This keyword can be used in combination with other keywords to refine the reallocation configuration.

frequency must be an integer from 1 to 50.

By default, frequency is not defined and, therefore, reallocation is done for every request message and none are skipped.

interval *minutes*

Enter an integer between 1 and 1440 to define the time interval (in minutes) for skipping the service/RAU/attach request message procedure.

routing-area-update [update-type]

Enables/disables P-TMSI reallocation for RAU (routing area update) with local P-TMSI. To refine the reallocation configuration, include one of the optional types of updates to limit reallocation:

- **combined-update**
- **imsi-combined-update**
- **periodic**
- **ra-update**

Important Inter-SGSN RAU will always be reallocated.

service-request [service-type]

Enables/disables P-TMSI reallocation for Service Requests. To refine the Service-Request reallocation configuration, include on of the optional service-types to limit the reallocation:

- **data**
- **page-response**
- **signaling**

Usage Guidelines

By default, reallocation is not enabled. Use this command to enable P-TMSI reallocation for Attach Requests, RAU Request, and Service Requests. Fine-tune the reallocation configuration according to frequency, interval, or access-type.

Example

The following command configures the SGSN to perform P-TMSI reallocation upon receiving 2G Attach Requests

```
ptmsi-reallocate attach access-type gprs
```

The following command configures the SGSN to disable all previously defined P-TMSI reallocations based on the combined criteria of interval and 3G requests:

```
no ptmsi-reallocate interval access-type umts
```

ptmsi-signature-reallocate

Enables P-TMSI signature reallocation during Attach/RAU procedures.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

```
ptmsi-signature-reallocate { attach | frequency frequency | interval interval
  | ptmsi-reallocation-command | routing-area-update [ update-type ] } [
 access-type { gprs | umts } | frequency frequency ]
ptmsi-signature-reallocate routing-area-update [ access-type { gprs |
umts } | frequency frequency | update-type { combined-update |
imsi-combined-update | periodic | ra-update } ] [ access-type { gprs |
umts } | frequency frequency ]
[ no | remove ] ptmsi-signature-reallocate { attach | frequency | interval
 | routing-area-update [ update-type { combined-update |
imsi-combined-update | periodic | ra-update } ] } [ access-type { gprs |
 umts } ]
```

no

Disables the authentication procedures configured for the specified P-TMSI signature reallocation configuration in the call control profile.

remove

Deletes the defined authentication procedures for the specified P-TMSI signature reallocation configuration from the call control profile configuration file.

attach

Enables/disables P-TMSI signature reallocation for Attach with local P-TMSI.

access-type *type*

One of the following must be selected to reallocate on the basis of the type of network access:

- **gprs**
- **umts**

This keyword can be used in combination with other keywords to refine the reallocation configuration.

frequency *frequency*

Defines 1-in-N selective reallocation. If the frequency is set for 12, then the SGSN skips reallocation for the first 11 messages and reallocates on receipt of the twelfth request message.

frequency must be an integer from 1 to 50.

This keyword can be used in combination with other keywords to refine the reallocation configuration.

interval *minutes*

Enter an integer between 1 and 1440 to define the time interval (in minutes) for skipping the service/RAU/attach request message procedure before performing a P-TMSI signature reallocation.

ptmsi-reallocation-command

Includes P-TMSI signature reallocation as a part of the P-TMSI reallocation configuration.

routing-area-update [update-type]

Enables/disables P-TMSI signature reallocation for RAU (routing area update) with local P-TMSI. To refine the reallocation configuration, include one of the optional types of updates to limit reallocation:

- **combined-update**
- **imsi-combined-update**
- **periodic**
- **ra-update**

Usage Guidelines

By default, P-TMSI signature reallocation is disabled. This command allows the operator to configure when the P-TMSI signature is reallocated.

Example

The following command configures the SGSN to reallocate the P-TMSI signature for every third UMTS attach procedure:

```
ptmsi-signature-reallocate attach frequency 3 access-type umts
```

The following command configures the SGSN to reallocate the P-TMSI signature for every seventh GPRS periodic RAU procedure:

```
ptmsi-signature-reallocate routing-area-update uupdate-type periodic
frequency 7 access-type gprs
```

The following command removes all configuration instances for reallocating the P-TMSI signature based on intervals and UMTS access:

```
remove ptmsi-signature-reallocate interval access-type umts
```

qos

Configures the quality of service (QoS) parameters to be applied.

Product

MME

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-call-control-profile-`*`profile_name`*`)#`

Syntax Description

```
qos { gn-gp | ue-ambr }
qos gn-gp { arp high-priority priority medium-priority priority | pre-emption
 { capability { may-trigger-pre-emption | shall-not-trigger-pre-emption
} | vulnerability { not-pre-emptable | pre-emptable }
qos ue-ambr { max-ul mbr_up max-dl mbr_dl | prefer-as-cap {
both-hss-and-local  minimum | local } }
qos ue-ambr { max-ul mbr_up max-dl mbr_dl | prefer-as-cap both-hss-and-local
 { local-when-subscription-not-available | minimum |
subscription-exceed-reject [ emm-cause-code [ eps-service-disallowed |
eps-service-not-allowed-in-this-plmn | no-suitable-cell-in-tracking-area
 | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area |
tracking-area-not-allowed ] ] }
remove qos { gn-gp | ue-ambr }
```

remove

Deletes the configuration from the call control profile.

gn-gp

Configures Gn-Gp pre-release 8 ARP and pre-emption parameters.

arp

Maps usage of ARP (allocation/retention policy) high-priority (H) and medium-priority (M):

- **high-priority** *priority*: Enter an integer from 1 to 13.
- **medium-priority** *priority*: Enter an integer from 2 to 14.

pre-emption

Defines the pre-emption/vulnerability criteria for PDP Contexts imported from SGSN on Gn/Gp:

- **capability**
  - **may-trigger-pre-emption**: PDP Contexts imported from Gn/Gp SGSN may preempt existing bearers.
  - **shall-not-trigger-pre-emption**: PDP Contexts imported from Gn/Gp SGSN shall not preempt existing bearers.

- **vulnerability**
  - **not-pre-emptable**: PDP Contexts imported from Gn/Gp SGSN are not vulnerable to pre-emption.
  - **pre-emptable**: PDP Contexts imported from Gn/Gp SGSN are vulnerable to pre-emption.

ue-ambr

This keyword enables the operator to configure either the aggregate maximum bit rate stored on the UE (UE AMBR) or select the preferred uplink and downlink QoS cap values.

Important The SGSN only supports the **ue-ambr** keyword beginning in Release 16.

Configures the aggregate maximum bit rate that will be stored on the UE (user equipment).

- **max-ul** *mbr_up*: Defines the maximum bit rate for uplink traffic.

  mbr_up: Enter a value from 1 to 1410065408 (StarOS release 16.1 and higher), or 0 to 1410065408 (Kbps).

  In StarOS 21.8 and later releases: *mbr_up* must be an integer from 0 to 4000000000000 (4 Tbps).

- **max-dl** *mbr_down*: Defines the maximum bit rate for downlink traffic.

  mbr_down: Enter a value from 1 to 1410065408 (StarOS release 16.1 and higher), or 0 to 1410065408 (Kbps).

  In StarOS 21.8 and later releases: *mbr_down* must be an integer from 0 to 4000000000000 (4 Tbps).

prefer-as-cap both-hss-and-local { local-when-subscription-not-available | minimum | subscription-exceed-reject [emm-cause-code [eps-service-disallowed | 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]] }

This set of options is only available on the MME.

Specifies the QoS cap value to use.

- **local-when-subscription-not-available**: Use the locally configured values if the Home Subscriber Server (HSS) does not provide QoS bit rate values.
- **minimum**: Use the lower of either the locally configured QoS bit rate or the HSS-provided QoS bit rate. This will override the HSS provided values if it is greater than the locally configured values, or if the HSS does not provide any values.
- **subscription-exceed-reject**: If the requested QoS bit rate exceeds the locally configured value, reject the PDN connection.
- **emm-cause-code**: Specifies the EPS Mobility Management (EMM) cause code to return when the PDN connection is rejected.
  - **eps-service-disallowed** - Default
  - **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**

prefer-as-cap { both-hss-and-local minimum | local }

This set of options is only available on the SGSN.

Specifies the QoS cap value to use:

- **both-hss-and-local minimum** Use the lower of either the locally configured QoS bit rate or the Home Subscriber Server (HSS)-provided QoS bit rate.
- **local** Use the locally configured QoS bit rate.

Usage Guidelines

Use this command to configure the QoS parameters for the call control profile for either the MME or the SGSN.

On an S4-SGSN, this command ensures proper QoS parameter mapping between the S4-SGSN and EPC UEs, SGWs and PGWs:

- Map EPC ARP parameters to pre-release 8 ARP (Gn/Gp ARP) used during S4-SGSN-to-Gn SGSN call handovers.
- Map ARP parameters received in a GPRS subscription from the HLR to EPC ARP parameters if:
  - The S4 interface is selected for an EPC capable UE, and
  - The UE has only a GPRS subscription (but no EPS subscription) in the HLR / HSS.

Example

Configure the Gn/Gp interface ARP priority values:

```
qos gn-gp arp high-priority 2 medium-priority 3
```

rau-inter

Defines acceptable parameters for inter-SGSN routing area updates.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

rau-inter { accept use-auth-vector | access-type gprs { all | location-area-list instance *instance_id* **| routing-area-list instance** *instance_id* **} { failure-code** *fail_code* **| user-device-release { before-r99 | r99-or-later } failure-code** *fail_code* **} } | allow accept access-type gprs**

location-area-list instance *instance_id* **| avoid-s12-direct-tunnel | ctxt-xfer-failure | exclude-uteid-in-mbr | ignore-peer-context-id | peer-sgsn-addr-resolution-failure failure-code** *fail_code* **| restrict access-type { { gprs | umts } { all | location-area-list instance** *instance_id* **| routing-area-list instance** *instance_id* **} }**
default rau-inter (accept use-auth-vector | access-type { { gprs | umts } { all | location-area-list instance *instance_id* **| routing-area-list instance** *instance_id* **} user-device-release { before-r99 | r99-or-later } failure-code** *fail_code* **} } | avoid-s12-direct-tunnel | failure-code** *fail_code* **| ignore-peer-context-id | peer-sgsn-addr-resolution-failure failure-code** *fail_code* **}**
no rau-inter (accept use-auth-vector | allow access-type { gprs | umts } location-area-list instance *instance_id* **| routing-area-list instance** *instance_id* **| ignore-peer-context-id | restrict access-type { gprs | umts } { all | location-area-list instance** *instance_id* **| routing-area-list instance** *instance_id* **} }**
remove rau-inter { avoid-s12-direct-tunnel | exclude-uteid-in-mbr | ctxt-xfer-failure}

no

Including **no** as part of the command structure disables the values already configured for parameters specified in the command.

default

Resets the configuration of specified parameters to system default values.

remove

remove can only be used with the **avoid-s12-direct-tunnel** keyword to erase a configuration instructing the SGSN to avoid establishment of a direct tunnel for S12 interfaces.

accept use-auth-vector

Sets the SGSN to accept using the authorization vector.

allow access-type

Including this keyword with one of the following options, configures the SGSN to allow MS/UE with the identified access-type extension to be part of the intra-RAU procedure.

- **gprs** - General Packet Radio Service
- **umts** - Universal Mobile Telecommunications System

avoid-s12-direct-tunnel

Enables the operator to modify the Call-Control profile default configuration and instructs the SGSN to avoid establishment of a direct tunnel for S12 interfaces.

This keyword is only supported for configuration of S12 interfaces.

ctxt-xfer-failure *fail_code*

Configure or removes a GMM failure cause code to be sent in a RAU Reject to the UE due to context transfer failures.

fail_code For acceptable options, refer to the failure-codes listed below.

remove filter works with this keyword to erase the context transfer failure cause code definition.

exclude-uteid-in-mbr

By default, the SGSN sends user plane fully qualified tunnel end-point identifier (UTEID) in the Modify Bearer Reqeust (MBR). If RABs are not yet established, this keyword disables or enables the sending of the UTEID in the MBR during a new SGSN RAU over S16/S3. This keyword is in compliance with 3GPP TS 23.401 v11.8.0.

ignore-peer-context-id

Sets the SGSN to ignore the peer's context-ID and replace with PDP context-ID information based on the HLR subscription.

peer-sgsn-addr-resolution-failure *fail_code*

Configure or remove a GMM failure cause code to be sent in a RAU Reject to the UE due to peer address resolution failures at the SGSN.

fail_code Enter either 9 (MSID cannot be derived by the network) or 10 (Implicitly detached) to identify the GMM failure cause code.

remove filter works with this keyword to erase the failure code definition.

restrict access-type

Including this keyword-set with one of the following options, configures the SGSN to restrict MS/UE with the identified access-type extension from the inter-RAU procedure.

- **gprs** - General Packet Radio Service
- **umts** - Universal Mobile Telecommunications System

all

all - adding this option to the keyword determines that the failure cause code will be applicable to all location areas.

location-area-list instance *instance_id*

instance_id must be an integer between 1 and 5. The value must be an already defined instance of a location area code (LAC) list created with the **location-area-list** command.

routing-area-list instance *instance_id*

Instructs the SGSN to apply the command action to a specific routing area list. Routing area lists should already have been created with the **routing-area-list** command.

instance_id must be an integer from 1 to 5.

failure-code *fail-code*

Specify a GSM Mobility Management (GMM) failure cause code to identify the reason an inter SGSN RAU does not occur. This GMM cause code will be sent in the reject message to the MS.

fail-code must be an integer from 2 to 111. Refer to the GMM failure cause codes listed below (from section 10.5.5.14 of the 3GPP TS 124.008 v7.2.0 R7):

- 2 - IMSI unknown in HLR
- 3 - Illegal MS
- 6 - Illegal ME
- 7 - GPRS services not allowed
- 8 - GPRS services and non-GPRS services not allowed
- 9 - MSID cannot be derived by the network
- 10 - Implicitly detached
- 11 - PLMN not allowed
- 12 - Location Area not allowed
- 13 - Roaming not allowed in this location area
- 14 - GPRS services not allowed in this PLMN
- 15 - No Suitable Cells In Location Area
- 16 -MSC temporarily not reachable
- 17 - Network failure
- 20 - MAC failure
- 21 - Synch failure
- 22 - Congestion
- 23 - GSM authentication unacceptable
- 40 - No PDP context activated
- 48 to 63 - retry upon entry into a new cell
- 95 - Semantically incorrect message
- 96 - Invalid mandatory information
- 97 - Message type non-existent or not implemented
- 98 - Message type not compatible with state
- 99 - Information element non-existent or not implemented
- 100 - Conditional IE error
- 101 - Message not compatible with the protocol state
- 111 - Protocol error, unspecified

user-device-release { before-r99 | r99-or-later } failure-code *code*

Default: Disabled

Enables the SGSN to reject an Inter-RAU procedure based on the detected 3GPP release version of the MS equipment and selectively send a failure cause code in the reject message. The SGSN uses the following procedure to implement this configuration:

1. When Attach Request is received, the SGSN checks the subscriber's IMSI and current location information.
2. Based on the IMSI, an operator policy and call control profile is found that relates to this Attach Request.
3. call control profile is checked for access limitations.
4. Attach Request is checked to see if the revision indicator bit is set
   - if not, then the configured common failure code for reject is sent;
   - if set, then the 3GPP release level is verified and action is taken based on the configuration of this parameter

One of the following options must be selected and completed:

- **before-r99**: Indicates the MS would be a 3GPP release prior to R99 and an appropriate failure code should be defined.

  failure-code *code*: Enter an integer from 2 to 111.

- **r99-or-later**: Indicates the MS would be a 3GPP Release 99 or later and an appropriate failure code should be defined.

  failure-code *code*: Enter an integer from 2 to 111.

Usage Guidelines Use this command to configure the restrictions and function of the inter-RAU procedure.

Example

Configure default inter-RAU settings for Edge calls from subscribers on location-area-list no. *1*:

```
default rau-inter allow access-type gprs location-area-list instance 1
```

rau-inter-plmn

Enables or disables restriction of all Routing Area Updates (RAUs) occurring between different PLMNs.

Product SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

rau-inter-plmn access-type { all | location-area-list instance *instance* **} { failure-code** *fail_code* **| user-device-release { before-r99 } failure-code** *fail_code* **| r99-or-later } { failure-code** *fail_code* **} }**
default rau-inter-plmn access-type { all | location-area-list instance *instance*} **user-device-release { before-r99 failure-code | r99-or-later failure-code }**
[no] rau-inter-plmn { restrict | allow } access-type { gprs | umts } { all | location-area-list instance instance }
[no] rau-inter-plmn { allow access-type | restrict access-type } { [all] failure-code *fail_code* **| location-area-list instance** *instance* **}**
default rau-inter { allow access-type | restrict access-type } { [all] failure-code *fail_code* **| location-area-list instance** *instance* **} }**

no

Including "no" as part of the command structure disables the values already configured for parameters specified in the command.

default

Resets the configuration of specified parameters to system default values.

allow access-type

Including this keyword-set with one of the following options, configures the SGSN to allow MS/UE with the identified access-type extension to be part of the intra-RAU procedure.

- **gprs** - General Packet Radio Service
- **umts** - Universal Mobile Telecommunications System

restrict access-type

Including this keyword-set with one of the following options, configures the SGSN to restrict MS/UE with the identified access-type extension from the inter-RAU procedure.

- **gprs** - General Packet Radio Service
- **umts** - Universal Mobile Telecommunications System

all

all - adding this option to the keyword determines that the failure cause code will be applicable to all location areas.

location-area-list instance *instance*

list_id must be an integer between 1 and 5. The value must be an already defined instance of a LAC list created with the **location-area-list** command.

failure-code *fail-code*

Specify a GSM Mobility Management (GMM) failure cause code to identify the reason an inter SGSN RAU does not occur. This GMM cause code will be sent in the reject message to the MS.

fail-code must be an integer from 2 to 111. Refer to the GMM failure cause codes listed below (from section 10.5.5.14 of the 3GPP TS 124.008 v7.2.0 R7):

- 2 - IMSI unknown in HLR
- 3 - Illegal MS
- 6 - Illegal ME
- 7 - GPRS services not allowed
- 8 - GPRS services and non-GPRS services not allowed
- 9 - MSID cannot be derived by the network
- 10 - Implicitly detached
- 11 - PLMN not allowed
- 12 - Location Area not allowed
- 13 - Roaming not allowed in this location area
- 14 - GPRS services not allowed in this PLMN
- 15 - No Suitable Cells In Location Area
- 16 -MSC temporarily not reachable
- 17 - Network failure
- 20 - MAC failure
- 21 - Synch failure
- 22 - Congestion
- 23 - GSM authentication unacceptable
- 40 - No PDP context activated
- 48 to 63 - retry upon entry into a new cell
- 95 - Semantically incorrect message
- 96 - Invalid mandatory information
- 97 - Message type non-existent or not implemented
- 98 - Message type not compatible with state
- 99 - Information element non-existent or not implemented
- 100 - Conditional IE error
- 101 - Message not compatible with the protocol state
- 111 - Protocol error, unspecified

user-device-release { before-r99 | r99-or-later } failure-code *code*

Default: Disabled

Enables the SGSN to reject an Inter-RAU procedure based on the detected 3GPP release version of the MS equipment and selectively send a failure cause code in the reject message. The SGSN uses the following procedure to implement this configuration:

1. When Attach Request is received, the SGSN checks the subscriber's IMSI and current location information.
2. Based on the IMSI, an operator policy and call control profile are found that relate to this Attach Request.
3. The call control profile is checked for access limitations.
4. Attach Request is checked to see if the revision indicator bit is set
   - if not, then the configured common failure code for reject is sent;
   - if set, then the 3GPP release level is verified and action is taken based on the configuration of this parameter

One of the following options must be selected and completed:

- **before-r99**: Indicates the MS would be a 3GPP release prior to R99 and an appropriate failure code should be defined.

  failure-code *code*: Enter an integer from 2 to 111.

- **r99-or-later**: Indicates the MS would be a 3GPP Release 99 or later and an appropriate failure code should be defined.

  failure-code *code*: Enter an integer from 2 to 111.

Usage Guidelines

Use this command to configure the restrictions and function of the inter-RAU procedure occurring across RNCs or BSSs where the PLMN changes. For example:

- inter-IuPS RAU, where the two IuPSs have different PLMNs
- inter-GPRS RAU, where the two GPRSs have different PLMNs
- inter-RAT RAU (2G > 3G), where the IuPS/GPRS services have different PLMNs
- inter-RAT-RAU (3G > 2G), where the IuPS/GPRS services have different PLMNs

Example

```
default rau-inter allow access-type gprs location-area-list instance 1
```

rau-intra

Defines an acceptable procedure for intra-SGSN Routing Area Updates (RAUs).

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
rau-intra access-type { all | location-area-list instance instance_id |
routing-area-list instance instance_id } { failure-code fail_code |
user-device-release { before-r99 } { failure-code fail_code | r99-or-later
 } { failure-code fail_code } }
default rau-intra access-type { all | location-area-list instance instance_id
 | routing-area-list instance instance_id} user-device-release { before-r99
 failure-code | r99-or-later failure-code }
rau-intra { allow access-type | restrict access-type } { [ all ]
failure-code fail_code | location-area-list instance instance_id |
routing-area-list instance instance_id } }
no rau-intra { allow access-type | restrict access-type } { [ all ]
failure-code fail_code | location-area-list instance instance_id |
routing-area-list instance instance_id }
default rau-intra { allow access-type | restrict access-type } { [ all ]
 failure-code fail_code | location-area-list instance instance_id  |
routing-area-list instance instance_id} }
```

no

Including "no" as part of the command structure disables the values already configured for parameters specified in the command.

default

Resets the configuration of specified parameters to system default values.

allow access-type

Including this keyword-set with one of the following options, configures the SGSN to allow an MS/UE with the identified access-type extension to be part of the intra-RAU procedure.

- **gprs** - General Packet Radio Service
- **umts** - Universal Mobile Telecommunications System

restrict access-type

Including this keyword-set with one of the following options, configures the SGSN to restrict an MS/UE with the identified access-type extension from the intra-RAU procedure.

- **gprs** - General Packet Radio Service
- **umts** - Universal Mobile Telecommunications System

all

all - adding this option to the keyword determines that the failure cause code will be applicable to all location areas.

location-area-list instance *instance_id*

instance_id must be an integer from 1 to 5. The value must be an already defined instance of a location area code (LAC) list created via the **location-area-list** command.

routing-area-list instance *instance_id*

Instructs the SGSN to apply the command action to a specific routing area list. Routing area lists should already have been created with the **routing-area-list** command.

instance_id must be an integer from 1 to 5.

failure-code *fail-code*

Specify a GSM Mobility Management (GMM) failure cause code to identify the reason an inter SGSN RAU does not occur. This GMM cause code will be sent in the reject message to the MS.

fail-code must be an integer from 2 to 111. Refer to the GMM failure cause codes listed below (from section 10.5.5.14 of the 3GPP TS 124.008 v7.2.0 R7):

- 2 - IMSI unknown in HLR
- 3 - Illegal MS
- 6 - Illegal ME
- 7 - GPRS services not allowed
- 8 - GPRS services and non-GPRS services not allowed
- 9 - MSID cannot be derived by the network
- 10 - Implicitly detached
- 11 - PLMN not allowed
- 12 - Location Area not allowed
- 13 - Roaming not allowed in this location area
- 14 - GPRS services not allowed in this PLMN
- 15 - No Suitable Cells In Location Area
- 16 -MSC temporarily not reachable
- 17 - Network failure
- 20 - MAC failure
- 21 - Synch failure
- 22 - Congestion
- 23 - GSM authentication unacceptable
- 40 - No PDP context activated
- 48 to 63 - retry upon entry into a new cell
- 95 - Semantically incorrect message

- 96 - Invalid mandatory information
- 97 - Message type non-existent or not implemented
- 98 - Message type not compatible with state
- 99 - Information element non-existent or not implemented
- 100 - Conditional IE error
- 101 - Message not compatible with the protocol state
- 111 - Protocol error, unspecified

user-device-release { before-r99 | r99-or-later } failure-code *code*

Default: Disabled

Enables the SGSN to reject an Intra-RAU procedure based on the detected 3GPP release version of the MS equipment and selectively send a failure cause code in the reject message. The SGSN uses the following procedure to implement this configuration:

1. When Attach Request is received, the SGSN checks the subscriber's IMSI and current location information.
2. Based on the IMSI, an operator policy and call control profile are found that relate to this Attach Request.
3. Call control profile is checked for access limitations.
4. Attach Request is checked to see if the revision indicator bit is set
   - if not, then the configured common failure code for reject is sent;
   - if set, then the 3GPP release level is verified and action is taken based on the configuration of this parameter

One of the following options must be selected and completed:

- **before-r99**: Indicates the MS would be a 3GPP release prior to R99 and an appropriate failure code should be defined.

  failure-code *code*: Enter an integer from 2 to 111.

- **r99-or-later**: Indicates the MS would be a 3GPP Release 99 or later and an appropriate failure code should be defined.

  failure-code *code*: Enter an integer from 2 to 111.

Usage Guidelines

Use this command to configure the restrictions and function of the intra-RAU procedure.

Example

```
default rau-intra allow access-type gprs location-area-list instance 1
```

re-authenticate

Enables or disables the re-authentication feature. This command is available in releases 8.1 and higher.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-call-control-profile-`*`profile_name`*`)#`

Syntax Description

`re-authenticate [ access-type { gprs | umts } ]`
`remove re-authenticate`

remove

Including this keyword with the command disables the feature. The feature is disabled by default.

access-type

Defines the type of access to be allowed or restricted.

- **gprs**
- **umts**

If this keyword is not included, then both access types are allowed by default.

Usage Guidelines

Use this command to enable or disable the re-authentication feature, which instructs the SGSN to retry authentication with another RAND in situations where failure of the first authentication has occurred. To address the introduction of new SIM cards, for security reasons a systematic "last chance" authentication retry with a fresh Authentication Vector is needed, particularly in cases where there is an SRES mismatch at authentication.

Example

`re-authenticate`

regional-subscription-restriction

Allows the operator to define the cause code for subscriber rejection when it is due to regional subscription information failure.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

`[ remove ] regional-subscription-restriction [ failure-code` *`code`* `| user-device-release { before-r99 failure-code` *`code`* `| r99-or-later failure-code` *`code`* `} ]`

remove

This keyword causes the configuration to be deleted from the call control profile configuration.

failure-code *cause_code*

cause_code: Enter an integer from 2 to 111; default code is 13 (roaming not allowed in this location area [LA]).

Refer to the GMM failure cause codes listed below (from section 10.5.5.14 of the 3GPP TS 124.008 v7.2.0 R7):

- 2 - IMSI unknown in HLR
- 3 - Illegal MS
- 6 - Illegal ME
- 7 - GPRS services not allowed
- 8 - GPRS services and non-GPRS services not allowed
- 9 - MSID cannot be derived by the network
- 10 - Implicitly detached
- 11 - PLMN not allowed
- 12 - Location Area not allowed
- 13 - Roaming not allowed in this location area
- 14 - GPRS services not allowed in this PLMN
- 15 - No Suitable Cells In Location Area
- 16 - MSC temporarily not reachable
- 17 - Network failure
- 20 - MAC failure
- 21 - Synch failure
- 22 - Congestion
- 23 - GSM authentication unacceptable

- 40 - No PDP context activated
- 48 to 63 - retry upon entry into a new cell
- 95 - Semantically incorrect message
- 96 - Invalid mandatory information
- 97 - Message type non-existent or not implemented
- 98 - Message type not compatible with state
- 99 - Information element non-existent or not implemented
- 100 - Conditional IE error
- 101 - Message not compatible with the protocol state
- 111 - Protocol error, unspecified

user-device-release { before-r99 | r99-or-later } failure-code *code*

Enables the SGSN to assign a reject cause code based on the detected 3GPP release version of the MS equipment.

One of the following options must be selected and completed:

- **before-r99**: Indicates the MS would be a 3GPP release prior to R99 and an appropriate failure code should be defined.

  failure-code *code*: Enter an integer from 2 to 111. Refer to the list above.

- **r99-or-later**: Indicates the MS would be a 3GPP Release 99 or later and an appropriate failure code should be defined.

  failure-code *code*: Enter an integer from 2 to 111. Refer to the list above.

Usage Guidelines Use this command to define GMM reject cause codes when rejection is due to regional subscription information failure.

Example

The following command sets a location area rejection message, code 12 for regional restriction rejections:

```
regional-subscription-restriction failure-code 12
```

release-access-bearer

Enables sending of Release Access Bearer and configures the S4-SGSN to send Release Access Bearer Request on Iu-Release for non-DT and non-ISR subscribers in 3G and on Ready-to-Standby or Radio-Status-Bad for non-ISR subscribers in 2G.

Product

Important We recommend that Release Access Bearer be enabled (with this command) prior to enabling Subscriber Overcharing Protection for S4-SGSN. This will ensure that the S4-SGSN sends Release Access Bearer with the ARRL bit set if LORC (loss of radio coverage) is detected.

SGSN.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-call-control-profile-`*`profile_name`*`)#`

Syntax Description

release-access-bearer [on-iu-release | on-ready-to-standby]
remove release-access-bearer [on-iu-release | on-ready-to-standby]

remove

When included with the command, **remove** disables sending Release Access Bearer in either the selected (with optional keyword) 2G or 3G environment or both environments (with no keyword included).

on-iu-release

This optional keyword instructs the SGSN to send Release Access Bearer upon Iu-Release in a 3G network so that Release Access Bearer will be initiated for non-ISR and non-DT subscribers upon Iu-Release. For ISR and DT subscribers, Release Access Bearer will be initiated unconditionally.

on-ready-to-standby

This optional keyword instructs the SGSN to send Release Access Bearer on Ready-to-Standby transition in a 2G network so that Release Access Bearer will be initiated for non-ISR subscribers on Ready-to-Standby transition. For ISR subscribers, Release Access Bearer will be initiated unconditionally.

Usage Guidelines

If no optional keywords are included with the **release-access-bearer** command, then the S4-SGSN applies Release Access Bearer for both 2G and 3G networks.

By default, Release Access Bearer initiation on Iu-Release or Ready-to-Standby transition is not enabled. When disabled or prior to being enabled, either/both remove release-access-bearer on-iu-release or/and remove release-access-bearer on-ready-to-standby will display in the output generated by the **show configuration [verbose]** command.

This command, in compliance with 3GPP TS 23.060 v11.7.0, provides the operator with the option to have the S4-SGSN send Release Access Bearer Request to the S-GW to remove the downlink user plane on the S4 interface for non-DT and non-ISR scenarios.

In accordance with 3GPP TS 23.401 v11.8.0, if the SGSN and the S-GW are configured to release S4 U-Plane when the EPS bearer contexts associated with the released RABs are to be preserved, then the SGSN should not send SGSN address and TEID for U-Plane in the Modify Bearer Request (MBR). The operator can now

use the **rau-inter exclude-uteid-in-mbr** command (under Call-Control Profile configuration mode) to configure the SGSN not to send the UTEID in the MBR.

Example

To enable release access bearer in both 2G and 3G networks, use a command similar to the following:

```
release-access-bearer
```

To disable release access bearer in 3G networks, use a command similar to the following:

```
remove release-access-bearer on-iu-release
```

reporting-action

This command enables event logging in the MME.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
[ remove ] reporting-action mme-event-record
```

remove

This command disables the reporting action configuration.

mme-event-record

Provides event logs for MME procedures in the form of event records using CDRMOD.

Usage Guidelines

The **reporting-action** command is configured in the Call Control Profile Configuration mode. This command enables procedure reports (Event Data Records). However, the Event Data Records (EDRs) are configured in the Context Configuration mode under the **edr-module active-charging-service** command. Along with EDR configuration, the file parmeters can also be confgured in the Context Configuration mode under the **session-event-module** command. Finally, to enable the Event Logging, the EDR configuration profile must be associated to an MME-Service available under Operator Policy and LTE Policy configuration.

Example

The following configuration enables Event Logging in the MME:

```
reporting-action mme-event-record
```

reuse-authentication-triplets

Creates a configuration entry to enable or disable the reuse of authentication triplets in the event of a failure.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-call-control-profile-`*`profile_name`*`)#`

Syntax Description

`[ no | remove ] reuse-authentication-triplets no-limit`

no

Disables this configuration entry and disables reuse of authentication triplets.

remove

This keyword causes the reuse configuration to be deleted from the call control profile configuration.

This is the default behavior. Triplets are reused.

no-limit

This keyword enables reuse triplets as needed.

Usage Guidelines

Use this command to enable reuse of authentication triplets.

Example

`reuse-authentication-triplets no limit`

rfsp-override

Configures RAT frequency selection priority override parameters for this call control profile.

Product

MME

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

rfsp-override { default *value* **| eutran-ho-restricted** *value* **| ue-val** *value* **new-val** *value* **+ }**
remove rfsp-override { default | eutran-ho-restricted | ue-val *value* **}**

remove

Deletes the rfsp-override configuration from the call control profile.

default

Restores the default value assigned.

eutran-ho-restricted *value*

This keyword is used to configure the value for RAT frequency selection priority when Handover to EUTRAN is restricted. This value overrides the RFSP ID value sent by the HLR/HSS in an EPS subscription.

value: Enter an integer from 1 to 256.

ue-val *value*

Assign the UE value for the RAT frequency selection priority.

value: Enter an integer from 1 to 256.

new-val *value*

Assign a new RFSP Index value.

value: Enter an integer from 1 to 256.

Multiple UE value/new value combinations can be configured in a single command.

Usage Guidelines

Use this command to configure the RAT frequency selection priority override parameter.

Multiple UE value/new value combinations can be configured.

Example

The following command resets the specified RFSP Index value (1) to its default value, thereby removing the RFSP Index override value previously configured:

```
rfsp-override default 1
```

rfsp-override ue-settings

Configures the override of the RAT Frequency Selection Priority (RFSP) of matching subscribers.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

```
[ remove ] rfsp-override ue-settings { data-centric
ue-voice-domain-preference { cs-voice-only |
cs-voice-preferred-ims-ps-voice-secondary | ims-ps-voice-only |
ims-ps-voice-preferred-cs-voice-secondary } | voice-centric
ue-voice-domain-preference { cs-voice-only |
cs-voice-preferred-ims-ps-voice-secondary | ims-ps-voice-only |
ims-ps-voice-preferred-cs-voice-secondary } new-val value }
```

remove

Deletes the rfsp-override configuration from the call control profile.

ue-settings *value*

Assign the UE value for the RAT frequency selection priority.

data-centric ue-voice-domain-preference

Assign the UE value for the RAT frequency selection priority for data-centric calls.

- **cs-voice-only**: Circuit switched voice only.
- **cs-voice-preferred-ims-ps-voice-secondary**: Circuit switched voice preferred.
- **ims-ps-voice-only**: IMS Packet switched voice only.
- **ims-ps-voice-preferred-cs-voice-secondary**: IMS Packet switched voice preferred.

voice-centric ue-voice-domain-preference

Assign the UE value for the RAT frequency selection priority for voice-centric calls.

- **cs-voice-only**: Circuit switched voice only.
- **cs-voice-preferred-ims-ps-voice-secondary**: Circuit switched voice preferred.
- **ims-ps-voice-only**: IMS Packet switched voice only.
- **ims-ps-voice-preferred-cs-voice-secondary**: IMS Packet switched voice preferred.

new-val *value*

Assign a new RFSP Index value.

value: Enter an integer from 1 to 256.

Multiple UE value/new value combinations can be configured in a single command.

Usage Guidelines

Use this command to assign an RFSP Index for a UE based on the following factors:

- Operator policy (where IMSI range or PLMN can influence the selected RFSP)
- UE usage setting (voice centric, data centric)

- Voice domain preference (CS voice only, CS voice preferred, IMS PS voice preferred, IMS PS voice only).

To support Radio Resource Management (RRM) in E-UTRAN, the MME provides the parameter RFSP Index to an eNodeB across S1. The RFSP Index is used by the eNodeB to apply specific RRM strategies.

The MME receives the subscribed RFSP Index from the HSS, then overrides the RFSP Index for the UE based on the settings defined in this command.

Multiple UE value/new value combinations can be configured.

Example

The following command overrides the RFSP Index value for voice-centric circuit switched calls to an RFSP Index of 10:

```
rfsp-override ue-setting voice-centric voice-domain-pref cs-voice_only
new-val 10
```

routing-area-list

Defines the routing area list to allow or restrict services in the specified routing areas identified by routing area code (RAC).

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
routing-area-list instance instance_id lac lac rac rac
no routing-area-list instance instance_id
```

no

Deletes the specified routing area list configurations.

instance *instance_id*

Specifies an identification for the specific routing area list.

instance must be an integer between 1 and 5. Instance number will be valid only if the area code is configured for this instance.

lac *lac*

This keyword defines the location area codes (LACs) to be used by this call control profile as a determining factor in the handling of incoming calls.

lac must be an integer from 1 to 65535.

rac *rac*

This keyword defines the routing area codes (RACs) to be used by this call control profile as a determining factor in the handling of incoming calls.

rac must be an integer from 0 to 255.

Usage Guidelines

Use the command multiple times to configure multiple RAC lists or to modify the list.

Example

The following command creates a routing area list:

```
routing-area-list instance 1 lac 514 rac 10
```

s1-reset

Configures the behavior of user equipment (UE) on S1-reset.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
s1-reset { detach-ue | idle-mode-entry }
default s1-reset
```

default

Reset the profile configuration to the system default of **idle-mode-entry**.

detach-ue

Upon S1-reset the MME will detach the UE.

idle-mode-entry

Upon S1-reset the MME will move the UE to idle-mode. This is the default setting for this command.

Usage Guidelines

Use this command to set the MME's reactions to an S1-reset.

Example

Configure the MME to put the UE into idle-mode upon receipt of S1-reset:

```
s1-reset idle-mode-entry
```

samog-cdr

Enables the SaMOG Gateway to send the AP Group Name in the SSID field of tWANUserLocationInformation in the S-GW CDR.

Product

SaMOG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-call-control-profile-`*`profile_name`*`)#`

Syntax Description

samog-cdr twanuli ap-group-name

no samog-cdr twanuli ap-group-name

no

If configured, disables SaMOG from sending the AP Group Name in the SSID field of tWANUserLocationInformation in the S-GW CDR, and reverts the configuration to its default behavior. By default, the SaMOG Gateway sends the SSID information in the tWANUserLocationInformation attribute.

Usage Guidelines

Use this command to enable the SaMOG Gateway to send the AP Group Name in the SSID field of tWANUserLocationInformation (TWAN ULI) in the S-GW CDR.

To enable the SaMOG Gateway to send the TWAN ULI attribute in the GTPP requests, use the **gtpp attribute twanuli** command under the GTPP Group Configuration Mode.

Important

SaMOG services and standalone S-GW services must not share a GTTP group that has the **gtpp attribute twanuli** command configured. Instead, configure the command under different GTPP groups for each service.

Example

Configure SaMOG Gateway to send the AP Group Name in the SSID field of tWANUserLocationInformation in the S-GW CDR:

```
samog-cdr twanuli ap-group-name
```

samog-gtpv1

Enables SaMOG to forward the User Equipment's (UE) Identity, and/or the Access Point's (AP) Location information over the GTPv1 interface.

Product

SaMOG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

`samog-gtpv1 send { imeisv value ue-mac [ decimal | filler` *`filler_value`* `] | uli value cgi }`
`no samog-gtpv1 send { imeisv | uli }`

no

If configured, disables SaMOG from forwarding the UE Identity and/or AP Location information over the GTPv1 interface.

imeisv value ue-mac

Specifies to forward the UE Identity. By default this configuration is disabled.

decimal

Specifies to encode the UE's MAC address for the IMEIsV IE value in decimal format. By default, the UE's MAC address in the IMEIsV IE value is encoded in Hexa-decimal format.

filler *filler_value*

Specifies the 2 bytes of padding to be used with the UE's MAC address for the IMEIsV IE value.

filler_value must be a hexadecimal number from 0x0 through 0xFFFE. The default filler value is 0xFFFF.

uli value cgi

Specifies to forward the AP's User Location Information (ULI) IE during the PDP context setup.

Usage Guidelines

Use this command to enable SaMOG to forward the User Equipment's (UE) Identity, and/or the Access Point's (AP) Location information over the GTPv1 interface.

Example

Configure SaMOG to forward the AP location information :

`samog-gtpv1 uli value cgi`

samog-s2a-gtpv2

Enables SaMOG to forward S2a GTPv2 Information Element (IE) related parameters.

Important This command is available only when the SaMOG General license (supporting both 3G and 4G) is configured. Contact your Cisco account representative for more information on license requirements.

Product

SaMOG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

samog-s2a-gtpv2 send { imeisv value ue-mac [decimal | filler *filler_value* **] | pco pap value mn-nai | serving-network value uli | twan-identifier { civic-addr-fld ca-type name value ap-group-name | ssid-fld value ap-group-name } | uli }**

no samog-s2a-gtpv2 send { imeisv | pco pap value mn-nai | serving-network value uli | twan-identifier { civic-addr-fld | ssid-fld value ap-group-name } | uli }

no

Disables a previously enabled configuration.

imeisv value ue-mac [decimal | filler *filler_value*]

Specifies to forward the UE Identity in the IMEIsV IE value. By default this configuration is disabled.

decimal: Specifies to encode the UE's MAC address for the IMEIsV IE value in decimal format. By default, the UE's MAC address in the IMEIsV IE value is encoded in Hexa-decimal format.

filler: Specifies the 2 bytes of padding to be used with the UE's MAC address for the IMEIsV IE value.

filler_value must be a hexadecimal number from 0x0 through 0xFFFE.

pco pap value mn-nai

Specifies to forward the UE's MN-NAI value in the PAP container within the PCO IE in the CSR message to P-GW.

This configuration is disabled by default.

serving-network value uli

Specifies to populate the Serving-Network Information Element (IE) with the PLMN ID (MCC and MNC values) from the 3GPP-User-Location-Information AVP sent by the AAA Server (STa interface).

This configuration is disabled by default.

twan-identifier ssid-fld value ap-group-name

Specifies to forward the AP group name in the SSID sub-field of TWAN-Identifier.

By default, the SSID value is forwarded in the SSID sub-field of TWAN-Identifier.

twan-identifier civic-addr-fld ca-type name value ap-group-name

Specifies to the AP group name value in the Civic Address Information sub-field of the TWAN-Identifier IE over the S2a interface.

This configuration is disabled by default.

uli

Specifies to forward the User-Location-Information (ULI) Information Element (IE) in the CSR message over the S2a interface. SaMOG populates the ULI IE from the 3GPP-User-Location-Information AVP received from the AAA Server over the STa interface.

This configuration is disabled by default.

Usage Guidelines

Use this command to enable SaMOG to forward:

- The User Equipment's (UE) Identity information over the GTPv2 interface in decimal or hexa-decimal format
- The UE's MN-NAI value in the PAP container within the PCO IE in the CSR message.
- The Serving-Network IE information in the Create Session Request message over the S2a interface.
- The AP group name in the SSID sub-field of the TWAN-Identifier.
- The AP group name in the Civic Address Information sub-field of the TWAN-Identifier .
- The ULI IE information in the Create Session Request message over the S2a interface.

Example

Configure SaMOG to forward the UE identity with a padding value of **0xFEFE**:

```
samog-s2a-gtpv2 send imeisv value ue-mac filler 0xFEFE
```

Configure SaMOG to forward the UE's MN-NAI value in the PAP container within the PCO IE in the CSR message:

```
samog-s2a-gtpv2 send pco pap value mn-nai
```

sctp-down

Configures the behavior towards UE (user equipment) when Stream Control Transmission Protocol (SCTP) goes down.

Product MME

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

```
sctp-down { detach-ue | idle-mode-entry }
default sctp-down
```

default

Reset the profile configuration to the system default when SCTP layer goes down. The default for this command is **idle-mode-entry**.

detach-ue

When SCTP goes down, the MME will detach the UE.

idle-mode-entry

When the SCTP goes down, the MME will move the UE to idle-mode. This is the default for this command.

Usage Guidelines Use this command to set the MME's reactions when the SCTP goes down.

Example

Configure the MME to put the UE into idle-mode when the SCTP layer goes down:

```
sctp-down idle-mode-entry
```

secondary-rat

Enables the Secondary RAT Data Usage Report to support 5G NSA.

Product MME

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

```
secondary-rat data-usage-report { pgw [ sgw ]  | sgw [ pgw ] }
[ no | remove ] secondary-rat data-usage-report
```

no

Disables the Secondary RAT Usage Report at call-control-profile.

remove

Removes the Secondary-RAT Usage Report configuration from call-control-profile. It fall-back to MME service level configuration.

secondary-rat data-usage-report { pgw [sgw] | sgw [pgw] }

MME sets IR-SGW and IR-PGW flags based on the available options configured for Secondary-RAT data usage report. By default, MME disables the Secondary-RAT data usage reporting towards both SGW and PGW. If the configuration is removed from call-control-profile, then it fall-back to MME-SERVICE level configuration for Secondary-RAT-Data-Usage-Report functionality.

- **secondary-rat data-usage-report pgw**: Disables the Secondary-RAT Usage Report option for S-GW and enables only for PGW.
- **secondary-rat data-usage-report sgw**: Disables the Secondary-RAT Usage Report option for P-GW and enables only for S-GW.
- **secondary-rat data-usage-report pgw sgw**: Enables Secondary-RAT Usage Report option for both SGW and PGW.
- **secondary-rat data-usage-report sgw pgw**: Enables Secondary-RAT Usage Report option for both SGW and PGW.

Usage Guidelines

Use this command to enable the Secondary RAT Data Usage Report to support 5G NSA.

Example

Configures the Secondary-RAT Usage Report option for both SGW and PGW:

```
secondary-rat data-usage-report pgw sgw
```

serving-plmn

Configures a static serving node PLMN Identifier (MCC and MNC) for this Call Control Profile.

Product

SaMOG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

`serving-plmn id mcc` *`mcc_value`* **`mnc`** *`mnc_value`*
`remove serving-plmn id`

remove

Removes the static serving node PLMN ID configuration from this Call Control Profile.

mcc *mcc_value*

Specifies the Mobile Country Code (MCC) of the serving PLMN Identifier for this Call Control Profile.

mcc_value must be an integer between 100 and 999.

mnc *mnc_value*

Specifies the Mobile Network Code (MNC) of the serving PLMN Identifier for this Call Control Profile.

mnc_value must be an integer between 0 and 999.

Usage Guidelines

Use this command to configure a static serving node PLMN Identifier (MCC and MNC) for this Call Control Profile.

Example

Configure a static serving PLMN ID with a value of 777 for MCC and 109 for MNC using the following example:

```
serving-plmn id mcc 777 mnc 109
```

serving-plmn-rate-control

This command is used to configure the serving PLMN rate control for control plane CIoT optimization. The serving PLMN rate control limits the rate at which UE or PGW/SCEF can send data over the control plane when CP optimization is enabled.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

serving-plmn-rate-control ul-rate *ul_rate_value* **dl-rate** *dl_rate_value*
remove serving-plmn-rate-control

remove

The keyword remove deletes the existing configuration.

ul-rate *ul_rate_value*

The maximum number of data NAS PDUs the UE can send in uplink path per deci-hour (6 minutes). The uplink rate is an integer from 10 up to 65535. A value of 65535 in this case implies no limit on the number of PDUs the UE can send in the uplink path per deci-hour.

dl-rate *dl_rate_value*

The maximum number of data NAS PDUs the PGW/SCEF can send in the downlink path to the UE per deci-hour (6 minutes). The downlink rate is an integer from 10 up to 65535. A value of 65535 in this case implies no limit on the number of PDUs the PGW/SCEF can send in the downlink path per deci-hour.

Usage Guidelines

This command configures serving PLMN rate for data over NAS. It limits the rate for data exchange between UE and the PGW/SCEF while using control plane CIoT optimization. This command is not enabled by default.

Example

Use the following command to configure the serving PLMN rate for data over NAS, with uplink rate as 35 and downlink rate as 45:

serving-plmn-rate-control ul-rate *35* **dl-rate** *45*

sgs-cause-code-mapping

Configures the EMM reject cause code to send to a UE when an SGs cause code is received.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

sgs-cause-code-mapping *sgs-cause* **emm-cause-code** *emm_cause_code*
remove sgs-cause-code-mapping *sgs-cause*

remove sgs-cause-code-mapping *sgs-cause*

Removes the configured cause code mapping and returns it to its default value.

sgs-cause-code

Specifies the SGs cause code received on the SGs interface to which the new cause code should be mapped.

- **congestion** - Default mapped EMM cause code: #22 Congestion.
- **illegal-me** - Default mapped EMM cause code: #16 MSC temporarily unreachable.
- **illegal-ms** - Default mapped EMM cause code: #16 MSC temporarily unreachable.
- **imei-not-accepted** - Default mapped EMM cause code: #16 MSC temporarily unreachable.
- **imsi-unknown-in-hss** - Default mapped EMM cause code: #2 IMSI unknown in HSS.
- **imsi-unknown-in-vlr** - Default mapped EMM cause code: #16 MSC temporarily unreachable.
- **la-not-allowed** - Default mapped EMM cause code: #16 MSC temporarily unreachable.
- **network-failure** - Default mapped EMM cause code: #17 Network failure.
- **no-suitable-cells-in-la** - Default mapped EMM cause code: #16 MSC temporarily unreachable.
- **plmn-not-allowed** - Default mapped EMM cause code: #16 MSC temporarily unreachable.
- **protocol-error** - Default mapped EMM cause code: #16 MSC temporarily unreachable.
- **roaming-not-allowed-in-la** - Default mapped EMM cause code: #16 MSC temporarily unreachable.
- **service-not-subscribed** - Default mapped EMM cause code: #16 MSC temporarily unreachable.
- **service-not-supported** - Default mapped EMM cause code: #16 MSC temporarily unreachable.
- **service-out-of-order** - Default mapped EMM cause code: #16 MSC temporarily unreachable.

emm-cause-code *emm_cause_code*

Specifies the EPS Mobility Management (EMM) cause code to return to the UE for the given SGs cause code.

- **congestion**
- **cs-domain-unavailable**
- **imsi-unknown-in-hss**
- **msc-temp-unreachable**
- **network-failure**

Usage Guidelines

Use this command to configure the EMM cause code returned to a UE when an error is reported via the SGs inteface when attachment to the VLR has failed.

If a condition is specified in both the call control profile associated with a call and also the MME service, the cause configured on the call control profile is signalled to the UE.

Important EMM cause code #18 "CS Domain not available" is not mapped to any SGs code but is returned when SGs service is disallowed by a policy or on unexpected behavior such as when the MME is unable to send an SGs message to a VLR.

Related Commands

To set the cause codes for situations where a call control profile cannot be attached to a call (for example new-call restrictions, congestion during new call attempt, etc.), use the **local-cause-code-mapping** command in the mme-service configuration mode. This command is described in the *MME Service Configuration Mode Commands* chapter.

Example

The following command maps the "congestion" EMM cause code to the "network-failure" SGs cause code:

```
sgs-cause-code-mapping network-failure emm-cause-code congestion
```

sgsn-address

Defines the IP addresses for peer SGSNs in a static SGSN address table. These configured addresses can be used if operators wish to bypass DNS.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

sgsn-address { nri *nri* **| rac** *rac-id* **lac** *lac_id* **| rnc_id** *rnc_id* **} [nri** *nri* **]**
prefer { fallback-for-dns | local } address { ipv4 *ip_address* **| ipv6** *ip_address* **} interface { gn | s16 }**
no sgsn-address { ipv4 *ip_address* **| ipv6** *ip_address* **} { nri** *nri* **| rac** *rac_id*
lac *lac_id* **[nri** *nri* **| rnc_id** *rnc_id* **} [interface { gn | s16 }]**

no

Disables the specified peer-SGSN address configuration.

rac *rac_id*

Identifies the foreign routing area code (RAC) of the peer-SGSN address to be configured in the static peer-SGSN address table. *rac_id* must be an integer from 1 to 255.

lac *lac_id*

Identifies the foreign location area code (LAC) ID of the peer-SGSN address to be configured in the static peer-SGSN address table. *lac_id* must be an integer from 1 to 65535.

rnc_id *rnc_id*

Optional. Specifies the target RNC ID that maps to the address of the peer SGSN via the S16 interface. The RNC ID is used by the S4-SGSN for inter-SGSN SRNS relocations. Valid entries are 1 to 65535. This setting only applies if SRNS relocation has been configured via the **srns-inter** and/or **srns-intra** commands in *Call Control Profile Configuration Mode*.

nri *nri*

Identifies the network resource identifier stored in the P-TMSI (bit 17 to bit 23). *nri* must be an integer from 0 to 63.

Important Typically, use of this keyword is optional. However, it must be included in the command when Flex (SGSN-Pooling) is implemented.

Important Look up for peer SGSN in the local pool can be performed by configuring only the NRI value, as the NRI value is unique in a pool.

prefer { fallback-for-dns | local }

Indicates the preferred source of the address to be used.

- **fallback-for-dns** - Instructs the SGSN to perform a DNS query to get the IP address of the peer-SGSN. If the DNS query fails, then the IP address configured with this command is used.
- **local** - instructs the system to use the local IP address configured with this command.

Important If the **prefer** command is used to change an existing sgsn-address configuration (with the same LAC and RAC) from **fallback-for-dns** to **local** or from **local** to **fallback-for-dns**, the new setting overwrites the previously configured setting for all interfaces.

address { ipv4 *ip_address* | ipv6 *ip_address* }

Specifies the IP address of the peer SGSN. Currently, the IPv6 address option is not supported on the S4-SGSN.

- **ipv4** *ip_address* - specifies a valid address in IPv4 dotted-decimal notation.
- **ipv6** *ip_address* -

Important The **ipv6** option is under development for future use and is not supported in this release.

interface { gn | s16 }

interface - optional. Specifies the interface type used for communicating with the peer SGSN. Must be one of the following:

- **gn** specifies that communication will occur over the Gn interface with a peer SGSN configured for 2.5G, 3G, or dual access SGSN services.
- **s16** specifies that communication will occur over the S16 interface with a peer S4-SGSN.

Usage Guidelines

Use this command to save time by avoiding DNS. This command enables a local mapping by setting the peer-SGSN IP address to be used for inter-SGSN Attach and inter-SGSN-RAU. When configured, if the SGSN receives a RAU or an Attach Request with a P-TMSI and an old-RAI that is not local, the SGSN consults this table and uses the configured IP address instead of resolving via DNS. If this table is not configured, then IP address resolution is done using DNS.

The MCC and MNC of the RAI are taken from the IMSI range configured in the operator policy and the LAC and RAC are configured here in the call control profile configuration mode.

The **sgsn-address** command differs from other Call Control Profile configuration mode commands in the following ways:

- Within the SGSN's call logic, all other configuration elements defined with the other commands in this mode are used ***after*** the IMSI is learnt. The configuration defined with this command is part of the decision logic ***prior*** to the IMSI being known.
- With the peer-SGSN address configured using this **sgsn-address** command, the peer-SGSN-RAI's MCC/MNC is used as a 5 or 6-digit IMSI and the operator policy and call control profile selection are completed.

Important Typically, use of this command is optional. However, it must be included in the configuration when Flex (SGSN-Pooling) is implemented if (1) the SGSN functions as a default SGSN, then configure the local-NRI of other SGSN with this command; or if (2) another SGSN is offloading, then configure the NB-RAI/null-NRI of the peer-SGSN with this command.

Important It is recommended to execute the S4 SGSN configuration commands during the maintenance window. After configuring the node, re-start the node to activate the configuration commands. This will ensure that the node is in a consistent state and S4 SGSN service instability scenarios are avoided.

Example

Create a local peer-SGSN address mapping of an RAI with RAC of *123* and LAC of *4444* and an *IPv4* address of *123.11.313.11* for the peer-SGSN:

```
sgsn-address rac 123 lac 4444 local address ipv4 123.11.313.11
```

sgsn-core-nw-interface

This command enables operators to select the Gn interface or the S4 interface for EPC capable UEs and Non-EPC capable UEs on the S4-SGSN.

Product SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
sgsn-core-nw-interface { gn | s4 [ epc-ue { always | eps-subscribed }
non-epc-ue { never | always | eps-subscribed } ] }
```

sgsn-core-nw-interface { gn | s4 }

Specifies the interface that EPC-capable UEs will use to communicate wit the packet core gateways (GGSN/SGW). Selection must be one of:

- **gn**: Forces the SGSN to forcefully select the Gn interface for EPC-capable UEs.
- **s4**: Specifies that the SGSN will use the S4 interface between the S4-SGSN and packet core gateways (GGSN/SGW). This is the default setting for EPC-capable UEs.

The S4-SGSN uses GTPv2 by default and allows new Inter SGSN RAUs over GTPv2 for all subscribers. The S4-SGSN allows ISRAUs over GTPv2 even if the subscriber's call-control-profile is configured explicitly with Gn interface as the S4-SGSN does not check for core network interface configured for a specific subscriber before allowing GTPv2. The inbound ISRAUs over GTPv2 interface has to be restricted for roaming subscribers. Access to S4 interface or GTPv2 should be limited only to home subscribers.

In release 19.3.10 the configuration of the CLI command **sgsn-core-nw-interface** was used to decide whether to reject/honor the RAU request upon context response received via GTPv2.

The configuration of the CLI command **sgsn-core-nw-interface** is used to impose restriction on roaming subscribers for ISRAU over GTPv2. The command **sgsn-core-nw-interface gn** has to be configured in the roaming subscribers call-control-profile to implement the restriction on ISRAU over GTPv2 for roaming subscribers. When the EGTP context response is received from the peer during inbound ISRAU over GTPv2, a new check is introduced where the **sgsn-core-nw-interface gn** command configuration is verified. If the subscriber’s call-control profile is configured to use Gn interface alone, then EGTP Context ACK with failure cause will be sent to peer and RAU will fall back to GTPv1. The failure cause value sent in EGTP context Ack message to peer is EGTP_CAUSE_USER_AUTHENTICATION_FAILED. This is applicable for both 2G and 3G scenarios. The following table displays the actions based on the configuration:

Interface	sgsn-core-nw-interface gn	sgsn-core-nw-interface s4
GTPv1 protocol	Proceed with call	Proceed with call
GTPv2 protocol	RAU fall back to GTPv1 and proceed with call	Proceed with call

epc-ue

Configures the S4 Interface Selection Option for EPC Capable UE.

non-epc-ue

Configures the S4 Interface Selection Option for Non-EPC Capable UE.

always

Instructs the SGSN to always choose a S4 Interface.

never

Instructs the SGSN to not choose a S4 Interface.

eps-subscribed

Instructs the SGSN to choose a S4 Interface if EPS Subscription is available.

Important

- When keywords or options are not selected with the selection of the S4 interface option, it implies that the SGSN will apply S4 interface always for both EPC and Non- EPC devices. This is also synonymous to the CLI command configured as **sgsn-core-nw-interface s4 epc-ue always non-epc-ue always**.
- To configure SGSN behavior supported in previous releases, the CLI is configured as **sgsn-core-nw-interface s4 epc-ue always non-epc-ue eps-subscribed**. This is also the default behavior when the CLI is not configured.

Important It is recommended to execute the S4 SGSN configuration commands during the maintenance window. After configuring the node, re-start the node to activate the configuration commands. This will ensure that the node is in a consistent state and S4 SGSN service instability scenarios are avoided.

Usage Guidelines

Use this command to forcefully select the interface that the SGSN will use for EPC-capable UEs.

This command is available only if the *SGSN S4 Interface* license is enabled on the SGSN.

Example

sgsn-core-nw-interface gn

sgsn-number

Defines the SGSN's E.164 number to be used for interactions via the Mobile Application Part (MAP) protocol. E.164 is an ITU-T recommendation that defines the international public telecommunication numbering plan used in public switched telephone networks (PSTN) and some other data networks.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

sgsn-number *E164_number*
no sgsn-number

no

Disables the use of this configuration definition.

E164_number

Specifies a string of 1 to 16 digits that serve as the SGSN's E.164 identification.

Usage Guidelines

This command configures the current SGSN E164 contact number.

The SGSN number configured for a call control profile is related to the SGSN number configured in the SGSN service configuration and/or in the GPRS service configuration. If the SGSN number is not configured as part of the call control profile configuration, then the SGSN number defined as part of the SGSN service or GPRS service configuration is used.

When the 3G SGSN supports multiple PLMNs configured through different IuPS services or when network sharing is implemented, then it may be required to use different SGSN numbers for each PLMN. In such cases, configure the per-PLMN SGSN number in a call control profile. SGSN number definition for a call control profile allows emulation of a different SGSN to each HLR per PLMN. SGSN number definitions in the call control profile also enable the SGSN to use a different SGSN number per operator when network sharing is implemented.

Example

Map the E.164 number *198765432123456* for the SGSN to this call control profile configuration:

```
sgsn-number 198765432123456
```

sgtp-service

Identifies the SGTP service configuration to be used according to this call control profile.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
sgtp-service context ctxt_name service sgtp_service_name
no sgtp-service context
```

context *ctxt_name*

Specifies the SGTP context as an alphanumeric string of 1 through 64 characters.

service *sgtp_service_name*

Specifies the SGTP service name as an alphanumeric string of 1 through 64 characters.

no

Disables use of SGTP service.

Usage Guidelines Use this command to configure enabling or disabling of SGTP service for this call control profile.

Example

```
sgtp-service context sgtp1 service sgtp-srvc1
```

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 > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-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.

Example

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
```

sms-in-mme

Configures the MME preference for SMS and SMSC address.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
sms-in-mme { preferred [ smsc-address smsc_address ] | smsc-address smsc_address
 | subscribe [ notify ue ] }
default sms-in-mme { subscribe [ notify ue ] }
no sms-in-mme { preferred [ smsc-address ] | smsc-address | subscribe [
notify ue ] }
```

default

Restores the default configuration, which is to enable the Subscription Request for SMS services (via SGd) to HSS for all users.

no

Deletes the specified configuration.

sms-in-mme { preferred [smsc-address *smsc_address*] | smsc-address *smsc_address* }

Configures the SMS capability (SGd interface for SMS) in MME.

- **preferred**: Configures the SMS preference in MME.

- **smsc-address** *smsc_address*: Configures the SMSC address (ISDN identity) for the MME to send SMS on the SGd interface. *smsc_address* must be an integer from 1 to 15.

subscribe [notify ue]

Enables the Subscription Request for SMS services (via SGd) to HSS for all users.

- **notify**: Configures the notification to be sent to the users.
- **ue**: Sends SMS-Only indication to UE in Attach/TAU Accept message (only if HSS accepts SMS Registration for SGd).

Usage Guidelines

Use this command to configure SGd as the preferred SMS service and to configure the SMSC address.

Example

The following command configures the preferred SGd SMS option with SMSC address *91984599136* for a subscriber:

```
sms-in-mme preferred smsc-address 91984599136
```

sms-mo

Configures how mobile-originated (MO) short message service (SMS) messages are handled.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
[ remove ] sms-mo { { access-type { gprs | umts } { all-location-areas |
 location-area-list } | allow access-type { gprs | umts } | restrict
access-type { gprs | umts } }
```

remove

Deletes the specified configuration.

access-type *type*

Access by SMS will be limited to SMS coming from this network type:

- **gprs**
- **umts**

allow

Allow either GPRS or UMTS type access for SMS.

restrict

Restrict either GPRS or UMTS type access for SMS.

location-area-list instance *instance*

instance must be an integer between 1 and 5. The value must identify an already defined location area code (LAC) list created with the **location-area-list** command.

failure-code *code*

code: Must be an integer from 2 to 111.

Usage Guidelines Configure filtering for SMS-MO messaging.

Example

```
sms-mo access-type gprs all-location-areas failure-code 100
```

sms-mt

This command configures how mobile-terminated (MT) short message service (SMS) messages are handled.

Product SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
[ remove ] sms-mt { { access-type { gprs | umts } { all-location-areas |
 location-area-list } | allow access-type { gprs | umts } | restrict
access-type { gprs | umts } }
```

remove

Deletes the specified configuration.

access-type *type*

Access by SMS will be limited to SMS coming from this network type:

- **gprs**

- **umts**

allow

Allow either GPRS or UMTS type access for SMS.

restrict

Restrict either GPRS or UMTS type access for SMS.

location-area-list instance *instance*

instance must be an integer between 1 and 5. The value must identify an already defined LAC list created with the **location-area-list** command.

failure-code *code*

code: Must be an integer from 2 to 111.

Usage Guidelines

Configure filtering for SMS-MT messaging.

Example

```
sms-mt access-type gprs all-location-areas failure-code 100
```

srns-inter

Defines handling parameters for Inter-SRNS (Serving Radio Network Subsystem) relocation.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
srns-inter ( all failure-code | allow { routing-area-list instance
instance_id | location-area-list instance instance_id | location-area-list
instance instance failure-code code| routing-area-list instance instance_id
failure-code code | restrict location-area-list instance instance_id|
routing-area-list instance instance_id }
no srns-inter { allow location-area-list instance instance_id |
routing-area-list instance instance_id  | restrict location-area-list
instance instance_id }
default srns-inter { all | location-area-list-instance instance_id |
routing-area-list instance instance_id  }
```

no

Deletes the inter-SRNS relocation configuration.

default

Resets the configuration to default values.

all failure-code *code*

Define the failure code that will apply to all inter-SRNS relocations.

code must be an integer from 2 to 111.

allow { location-area-list instance *instance_id* | routing-area-list instance *instance_id* }

Identifies the location area list Id (LAC Id) or routing area list Id (RAC Id) that will allow services in the defined area.

location-area-list instance *instance*

instance: Must be an integer between 1 and 5 that identifies the previously defined location area list created with the **location-area-list** command.

routing-area-list instance *instance_id*

Instructs the SGSN to apply the command action to a specific routing area list. Routing area lists should already have been created with the **routing-area-list** command.

instance_id must be an integer from 1 to 5.

restrict { location-area-list instance *instance_id* **| routing-area-list instance** *instance_id* **}**

Identifies the location area list Id (LAC Id) or routing area list Id (RAC Id) that indicates the areas where services will be restricted.

Usage Guidelines This command defines the operational parameters for inter-SRNS relocation.

Example

The following command allows services in areas listed in LAC list #3:

```
srns-inter allow location-area-list instance 3
```

srns-intra

Defines handling parameters for intra-SRNS (Serving Radio Network Subsystem) relocation.

Product SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
srns-intra ( all failure-code | allow { routing-area-list instance
instance_id | location-area-list instance instance_id | location-area-list
instance instance failure-code code| routing-area-list instance instance_id
failure-code code | restrict location-area-list instance instance_id|
routing-area-list instance instance_id }
no srns-intra { allow location-area-list instance instance_id |
routing-area-list instance instance_id  | restrict location-area-list
instance instance_id }
default srns-intra { all | location-area-list-instance instance_id |
routing-area-list instance instance_id  }
```

no

Deletes the intra-SRNS relocation configuration.

default

Resets the configuration to default values.

all failure-code *code*

Define the failure code that will apply to all intra-SRNS relocations.

code: Must be an integer from 2 to 111.

allow { location-area-list instance *instance_id* | routing-area-list instance *instance_id* }

Identifies the location area list Id (LAC Id) or routing area list Id (RAC Id) that will allow services in the defined area.

location-area-list instance *instance*

instance: Must be an integer between 1 and 5 that identifies the previously defined location area list created with the **location-area-list** command.

routing-area-list instance *instance_id*

Instructs the SGSN to apply the command action to a specific routing area list. Routing area lists should already have been created with the **routing-area-list** command.

instance_id must be an integer from 1 to 5.

restrict { location-area-list instance *instance_id* **| routing-area-list instance** *instance_id* **}**

Identifies the location area list Id (LAC Id) or routing area list Id (RAC Id) that indicates the areas where services will be restricted.

Usage Guidelines

This command defines the operational parameters for intra-SRNS relocation.

Example

The following command restricts service in areas listed in the LAC list 1:

```
srns-intra restrict location-area-list instance 1
```

srvcc exclude-stnsr-nanpi

Configures the MME to **not** include the Nature of Address and Numbering Plan Indicator (NANPI) in the Session Transfer Number for Single Radio Voice Call Continuity (STN-SR) IE on Sv interface in PS to CS requests to the MSC server and Forward Relocation requests to the peer-SGSN/peer-MME.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-call-control-profile-`*`profile_name`*`)#`

Syntax Description

`[ remove ] srvcc exclude-stnsr-nanpi`

remove

Deletes this configuration from the call control profile. This returns the MME to its default configuration where the NANPI is not included in the STN-SR IE.

Usage Guidelines

This command applies to Release 15.0 MR3 and higher.

In Release 15.0 MR3 and later releases, the encoding of the STN-SR IE on Sv interface now includes the NANPI from the HSS in PS to CS requests to the MSC server and Forward Relocation requests to the peer-SGSN/peer-MME. The value of NANPI sent by the MME is 0x11. This change in behavior is provided in support of TS 29.280 V10.1.0.

This command provides an option to maintain backward compatibility. When this command is issued, the MME excludes the NANPI from these requests, as was the default in releases prior to 15.0 MR3.

srvcc

This command configures the basic SRVCC support on the MME.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

`[ remove ] srvcc unauthorized`

remove

Deletes this configuration from the call control profile. This returns the MME to its default configuration where the SRVCC handovers are allowed.

unauthorized

Restricts the SRVCC handovers for a set of subscribers.

Usage Guidelines

This command is not enabled by default. The operator must enable **unauthorized** to restrict SRVCC handovers for a set of subscribers.

subscriber multi-device

Enable or disable the operator policy from allowing multiple PDN connections. When enabled, a maximum of 11 PDN connections are allowed for a subscriber.

Product

SaMOG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

`[ no ] subscriber multi-device`

no

If previously enabled, disables multiple PDN device connections for a subscriber.

Usage Guidelines

Use this command to enable or disable the operator policy from allowing multiple PDN connections for a subscriber. If this optional configuration is not enabled, only one PDN connection is allowed for a subscriber.

Important

The SaMOG Web Authorization feature is license dependent. Contact your Cisco account representative for more information on license requirements.

Example

The following command enables mutiple device connections for a subscriber:

subscriber multi-device

subscriber-control-inactivity

Configures \the subscriber-control inactivity timer. The system detects inactivity when no PDP context is activated and starts the timer.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-call-control-profile-`*`profile_name`*`)#`

Syntax Description

subscriber-control-inactivity timeout minutes *time* **detach { immediate | next-connection | reattach-time-period }**
{ no | default } subscriber-control-inactivity

no

Deletes the timer configuration.

default

Resets the timer configuration to the default value of 7 days (10080 minutes).

timeout minutes *time* [detach]

Sets the number of minutes the SGSN monitors the connection after inactivity has been detected. When the timer expires, the subscribe will be detached.

time: Enter an integer from 1 to 20160 (two weeks).

detach [immediate | next-connection | reattach-time-period]

Instructs the SGSN to detach and can be configured to specify when the detach will occur after inactivity is detected. To fine-tune the detach instruction, include one of the following with the command:

- **immediate** - Instructs the SGSN to detach immediately after inactivity is detected. May combine with **reattach-time-period**.
- **next-connection** - Instructs the SGSN to wait for the next Iu connection after inactivity is detected and then detach. Any message except Attach on the next Iu is unconditionally rejected with cause code “GPRS services not allowed”.

Important Supported for 3G SGSNs only.

- **reattach-time-period** *period* **[action]** - Specify the number of seconds the SGSN will monitor a new re-attach after the previous detach was due to inactivity. Also, you can define the action to be taken regarding new attaches.

  period: Enter an integer from 60 to 3600.

  action - Select an action:

  - **deny**
  - **permit-and-stop-monitoring**

Usage Guidelines Use this command to configure the timeout timer. After this timer times out the subscriber is detached from the SGSN.

Example

The following command instructs the SGSN to monitor the connection for up to *360* minutes after inactivity is detected, or detach immediately after inactivity is detected:

```
subscriber-control-inactivity timeout minutes 360 detach immediate
```

super-charger

Enables or disables the SGSN to work with a super-charged network.

Product SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description **[remove] super-charger**

remove

Disables the super-charger functionality.

Usage Guidelines By enabling the super charger functionality for 2G or 3G connections controlled by an operator policy, the SGSN changes the hand-off and location update procedures to reduce signalling traffic management.

Example

The following command enables the super charger feature:

super-charger

tau

Configure parameters for the tracking area update (TAU) procedure.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-call-control-profile-`*`profile_name`*`)#`

Syntax Description

tau { imei-query-type { imei | imei-sv | none } [verify-equipment-identity [allow-on-eca-timeout | deny-greylisted | deny-unknown | verify-emergency]] | inter-rat { notify-request | security-ctxt { allow-mapped | native } } }
remove tau { imei-query-type | inter-rat { notify-request | security-ctxt } }

remove

Deletes this TAU configuration from the call control profile.

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

This keyword set is specific to the MME.

Sets the IMEI query-type if an IMEI (International Mobile Equipment Identity) is not already present.

- **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.

inter-rat notify-request

Configure inter-RAT parameters for TAU. This keyword provides the operator with the option of sending Notify-Request to HSS from MME during 3G to 4G TAU/HO.

inter-rat security-ctxt { allow-mapped | native }

Configure inter-RAT parameters for TAU. This keyword provides the operator with the option of continuing with the mapped context or creating a new native context after an inter-RAT handover.

- **allow-mapped**: Configures inter-RAT security-context type as mapped. Mapped security context is allowed after inter-RAT handover. This is the default value.
- **native**: Configures inter-RAT security-context type as native only. Inter-RAT handover will always result in a native security context.

Usage Guidelines

Use this command to define tracking area update procedures such as inter-RAT security context and IMEI query-type.

Example

The following command sets the IMEI query type to IMEI-SV:

```
tau imei-query-type imei-sv verify-equipment- identity
```

tcp-maximum-segment-size

This command enables the operator to define a maximum segment size (MSS), that will be used to overwrite received TCP MSS values in uplink/downlink packets between UE and the server.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

tcp-maximum-segment-size *size*
remove tcp-maximum-segment-size

remove

Instructs the SGSN to forward the user data without changing the TCP MSS value.

size

This entry specifies the maximum number of octets for a segment. Valid range is 1 to 1460.

Usage Guidelines

When configuring with this command, an additional Yes/No prompt is included due to the high impact of the MSS configuration.

Configure the MSS, helps the operator to avoid fragmentation. This command enables the operator to modify or overwrite the TCP MSS value exchanged between the UE and the server (for both 2G and 3G uplink/downlink traffic) if the requested value is more than the SGSN's locally configured value.

Example

Use a command similar to the following to define 1200 octets as the maximum segment size:

tcp-maximum-segment-size 1200

timeout

Configure the duration after which the cached MAC to IMSI mapping entry maintained by the IPSG manager during the SaMOG web authorization pre-authentication phase is removed.

Product

SaMOG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]`*host_name*`(config-call-control-profile-`*profile_name*`)#`

Syntax Description

timeout imsi cache *timer_value*
{ default | no } timeout imsi cache

default

Sets the timeout duration to its default value.

Default: 1440 minutes

no

If previously configured, removes the timeout duration.

timer_value

timer_value must be an integer between 1 to 20160 minutes.

Usage Guidelines

Use this command to configure the duration after which the cached MAC to IMSI mapping entry of a subscriber device maintained by the IPSG manager during the SaMOG web authorization pre-authentication phase is removed.

Important

The SaMOG Web Authorization feature is license dependent. Contact your Cisco account representative for more information on license requirements.

Example

The following command sets a timeout value for clearing the MAC to IMSI mapping entry to 2000 minutes:

```
timeout imsi cache 2000
```

treat-as-hplmn

Enables or disables the SGSN to treat an IMSI series as coming from the home PLMN.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

```
[ remove ] treat-as-hplmn
```

remove

Deletes this configuration from the profile. This would disable this function and is the default.

Usage Guidelines

Use this command to enable or disable the SGSN to treat an IMSI series as coming from the home PLMN.

Example

The following command disables previously configured feature:

```
remove treat-as-hplmn
```

vplmn-address

Enables/disables the SGSN to override the VPLMN address-allowed flag.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(config-call-control-profile-`*`profile_name`*`)#`

Syntax Description

`vplmn-address { allowed | not-allowed }`
`remove vplmn-address`

remove

Using **remove** disables the override behavior and the VPLMN-Address-Allowed flag is interpreted as it is in the subscription data.

allowed

Using **allowed** instructs the SGSN to set the VPLMN-Address-Allowed flag during GGSN seletion - even if the flag was not received in the subscription data from the HLR.

not-allowed

Using **not-allowed** instructs the SGSN not to set the VPLMN-Address-Allowed flag during GGSN seletion - even if the flag is received in the subscription data from the HLR.

Usage Guidelines

Use this command to override the VPLMN-Address-Allowed flag received in subscription data from HLR during GGSN selection. This flag is used to decide whether to use the VPLMN-OI received from a roaming subscriber to form the full-APN. The full-APN is then used in a DNS query to select a GGSN. This override enables the operator to control selection of a different GGSN for a roaming subscriber by using/not-using VPLMN-OI in full-APN.

Example

The following command instructs the SGSN to set the VPLMN-Address-Allowed flag during GGSN selection, even if the flag was not received in subscription data from the HLR:

`vplmn-address allowed`

The following command instructs the SGSN not to set the VPLMN-Address-Allowed flag during GGSN selection, even if the flag was received in subscription data from the HLR:

`vplmn-address not-allowed`

The following command instructs the SGSN not to override standard behavior regarding the VPLMN-Address-Allowed flag:

```
remove vplmn-address
```

zone-code

Configures a zone code listing of one or more location area code (LACs) included in the zone.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax Description

zone-code *zc_id* **location-area-code** *lac*
no zone-code *zc_id* **[location-area-code** *lac* **]**

no

Removes either a specific LAC from the zone code list. If the **location-area-code** parameter is not included in the command, then the entire zone code list definition is removed from configuration.

zc_id

Identifies an instance of a zone code list as an integer from 1 to 65535.

An unlimited number of zone code lists can be configured per Call Control Profile as the zone code lists are allocated dynamically.

location-area-code *lac*

Prompts for the location area-code(s), where the subscribers can roam, that are part of the zone. *lac* is an integer from 1 to 65535.

Repeat the **zone-code** command with this keyword to include up to 100 LACs in each zone code list.

Usage Guidelines

Important While there is no limit to the number of zone codes that can be created, only 100 LACs per zone code can be defined.

Use this command to define zone code restrictions. Regional subscription data at the home location register (HLR) is used to determine the regional subscription area in which the subscriber is allowed to roam. The regional subscription data consists of a list of zone codes. A zone code is comprised of one or more location areas (identified by a LAC) into which the subscriber is allowed to roam. Regional subscription data, if present in the insert subscriber data (ISD) request from the HLR, defines the subscriber's subscription area for the

addressed SGSN. It contains the complete list (up to 10 zone codes) that apply to a subscriber in the currently visited PLMN.

During the GPRS Location Update procedure, the zone code list is received in the ISD request from the HLR. The zone code list from the HLR is validated against the configured values in the operator policy. If matched, then the ISD is allowed to proceed. If not matched, then the ISD response is that the Network Node Area is Restricted and the GPRS Location Update procedure fails. If no zone codes are included in the ISD (whether or not the zone codes are defined in the SGSN configuration), then checking is not done.

Example

The following command defines multiple LACs for zone code 1:

```
zone-code 1 lac 413 212 113
```