

SGSN Global Configuration Mode Commands

Command Modes

The commands in this mode configure parameters that impact the entire SGSN and that are independent of the GPRS or the IuPS services.

Exec > Global Configuration > SGSN Global Configuration

configure > sgsn-global

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

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

- aggregate-ipc-msg, on page 2
- apn-resolve-dns-query snaptr, on page 4
- bssgp-message dl-unitdata, on page 5
- bssgp-message ms-flow-control-from-unknown-ms , on page 6
- bssgp-message ptp-bvc-reset, on page 7
- bssgp-timer, on page 8
- bvc-unblock, on page 9
- canonical-node-name, on page 10
- common-ra-paging, on page 10
- congestion-control, on page 11
- do show, on page 12
- dscp-template, on page 12
- dual-address-pdp, on page 14
- ec-gsm, on page 15
- eir-profile, on page 15
- end, on page 16
- exit, on page 16
- gmm-message, on page 17
- gmm-sm-statistics, on page 17
- gprs-mocn, on page 18
- interface-management, on page 18

- ipms-suppress, on page 19
- imsi-range, on page 20
- location-services, on page 22
- map-message, on page 23
- max-pending-attaches, on page 24
- msisdn-group, on page 25
- msisdn-range, on page 26
- old-tlli invalidate tlli, on page 27
- old-tlli hold-time, on page 28
- pdp-deactivation-rate , on page 29
- qos-arp-rp-map-profile, on page 30
- ranap excess-len ignore, on page 31
- ran-information-management, on page 32
- target-offloading, on page 32
- tlli-cb-audit, on page 33
- umts-aka-r99, on page 34

aggregate-ipc-msg

Configures the number of inter-process communication (IPC) messages that can be aggregated in the various managers and defines the frequency of flushing the messages.

Important In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

Product

SGSN

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > SGSN Global Configuration

configure > sgsn-global

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

Syntax Description

aggregate-ipc-msg { gbmgr | linkmgr | sessmgr } { auto-num-msgs | flush-frequency*frequency* **| num-msgs** *number_msgs* **}**
default aggregate-ipc-msg { gbmgr | linkmgr | sessmgr }

default

Resets the managers to default values for flushing.

gbmgr

Selects the Gb manager to configure the number of IPC messages to be aggregated and frequency of flushing messages to the Session Manager that have been aggregated at the Gb Manager.

linkmgr

Selects the linkmgr to configure the number of IPC messages to be aggregated and frequency of flushing.

sessmgr

Selects the sessmgr to configure the number of IPC messages to be aggregated and frequency of flushing.

auto-num-msgs

Enables the automated aggregation of messages sent from LinkMgr or GbMgr to the SessMgr.

Default is Disabled.

flush-frequency *frequency*

Configure the frequency, in 100-millisecond intervals, that the aggregated IPC messages will be flushed. Flushing limits the number of messenger calls between managers to transfer the received packets.

frequency : Enter an integer from 1 to 3. Default is 1.

num-msgs *number_msgs*

Configure the number of IPC messages to aggregate before flushing.

number_msgs : Enter the integer 1 (to disable aggregation) or an integer from 2 to 164 to define the number of messages. Default is 10.



Important Setting **num-msgs** to a value of 1 will disable message packet aggregation.

Usage Guidelines

Use this command to enable/disable aggregation of IPC messages in the linkmgr and/or the sessmgr. This command includes options to configure the frequency of aggregated message flushing and the number of packets to be buffered before the flush. This command provides a solution for reducing latency while sending the IPC messages towards the core network (CN).

The flushing limit will be based on either desired flush-frequency or maximum number of messages to be aggregated. Repeat the command to engage multiple limits.

By default, the link manager buffers packets and then send them over the SCCP link if there are events to be sent via SCCP Connection Request (SCCP CR) towards the core node. The HNB-GW/SGSN aggregate packets for 100 msec and send them with whatever aggregation has been done during those 100 msecs.

At the HNB-GW/SGSN, this command can be used to reduce the processing involved in sending every event individually towards the core node in the following manner:

- If aggregation is enabled, then there could be a time delay for sending SCCP CRs depending on configuration of the HNB-GW or SGSN.
- If aggregation is reduced to 1, then there will be no delay for aggregation and events are sent via SCCP CR without delay. This reduces the SCCP connection setup time.

To view aggregate IPC message statistics, use command **show config | grep aggregate-ipc-msg**.

Example

Configure the linkmgr to buffer *45* messages before flushing the linkmgr IPC messages:

```
aggregate-ipc-msg linkmgr flush-frequency 45
```

The following command configures the *linkmgr* to flush the IPC messages towards the CN without aggregation:

```
aggregate-ipc-msg linkmgr1
```

The following command configures the *sessmgr* to flush the IPC messages towards the CN without aggregation:

```
aggregate-ipc-msg sessmgr1
```

apn-resolve-dns-query snaptr

Enable/disable sending of SNAPTR DNS query to resolve an APN for a subscriber with an EPS (evolved packet system)-capable handset.

Important This command is no longer available in all 12.0 and 12.2 releases. If you do not see this command in your release, look for the **apn-resolve-dns-query snaptr** command in the APN Profile configuration mode to accomplish the same task.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > SGSN Global Configuration

configure > sgsn-global

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

Syntax Description

```
[ no ] apn-resolve-dns-query snaptr
default apn-resolve-dns-query
```

default

Resets the default, the ability to send SNAPTR DNS query is disabled.

no

Disables the ability to send SNAPTR DNS query.

Usage Guidelines

By default, sending the SNAPTR DNS query is disabled. Use this command to send SNAPTR DNS query when resolving an APN for an EPS-capable subscriber.

At PDP context activation, the SGSN will use the UE capabilitly as input to select either a GGSN or a P-GW for the EPS-capable subscriber. The SNAPTR DNS query will be used for P-GW resolution. Enabling this feature will give priority to P-GW selection for E-UTRAN-capable UEs.

Example

Use the following command to enable sending of SNAPTR DNS query for APN resolution:

```
apn-resolve-dns-query
```

Use the following command to disable the use of SNAPTR DNS query for APN resolution:

```
no apn-resolve-dns-query
```

bssgp-message dl-unitdata

Configure this command to exclude or include RAT/Frequency Selection Priority (RFSP ID) in BSSGP DL-Unitdata messages to the BSC.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > SGSN Global Configuration

configure > sgsn-global

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

Syntax Description

```
bssgp-message dl-unitdata rfsp-id exclude
default bssgp-message dl-unitdata rfsp-id
```

default

By default, the RFSP-ID IE is included in BSSGP DL-Unitdata message.

dl-unitdata rfsp-id exclude

Use this keyword to exclude RFSP-ID IE in BSSGP DL-Unitdata message.

Usage Guidelines

The SGSN can control sending of RAT/Frequency Selection Priority (RFSP ID) from subscription or a local overridden value towards BSC.

Example

Use this command to exclude the RFSP ID in BSSGP DL-Unitdata message:

```
bssgp-message dl-unitdata rfsp-id exclude
```

Use this command to include the RFSP ID in BSSGP DL-Unitdata message:

default bssgp-message dl-unitdata rfsp-id

bssgp-message ms-flow-control-from-unknown-ms

This command determines the SGSN response to MS-Flow-Control messages received from an unknown MS.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > SGSN Global Configuration

configure > sgsn-global

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

Syntax Description

bssgp-message ms-flow-control-from-unknown-ms { discard-message | send-ack | send-status }
default bssgp-message ms-flow-control-from-unknown-ms

default

Including **default** with the command configures the SGSN to use default behavior so that the SGSN sends BSSGP-Status messages whenever the SGSN receives an MS-Flow-Control message from an unknown MS.

discard-message

This keyword instructs the SGSN to discard the received BSSGP message. With this option, the SGSN does not send any response to the MS after discarding the received BSSGP message.

send-ack

This keyword instructs the SGSN to send an acknowledgement message (MS-Flow-Control-ACK) after receiving an MS-Flow-Control message.

send-status

Default

This keyword instructs the SGSN to send a BSSGP-Status message to the MS whenever the SGSN receives an MS-Flow-Control message from an unknown MS.

Usage Guidelines

This command allows the operator to specify the action the SGSN needs to take whenever the SGSN receives an MS-Flow-Control message from an unknown mobile station. This configuration determines the response for the SGSN globally.

The list of possible actions are:

- send a BSSGP-Status response message

- send an ACK message (MS-Flow-Control-ACK)
- discard the BSSGP message

To see the statistics for the number of MS-Flow-Control messages that have been discarded, use the **show bssgp statistics** command from the Exec mode.

Example

Change the default configuration and have the SGSN acknowledge receipt of the MS-Flow-Control message:

```
bssgp-message ms-flow-control-from-unknown-ms send-ack
```

bssgp-message ptp-bvc-reset

This command determines the SGSN response, per BVCI, to receipt of a peer-to-peer BVC Reset.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > SGSN Global Configuration

configure > sgsn-global

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

Syntax Description

```
bssgp-message ptp-bvc-reset { frc-subscriber-standby | retain-current-state
 }
default bssgp-message ptp-bvc-reset
```

default

Including **default** with the command configures the SGSN to use default behavior so that the SGSN continues with the current state once a peer-to-peer BVC Reset is received.

frc-subscriber-standby

This keyword instructs the SGSN to change the state of the subscribers to standby when the peer-to-peer BVC Reset is received.

retain-current-state

Default

This keyword instructs the SGSN to continue the current state of the subscribers when the BVC Reset message is received.

Usage Guidelines

This command allows the operator to specify the action the SGSN needs to take whenever the SGSN receives a peer-to-peer BVC Reset message for a specific BVCI.

To confirm the configuration for the response to the BVC Reset, use the **show sgsn-mode** command from the Exec mode.

Example

Change the default configuration and have the SGSN change subscriber states to standby:

```
bssgp-message ptp-bvc-reset frc-subscriber-standby
```

bssgp-timer

Configures the T2 and TH timers for the BVCs (BSSGP virtual connections) of the NSE (network service entities).

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > SGSN Global Configuration

configure > sgsn-global

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

Syntax Description

```
bssgp-timer { t2 T2_time | th TH_time }
default bssgp-timer { t2 | th }
```

default

Resets the specified timers to default settings.

t2 *T2_time*

Configures the BVC reset guard timer (at the BSSGP layer) in units of 1 second.

T2_time : Enter an integer from 1 to 120. Default is 30 seconds.

th *TH_time*

Configures, at the BSSGP layer, the MS flow control parameter validity timeouts in units of 1 second.

TH_time : Enter an integer from 6 to 5999. Default is 500 seconds.

Usage Guidelines

Use this command to configure timer timeout values for MS flow control and BVC reset timers that control BVCs for the NSEs.

Example

Set the TH timeout for *20* seconds:

```
bssgp-timer th 20
```

bvc-unblock

This command enables (disabled by default) or disables the SGSN to unblock blocked BVCs based on the receipt of uplink packets from the BSC.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > SGSN Global Configuration

configure > sgsn-global

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

Syntax Description

bvc-unblock { data-or-flow-control | flow-control | ul-data }
[default | no] bvc-unblock

default

Include **default** with the command to disable the function.

no

Include **no** with the command to disable this function.

data-or-flow-control

Enables the BVC-Unblock function when the SGSN receives either a FLOW-CONTROL-BVC packet or a UL-UNITDATA packet.

flow-control

Enables the BVC-Unblock function when the SGSN receives a FLOW-CONTROL-BVC packet.

ul-data

Enables the BVC-Unblock function when the SGSN receives a UL-UNITDATA packet.

Usage Guidelines

Configurations defined with this command are common to all NSE defined for the SGSN.

This command is useful if there is a BVC status mismatch across different SGSN managers (such as the sessmgr and the linkmgr) when the BSC sends BVC-Block (SGSN should move to BLOCKED) followed by a BVC-Reset (SGSN should move to UNBLOCKED). Such mismatches can easily occur, particularly on Gb-IP network connection, when one link receives the BVC-Block and a different link receives the BVC-Reset with little delay between the two.

If BVC-Unblock function is enabled, the SGSN ensures that BVCs which are in the BLOCKED state move to the UNBLOCKED state upon receipt of the configured packet type(s).

Example

Instruct the SGSN to perform BVC-Unblock when a mismatch occurs and the SGSN receives a FLOW-CONTROL-BVC packet:

```
bvc-unblock flow-control
```

canonical-node-name

Defines the SGSN's canonical node name.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > SGSN Global Configuration

configure > sgsn-global

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

Syntax Description

`[ no ] canonical-node-name` *canonical_node_name*

no

Erases the specified canonical node name definition from the SGSN Global configuration.

Usage Guidelines

canonical_node_name is a fully or properly qualified domain name; for example sgsn.div.bng.kar.3gppnetwork.org.

In order for the Gn/Gp-SGSN to support the topological gateway selection feature, the SGSN's canonical node name must be defined in the SGSN's configuration. (This is not needed for the S4-SGSN). For additional information about this feature, refer to the *Topology-based Gateway Selection* section in the *SGSN Administration Guide*.

Example

Define the SGSN's canonical node name as *sgsn.div.bng.kar.3gppnetwork.org*:

```
canonical-node-name  sgsn.div.bng.kar.3gppnetwork.org
```

common-ra-paging

This command enables paging across common Routing Area (RA) for 2G and 3G.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > SGSN Global Configuration

configure > sgsn-global

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

Syntax Description

`[ default | no ] common-ra-paging`

default

Returns the SGSN to the default state: paging across commong Routing Area (RA) is disabled for 2G and 3G.

no

Disables paging across common Routing Area (RA) for 2G and 3G after it has been enabled using the **common-ra-paging** command

Usage Guidelines

When this CLI is enabled, the SGSN supports paging initiation in both the RATs (2G and 3G) if paging has to be done in RA which is common across the RATs. SGSN also accepts power-off detach from the MS, which is different from the RAT when the MS is attached.

Example

Use the following command to enable paging across common Routing Area (RA) for 2G and 3G.

`common-ra-paging`

congestion-control

Sets up the environment on the SGSN to support Machine Type Communications (MTC) congestion control and opens a new SGSN Global Congestion Control command configuration mode.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > SGSN Global Configuration

configure > sgsn-global

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

Syntax Description

`congestion-control`

Usage Guidelines

Provides access to the congestion-action-profile configuration command.

Example

Open the SGSN Global Congestion Control configuration mode.

```
congestion-control
```

do show

Executes all **show** commands while in Configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax Description

```
do show
```

Usage Guidelines

Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character | is only available if the command is valid in the Exec mode.



Caution

There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

dscp-template

Creates and/or deletes DSCP templates that can be configured for use for all GPRS services on the SGSN and provides access to the DSCP Template configuration mode. This command is also supported on HNB-GW service to create a DSCP template.



Important

In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

Product

SGSN

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > SGSN Global Configuration

configure > sgsn-global

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

Syntax Description

```
dscp-template template_name [ -noconfirm ]
no dscp-template template_name
```

no

Deletes the template instance from the SGSN Global configuration.

template_name

Enter 1 to 64 alphanumeric characters, including dots (.), dashes (-), and forward slashes (/). to identify a unique instance of a DSCP template.

There is no known limit to the number of templates that can be created.

Usage Guidelines

This command enables the operator to create or delete an instance of a DSCP template and access the DSCP Template configuration mode. The DSCP templates are used to define the DSCP configuration for control packets and data packets for the GPRS services.

Related commands:

- This command provides access to the mode containing all the configuration commands used to define DSCP markings for the control packets and data packets for a particular GPRS service (see the *DSCP Template Configuration Mode Commands* section).
- To associated a specific DSCP template with a specific GPRS service configuration, for builds prior to release 14.0 use the **associate-dscp-template downlink** command and for builds in releases 14.0 and higher use the **associate dscp-template downlink**command. Both commands are documented in the *GPRS Service Configuration Mode Commands* section.
- To check the list of DSCP templates configured, use the **show sgsn-mode** command documented in the *Exec Mode Commands* section.

This command is also supported on HNB-GW service to create a DSCP template.

Related commands for HNB-GW:

- This command provides access to the mode containing all the configuration commands used to define DSCP markings for the control packets and data packets for a particular HNB-GW service (see the *DSCP Template Configuration Mode Commands* chapter).
- To associated a specific DSCP template with a system for a PSP instance in SS7 routing domain, use the **associate-dscp-template downlink** documented in the *SGSN PSP Configuration Mode Commands* chapter.

Example

Use a command similar to the following to create a DSCP template with ID *dscp_london* that can be used specifically for Gb/IP calls from subscribers in London:

```
dscp-template dscp_london
```

Following command creates a DSCP template with ID *dscp_hnb1* that can be used specifically for HNB-GW services on a chassis:

```
dscp-template dscp_hnb1
```

dual-address-pdp

This command makes it possible for the operator to enable (default) / disable SGSN support for MS requests for dual PDP type (IPv4v6) addressing.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > SGSN Global Configuration

configure > sgsn-global

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

Syntax Description

```
[ default | no ] dual-address-pdp
```

default

Enables dual PDP type address support.

no

Disables the default behavior so that the SGSN does not honor requests for dual PDP type addresses.

Usage Guidelines

With release 12.2 and in accordance with 3GPP Release 9.0 specifications, by default the SGSN honors the MS/UE request for dual PDP type addressing (IPv4v6) for PDP context association with one IPv4 address and one IPv6 address/prefix. This support can be disabled by configuration.



Important For the dual PDP addressing feature to function, **common-flags** must be enabled with the **gptc send** command in the SGTP service configuration mode *prior* to enabling the feature with the **dual-address-pdp** command.

With this default behavior, the operator has multiple options to refine the level of support for dual PDP type addressing through the use of several related commands.

- **dual-address-pdp** command in the RNC configuration mode disables SGSN support for dual PDP type addressing for a specific RNC that either does or does not support this type of addressing..
- **pdp-type-ipv4v6-override** in the APN profile configuration mode allows the SGSN to override the MS/UE request for dual PDP type addressing.
- Using the **dual-ipv4v6** keyword with the **wildcard-apn pdp-type** command in the APN remap table configuration mode enables the operator to configure a default APN with a wildcard subscription with PDP type IPv4v6.

Example

Use the following command to disable support for dual PDP type addressing (IPv4v6):

```
no dual-address-pdp
```

If dual PDP addressing has been disabled, to renable the feature, move to the SGTP service configuration mode, in the appropriate context, to perform the following as the *first* command needed to re-enable support for dual PDP type addressing in the configuration:

```
gtpc send common-flags
```

Now in the SGSN global configuration mode, use the following as the second command required to re-enable support for dual PDP type addressing in the configuration:

```
dual-address-pdp
```

ec-gsm

This command enables extended coverage class support on the SGSN.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > SGSN Global Configuration

configure > sgsn-global

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

Syntax

```
[ no ] ec-gsm
```

no

Disables EC-GSM support on the SGSN.

Usage Guidelines

Use this command to enable EC-GSM for all GPRS services on the SGSN.

eir-profile

Creates an EIR profile and provides access to the EIR profile configuration mode commands that define the parameters of the profile.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes Exec > Global Configuration > SGSN Global Configuration

configure > sgsn-global

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

Syntax Description

eir-profile *profile_name*
no eir-profile *profile_name*

no

Deletes an EIR profile from the SGSN Global configuration.

profile_name

Enter a unique name for the profile, upto 64 alphanumeric characters in length.

Usage Guidelines This command creates up to 16 instances of EIR profiles and provides access to the EIR Profile configuration mode for the commands to configure the EIR profile parameters.

Example

Remove the 'testing' EIR profile from the SGSN Global configuration mode:

no eir-profile testing

end

Exits the current mode and returns to the Exec Mode.

Product SGSN

Privilege Security Administrator, Administrator

Syntax Description **end**

Usage Guidelines Change the mode back to the Exec Mode.

exit

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

Product SGSN

Privilege Security Administrator, Administrator

Syntax Description **end**

Usage Guidelines Change the mode to the Global Configuration Mode.

gmm-message

This command configures the SGSN to discard (drop) the Attach-Request message received with a random TLLI already in use.

Product SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > SGSN Global Configuration

configure > sgsn-global

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

Syntax Description **`[ default ] gmm-message attach-with-tlli-in-use discard-message`**

default

Resets the default function allowing multiple MS, using the same random TLLI, to attempt to Attach simultaneously and disables discarding the Attach-Request message for random TLLI already in use.

Usage Guidelines Working with the two related commands (noted below), this command is part of a procedure for handling multiple MS Attaches all with the Same Random TLLI. Use this command to configure the SGSN to allow only one subscriber at a time to attach using a fixed random TLLI.

Related Commands:

- The **old-tlli invalidate tlli** command configures a list of random TLLI to be invalidated from the GMM after the invalidate old-TLLI timer expires.
- The **old-tlli hold-time** command configures the old-TLLI expiry timer.

Example

Configure the SGSN to drop Attach Request containing TLLI already in use:

```
gmm-message attach-with-tlli-in-use discard-message
```

gmm-sm-statistics



Important This command has been deprecated.

Product SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > SGSN Global Configuration

configure > sgsn-global

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

Syntax Description

```
gmm-sm-statistics attach-rejects cause network-failure only-internal
no gmm-sm-statistics attach-rejects
```

gprs-mocn

Enables or disables General Packet Radio Service (GPRS) Multi-Operator Core Network (MOCN). With 2G MOCN, the radio network is shared among different operators, while each operator maintains its separate core network.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > SGSN Global Configuration

configure > sgsn-global

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

Syntax Description

```
[ no ] gprs-mocn
```

no

Disables GPRS MOCN when it has been previously enabled.

Usage Guidelines

Use this command to enable 2G MOCN, which is disabled by default.

For complete information about the 2G (GPRS) MOCN feature and its configuration, refer to the *MOCN for 2G SGSN* feature section in the *Serving GPRS Support Node Administration Guide*

Example

The following command enables GPRS MOCN support for SGSN:

```
gprs-mocn
```

interface-management

This command creates an interface management configuration and provides access to the SGSN Interface Management configuration mode.

Product SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > SGSN Global Configuration

configure > sgsn-global

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

Syntax Description **`interface-management`**

Usage Guidelines Use this command to access the SGSN Interface Management configuration mode to map NSE-ID and NSE-name to the Gb interface and/or to lock and unlock interface by the NSE/BSC identifier.

Example

Access the SGSN Interface Management configuration mode:

`interface-management`

ipms-suppress

This command enables suppressing of the specified RAT related ipms event reporting.

Product SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > SGSN Global Configuration

configure > sgsn-global

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

Syntax Description

```
ipms-suppress [ gprs | umts ]
no ipms-suppress [ gprs | umts ]
```

no

Disables suppressing of the specified RAT related ipms event reporting.

gprs

This keyword enables suppressing of 2G related ipms-event reporting to the Intracer.

umts

This keyword enables suppressing of 3G related ipms-event reporting to the Intracer.

Usage Guidelines

This command is configured to suppress or allow the IPMS-event reporting to Intracer for the specified RAT. This CLI command helps the operator to change the IPMS-event reporting and manage network load or congestion on the fly.

Note

- At a time only service (either gprs or umts service) related ipms event reporting to the Intracer server (IPMS server) can be suppressed using the CLI command, provided there is a valid IPMS-context and server address.
- When no **ipms-suppress [gprs | umts]** is configured then regardless of the service provided the suppression enabled on the service (configured through **ipms-suppress [gprs | umts]**) will be disabled. There is no one-to-one mapping of the **ipms-suppress** and **no ipms-suppress**.
  - For example, if ipms-suppress on gprs is configured using the command **ipms-suppress gprs**. To remove ipms suppress, either of the commands **no ipms-suppress gprs** or **no ipms-suppress umts** can be used. However the command **no ipms-suppress gprs** is recommended in such a scenario.
- By default the IPMS event reporting will be done by both the services, provided there is a valid IPMS-context and IPMS-server configured.
- IPMS suppression can be enabled on both the services (GPRS and UMTS service) at the same time. This provides independent control on the suppression of ipms-events from the GPRS and UMTS services.

Example

Use this command to enable suppressing of 2G related ipms-event reporting to the Intracer:

```
ipms-suppress gprs
```

imsi-range

Configure an IMSI range with an optional PLMN ID to associate with an Operator Policy.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > SGSN Global Configuration

configure > sgsn-global

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

Syntax Description

```
imsi-range mcc mcc_num mnc mnc_num { msin first start_number last stop_number [
 operator-policy policy_name [ description description ] ] | plmnid plmn_id
operator-policy policy_name [ description description ] } +
no imsi-range mcc mcc_num mnc mnc_num { msin first start_number last stop_number
 | plmnid plmn_id }
```

no

Using **no** in the command deletes the definition from the SGSN Global configuration.

mcc *mcc_num*

mcc defines the mobile country code (MCC) of an IMSI.

mcc_num: Enter a 3-digit number from 100 to 999 - 000 to 099 are reserved.

mnc *mnc_num*

mnc defines the mobile network code (MNC) of an IMSI.

mnc_num: Enter a 2 or 3-digit number from 00 to 999.

msin

MSIN (mobile subscriber international number) portion of the IMSI.

first *start_num:* Defines first MSIN prefix number in a range

last *stop_num:* Defines the last or final MSIN prefix number in a range.

operator-policy *policy_name* description *description*

Identify the operator policy that the IMSI range definition and/or the PLMN-ID is to be associated.

policy_name : Enter a string of 1 to 64 alphanumeric characters.

description: Enter a string of 1 to 100 alphanumeric characters to provide range clarification for converted Release 9.0 configurations.

Description is just an information field. From release 19.0 onwards the length of the string supported for this field has been reduced, the supported range is now "1" up to "50" alphanumeric characters. The reduction of the supported string size results in improvement in boot up time.

If a PLMN-ID is to be included in the definition, enter the **plmnid** before entering the operator policy name.

plmnid *plmn_id*

The 5-6 digit PLMN-ID consists of the MCC (mobile country code) plus the MNC (mobile network code) to identify the public land mobile network (PLMN) for a specific operator. This keyword associates a specific PLMN with this specific SGSN operator policy.

plmn_id : Enter 5 to 6 digits.

+

This symbol indicates that command can be repeated to create repeated definitions.

Usage Guidelines

An IMSI = maximum of 15 digits. An IMSI consists of the MCC (3 digits) + the MNC (2 or 3 digits) + the MSIN (the remaining 10 or 9 digits depending on the length of the MNC).

MCC and MNC are the minimum amount of information required to identify a unique operator policy with IMSI filtering. The MCC and MNC combine uniquely to identify the country and the network operator, for example: Cingular Wireless in the United States = **mcc** *311***mnc** *180*

To improve the granularity of call handling, an operator policy with additional IMSI filtering parameters can be defined, to include filtering based on the MSIN, by defining a MSIN range - first (or start-of-range) MSIN and last (or end-of-range) MSIN. The range numbers do not include the maximum allowed for the MSIN but should include a sufficient number to enable the operator policy to filter effectively.

For the most efficient IMSI filter, the operator policy should include all of the above parameters and the PLMN ID which defines the current location of the MS -- this parameter is particularly useful for highlighting which calls are roaming.

And if none of the operator policies contain useful filtering information, then the default operator policy will be applied as the information in this command is never defined for the default operator policy.

The following table will illustrate how these filtering parameters determine which operator policy will govern a call:

Operator Policy ID	MCC	MNC	MSINfirst	MSINlast	PLMN ID
OpPol-1	123	45	67890	67898	
OpPol-2	123	45			
OpPol-3	123	45	67890	67898	23232
OpPol-4	123	45			23232
OpPol-5	123	45	6789012	6789019	
OpPol-6	123	45	6789012	6789019	23232
default					

The filtering selects which operator policy will be used to determine how a call is handled - the operator policy that best matches the IMSI. So, a call with IMSI 123456789012345 PLMNID 23232 is best matched with OpPol-6.

In most cases, the operator policy with the most information defined will be used as a combination of PLMNID and IMSI provides the best match. But OpPol-6 won't always be the best match. Using the table above:

OpPol-1 is the best match for IMSI 123456789011111

OpPol-2 is the best match for IMSI 123456789099999

OpPol-5 is the best match for IMSI 123456789012345 if the PLMNID is 12344

Example

The following associates operator policy *oppol1* with country code *310*, mobile network code of *33*, and IMSI range *1231234* - *1231244*:

```
imsi-range mcc 310 mnc 33 msin first 1231234 last 1231244 operator-policy
 oppol1
```

location-services

Enable or 'start' Location Services (LCS) on the SGSN.

Product SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > SGSN Global Configuration

configure > sgsn-global

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

Syntax Description

```
location-services
no location-services
```

no

Disables or 'stops' LCS on the SGSN.

Usage Guidelines By default, Location Services is not enabled on the SGSN. This command is mandatory to enable the SGSN to support LCS, which is a license-controlled feature. Multiple other commands are required to configure LCS functionality. For more information about the operation and configuration of LCS on the SGSN, refer to the *Location Services* section of the *SGSN Administration Guide*.

Example

Use the following command to disable Location Services once they have been enabled:

```
no location-services
```

map-message

This command instructs the SGSN to ignore the CAMEL subscription when there is no CAMEL service associated or in existence.

Product SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > SGSN Global Configuration

configure > sgsn-global

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

Syntax Description

```
map-message insert-subscriber-data csi-handling when-camel-not-associated
 ignore-subscription
default map-message insert-subscriber-data csi-handling
```

default

Resets the SGSN's default behavior. By default, the SGSN validates the CAMEL subscription and rejects an Attach Request when there is no CAMEL service association.

Usage Guidelines

By default, the SGSN updates the the CAMEL subscription included in the INSERT-SUBSCRIBER-DATA (ISD) messages received from the HLR. While processing the ATTACH request from the CAMEL subscriber, the SGSN checks whether it has a CAMEL service associated with the corresponding service (either GPRS service or SGN service). It drops the ATTACH request if there is no CAMEL service associated with a corresponding service.

Also by default, the SGSN does not allow establishment of a Direct Tunnel (DT) for a CAMEL subscriber. It strictly validates the subscriber against the CAMEL subscription during the Direct Tunnel setup procedure.

This command enables the operator to control the behavior of the SGSN by configuring the SGSN to ignore the CAMEL subscription. This allows the SGSN to successfully complete an ATTACH procedure when there is an ATTACH Request from a CAMEL subscriber and there is no CAMEL service association in the SGSN. As well, during the Direct Tunnel establishment, validation of the CAMEL subscription is ignored to allow the DT to setup when there is no CAMEL service association in the SGSN.

Example

Instruct the SGSN to validate the CAMEL subscription:

```
default map-message insert-subscriber-data csi-handling
```

max-pending-attaches

Configure the maximum length of the pending attach queue.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > SGSN Global Configuration

configure > sgsn-global

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

Syntax Description

max-pending-attaches *limit*
default max-pending-attaches

default

Resets the SGSN's Attach queue to a maximum pending value of 10,000.

limit

Set the a maximum limit to the pending Attach/RAU messages queue in the LinkMgr. When the limit is reached a message is sent to the IMSIMgr.

limit : Enter an integer from 5000 - 50000. Default is 10000.

Usage Guidelines

With this command, configure the maximum limit to the pending ATTACH/RAU messages queue in the LinkMgr. When the limit is reached, the LinkMgr sends the Query/Forward messages to the IMSIMgr.

As the IMSIMgr gets busier and does not responded to Query/Forward requests, the response to the requests will get slower and slower and the queue size continues inflating if the incoming message rate is high. To avoid this situation, set the **max-pending-attaches** for the pending queue for Attach and RAU messages. All other messages from the HLR will be added to the queue as they cannot be dropped. High and low watermarks are set to the queue at 80% of **max-pending-attaches "** and 60% of **max-pending-attaches** respectively.

Once a high watermark is reached, the new Attach and RAU requests are dropped and relevant statistics are incremented. Once a low watermark is hit, the new Attach/RAU requests are accepted and added to the pending queue. The entries are added to the pending queue only when the window-size between IMSIMgr and LinkMgr becomes zero. This is a very rare occurrence and will not affect the current behavior in normal circumstances.

Example

Set the queue length to a maximum of *15000* requests:

```
max-pending-attaches 15000
```

msisdn-group

This command configures the Mobile Subscriber Integrated Services Digital Network (MSISDN) group to which the operator policy should be associated.

Product

SGSN

Privilege

Administrator

Command Modes

Exec > Global Configuration > SGSN Global Configuration

configure > sgsn-global

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

Syntax Description

msisdn-group *group_name* **operator-policy** *policy_name*
no msisdn-group *group_name*

no

Deletes the configured MSISDN group.

msisdn-group *group_name*

Specifies the MSISDN group name to which the operator policy should be associated. *group_name* must be an alphanumeric string of 1 through 64 characters. It can have a maximum of 50 groups.

operator-policy *policy_name*

Specifies the operator policy to which the IMSI range should be associated with.

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

Usage Guidelines Use this command to specify the MSISDN group to which the operator policy should be associated.

msisdn-range

This command configures the MSISDN range to which operator policy should be associated.

Product SGSN

Privilege Administrator

Command Modes Exec > Global Configuration > SGSN Global Configuration

configure > sgsn-global

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

Syntax Description

msisdn-range cc *cc_value* **number first** *start_range* **last** *end_range* **operator-policy** *policy_name*

no msisdn-range cc *cc_value* **number first** *start_range* **last** *end_range* **operator-policy** *policy_name*

no

Deletes the specified MSISDN numbers.

cc *cc_value*

cc is the country code of MSISDN. *cc_value* is a 1 to 3 digit number.

number first *start_range* last *end_range*

Specifies the start and end of MSISDN (combination of Country Code (CC), National Destination Code (NDC) or Number Planning Area (NPA), and Subscriber Number (SN)).

operator-policy *policy_name*

Specifies the operator policy to which the IMSI range should be associated with.

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

Usage Guidelines Use this command to configure the MSISDN range to which operator policy should be associated.

Example

The following command configures the MSISDN with CC as *334* and MSISDN range as *918369110173* and *918369110184*, and then associates with operator policy *OP1*:

```
msisdn-range cc 334 number first 918369110173 last 918369110184
operator-policy op1
```

old-tlli invalidate tlli

This command configures a list of random TLLI to be invalidated (removed) from the GMM after the invalidate old-TLLI timer expires.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > SGSN Global Configuration

configure > sgsn-global

Entering the above command sequence results in the following prompt:

`[local]host_name(config-sgsn-global)#`

Syntax Description

`[ no ] old-tlli invalidate tlli` *`< hexadecimal >`*

no

Removes a single random TLLI from the configured list.

< hexadecimal >

Identifies a single random TLLI to be removed from the GMM after the old-TLLI timer expires.

Usage Guidelines

Use this command to create a list of up to 50 random TLLI to be dropped from the GMM after the old-TLLI timer expires. This command also starts the invalidate old-TLLI timer.

Important If the old-TLLI expiry timer is not configured with the **old-tlli hold-time** command, then the SGSN will only drop second Attach Requests using the same random TLLI already in use.

Related Commands:

- The **gmm-message** configures the SGSN to discard (drop) the Attach-Request message received with a random TLLI already in use
- The **old-tlli hold-time** command configures the old-TLLI expiry timer.

Example

Add random TLLI *0x7f05a30a* to the Invalidate List:

```
old-tlli invalidate tlli 0x7f05a30a
```

old-tlli hold-time

This command configures the old-TLLI expiry timer to be started in GMM when anyone of the listed random TLLI are received.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > SGSN Global Configuration

configure > sgsn-global

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

Syntax Description

[default] old-tlli hold-time *< seconds >*

default

Resets the timer to 5 seconds

< seconds >

Sets the numbers of seconds before the timer expires; range 1 to 125.

Usage Guidelines

Use this command to configure the old-TLLI expiry timer to be started in GMM when anyone of the listed random TLLI are received. If the timer expires prior to receiving Attach-Complete then the SGSN invalidates (removes) the TLLI from the GMM.



Important For this configuration to work, the list of random TLLI to be removed (invalidated) from the GMM must be defined with the **old-tlli invalidate tlli** command.

Related Commands:

- The **gmm-message** configures the SGSN to discard (drop) the Attach-Request message received with a random TLLI already in use
- The **old-tlli invalidate tlli** command configures the random invalidate TLLI list.

Example

Set the timer for *2* seconds:

```
old-tlli hold-time 2
```

pdp-deactivation-rate

Set the rate the SGSN deactivates PDP connections per second per SessMgr when GPT-C path failure is detected. Beginning with release 15.0, this command is also supported on the S4-SGSN.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > SGSN Global Configuration

configure > sgsn-global

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

Syntax Description

pdp-deactivation-rate { connected-ready *rate* **| idle-standby** *rate* **}**
default pdp-deactivation-rate { connected-ready | idle-standby }

default

If this keyword is used with the command, then the default deactivation rates are used.

connected-ready *rate*

Subscribers that are in the PMM-Connected / GPRS-Ready state and actively using the SGSN service need to be deactivated at a faster rate to facilitate the deactivation/re-activation process.

rate -sets the number of subscribers to be deactivated per second per SessMgr and the valid range is 1 to 1000 and the default is 760 connected-ready subscribers deactivated per second.

idle-standby *rate*

Subscribers that are in the PMM-Idle / GPRS-Standby state are not actively using the SGSN service and can be deactivated at a slower rate. The deactivation process for idle-standby subscribers includes paging before the Deactivate Request is sent.

rate - sets the number of subscribers to be deactivated per second per SessMgr and the valid range is 1 to 1000 and the default is 240 idle-standby subscribers deactivated per second.

Usage Guidelines

Use this command to define a rate at which the SGSN processes PDP deactivations when a GTP-C path failure is detected (and confirmed according to the SGSN's default behavior). The operator can use this command to set a deactivation rate that ensures radio network congestion is avoided.

Related commands:

- **max-remote-restart-counter-change** - allows the operator to set a maximum variance between stored and received values for restart counter changes coming from the GGSN. For details, refer to the SGSN Global configuration mode documentation.
- **disable-remote-restart-counter-verification** - allows the operator to disable the default behavior. For details, refer to this command in the SGSN Global configuration mode documentation.

Example

Use the following command to deactivate PDP connections for *600* PMM-Connected / GPRS-Ready subscribers per second:

```
pdp-deactivation-rate connected-ready 600
```

Use the following command to deactivate PDP connections for *320* PMM-Idle / GPRS-Standby subscribers per second:

```
pdp-deactivation-rate idle-standby 320
```

Use the following command to reset the default *760* per second deactivation rate for PMM-Connected / GPRS-Ready subscribers:

```
default pdp-deactivation-rate connected-ready
```

qos-arp-rp-map-profile

This command creates an instance of an ARP-RP Mapping Profile and/or access the ARP-RP Mapping Profile configuration mode commands.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > SGSN Global Configuration

configure > sgsn-global

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

Syntax Description

qos-arp-rp-map-profile *arp-rp_prof_name*
no qos-arp-rp-map-profile *arp-rp_prof_name*

no

Removes the specified ARP-RP Map Profile from the SGSN Global configuration.

arp-rp_prof_name

Enter a string of 1 to 64 alphanumeric characters to identify the mapping profile and moves into the ARP-RP mapping profile configuration mode. The ARP-RP Map Profiles need to be associated with the SGSN and/or GPRS Services.

Usage Guidelines

Using the ARP to RP mapping, the SGSN can choose a preferred radio priority according to the ARP values sent by the GGSN and HLR. As well, these mappings will be used by corresponding 2G and/or 3G services to choose the radio priority value while triggering messages (such as those listed below) towards the MS/UE:

- Activate PDP Accept.
- Modify PDP Request during network-initiated PDP modification procedure.

- Modify PDP Accept during MS-initiated PDP modification procedure provided the ARP has been changed by the network.

The profiles will be populated via the **arp** command under the ARP-RP Map Profile configuration mode.

Example

Create an ARP-RP Map Profile named *arprpmap1* using the following command:

```
qos-arp-rp-map-profile  arprpmap1
```

ranap excess-len ignore

Configure the SGSN to ignore excess length of received RANAP messages.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > SGSN Global Configuration

configure > sgsn-global

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

Syntax Description

```
[ default | no ] ranap excess-len ignore
```

default

Resets the default behavior - a decode error is generated when received RANAP messages are more than an extra octet in length.

no

Disables the configuration to ignore overly long RANAP messages.

Usage Guidelines

By default, the SGSN issues a decode error when the RANAP messages include extra octets. Use this command to ignore RANAP messages that have excess octets.

Example

Use the following command to enable the SGSN to ignore overly long RANAP messages:

```
ranap excess-len ignore
```

Use the following command to disable ignoring of RANAP messages that are excessive in length:

```
no ranap excess-len ignore
```

ran-information-management

Enable/disable RAN information management (RIM) support for the SGSN.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > SGSN Global Configuration

configure > sgsn-global

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

Syntax Description

`[ default | no ] ran-information-management`

default

Resets the default so RIM is disabled.

no

Disables the RIM support in the configuration file.

Usage Guidelines

By default, handling of RAN information management (RIM) messages is disabled. This command enables the SGSN to handle RIM messages. When this command is enabled and RIM message handling is enabled on the destination node, then RIM PDUs will be forwarded to the BSC/RNC. If RIM message handling is not enabled on both nodes, then the RIM PDUs will be dropped silently.

Confirm RIM configuration with the **show sgsn-mode** command in the Exec mode.

Example

Use the following command to enable RIM support:

`ran-information-management`

Use the following command to disable RIM support that has been added to the configuration:

`no ran-information-management`

target-offloading

Selects the subscriber offloading algorithm to be applied to the SessMgr and the IMSIMgr.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > SGSN Global Configuration

configure > sgsn-global

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

Syntax Description

```
target-offloading algorithm [ optimized-for-speed |
optimized-for-target-count ]
default target-offloading algorithm
```

default

Resets the configuration to default values.

optimized-for-speed

Enables faster algorithm to achieve the target count.

optimized-for-target-count

Enables a reliable algorithm to achieve the target count.

Default.

Usage Guidelines

With the SGSN's distributed architecture, there are many SessMgrs and offloading will happen in parallel at all SessMgrs. This command enables the operator to control the total number of subscribers being offloaded.



Important The value for this command can not be altered once dynamic offloading has begun - refer to the command description for the **sgsn-offload** command in the *Exec Mode* chapter..

Example

Set the SGSN to use the faster algorithm for offloading:

```
target-offloading algorithm optimized-for-speed
```

tlli-cb-audit

This command enable (default is disabled) or disables a periodic (hourly) audit of TLLI-CBs in the BSSGP layer.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > SGSN Global Configuration

configure > sgsn-global

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

Syntax Description

```
tlli-cb-audit
[ default | no ] tlli-cb-audit
```

default

Include **default** with the command to disable the audit function.

no

Include **no** with the command to disable the audit function.

Usage Guidelines

This command is used to clean-up hanging or unassociated TLLI in the BSSGP layer. This configuration defined with this command will be common to all NSE configured for this SGSN.

Independent of this command configuration, the SGSN triggers and audit when the number of TLLI-CBs reaches 35,000.

Example

Use the following command to enable the hourly audit for unassociated TLLl-CBs:

```
tlli-cb-audit
```

umts-aka-r99

This command enables the operator to authenticate mobile equipment (MEs) with R99+ USIMs and capable of UMTS AKA.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > SGSN Global Configuration

configure > sgsn-global

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

Syntax Description

```
umts-aka-r99
no umts-aka-r99
```

no

Including **no** with the command disables the authentication.

Usage Guidelines

This command enables operators to authenticate MEs that are attempting to connect to a 2.5G network with R99+ USIMs if the MEs are UMTS AKA capable. For R99 mobiles, the SGSN will continue to perform GSM AKA even if quintuplets are received fromthe HLR.

Example

Use the following command to disable UMTS AKA authentication for MEs with R99+ USIMs:

```
no umts-aka-r99
```