## CONTENTS

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About this Guide</td>
<td>v</td>
</tr>
<tr>
<td>Conventions Used</td>
<td>vi</td>
</tr>
<tr>
<td>Contacting Customer Support</td>
<td>viii</td>
</tr>
<tr>
<td>Affected Document(s)</td>
<td>9</td>
</tr>
<tr>
<td>Card Configuration Mode Commands</td>
<td>11</td>
</tr>
<tr>
<td>framing</td>
<td>12</td>
</tr>
<tr>
<td>GPRS Service Configuration Mode Commands</td>
<td>13</td>
</tr>
<tr>
<td>llc</td>
<td>14</td>
</tr>
<tr>
<td>Gs Service Configuration Mode Commands</td>
<td>17</td>
</tr>
<tr>
<td>non-pool-area</td>
<td>18</td>
</tr>
<tr>
<td>pool-area</td>
<td>19</td>
</tr>
<tr>
<td>HLR Configuration Mode Commands</td>
<td>21</td>
</tr>
<tr>
<td>imsi</td>
<td>22</td>
</tr>
<tr>
<td>IuPS Service Configuration Mode Commands</td>
<td>23</td>
</tr>
<tr>
<td>relocation-aloc-timeout</td>
<td>24</td>
</tr>
<tr>
<td>reset</td>
<td>25</td>
</tr>
<tr>
<td>tigoc-timeout</td>
<td>26</td>
</tr>
<tr>
<td>tinct-timeout</td>
<td>27</td>
</tr>
<tr>
<td>SCCP Network Configuration Mode Commands</td>
<td>29</td>
</tr>
<tr>
<td>hop-count</td>
<td>30</td>
</tr>
<tr>
<td>SGSN Global Configuration Mode Commands</td>
<td>31</td>
</tr>
<tr>
<td>aggregate-ipc-msg</td>
<td>32</td>
</tr>
<tr>
<td>bssgp-message</td>
<td>33</td>
</tr>
<tr>
<td>max-pending-attaches</td>
<td>34</td>
</tr>
<tr>
<td>umts-aka-r99</td>
<td>35</td>
</tr>
<tr>
<td>SGSN Operator Policy</td>
<td>37</td>
</tr>
<tr>
<td>access-restriction-data</td>
<td>38</td>
</tr>
<tr>
<td>gtp send</td>
<td>40</td>
</tr>
<tr>
<td>rau-inter-plmn</td>
<td>41</td>
</tr>
<tr>
<td>srns-intra</td>
<td>44</td>
</tr>
<tr>
<td>SGTP Service Configuration Mode Commands</td>
<td>45</td>
</tr>
<tr>
<td>ignore-remote-restart-counter-change</td>
<td>46</td>
</tr>
<tr>
<td>SMS Service Configuration Mode Commands</td>
<td>47</td>
</tr>
<tr>
<td>smsc-routing</td>
<td>48</td>
</tr>
</tbody>
</table>
About this Guide

This document pertains to the features and functionality that run on and/or that are related to the Cisco® ASR 5000 Chassis, formerly the Starent Networks ST40.
Conventions Used

The following tables describe the conventions used throughout this documentation.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Notice Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Information Note Icon" /></td>
<td>Information Note</td>
<td>Provides information about important features or instructions.</td>
</tr>
<tr>
<td><img src="image" alt="Caution Icon" /></td>
<td>Caution</td>
<td>Alerts you of potential damage to a program, device, or system.</td>
</tr>
<tr>
<td><img src="image" alt="Warning Icon" /></td>
<td>Warning</td>
<td>Alerts you of potential personal injury or fatality. May also alert you of potential electrical hazards.</td>
</tr>
<tr>
<td><img src="image" alt="Electro-Static Discharge Icon" /></td>
<td>Electro-Static Discharge (ESD)</td>
<td>Alerts you to take proper grounding precautions before handling a product.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Typeface Conventions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Text represented as a screen display</td>
<td>This typeface represents displays that appear on your terminal screen, for example: Login:</td>
</tr>
<tr>
<td>Text represented as commands</td>
<td>This typeface represents commands that you enter, for example: show ip access-list This document always gives the full form of a command in lowercase letters. Commands are not case sensitive.</td>
</tr>
<tr>
<td>Text represented as a command variable</td>
<td>This typeface represents a variable that is part of a command, for example: show card slot_number slot_number is a variable representing the desired chassis slot number.</td>
</tr>
<tr>
<td>Text represented as menu or sub-menu names</td>
<td>This typeface represents menus and sub-menus that you access within a software application, for example: Click the File menu, then click New</td>
</tr>
</tbody>
</table>

Command Syntax Conventions

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>This typeface represents displays that appear on your terminal screen, for example: Login:</td>
</tr>
<tr>
<td>This typeface represents commands that you enter, for example: show ip access-list This document always gives the full form of a command in lowercase letters. Commands are not case sensitive.</td>
</tr>
<tr>
<td>This typeface represents a variable that is part of a command, for example: show card slot_number slot_number is a variable representing the desired chassis slot number.</td>
</tr>
<tr>
<td>This typeface represents menus and sub-menus that you access within a software application, for example: Click the File menu, then click New</td>
</tr>
</tbody>
</table>
## Command Syntax Conventions

<table>
<thead>
<tr>
<th>Command Syntax Conventions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>{keyword or variable}</code></td>
<td>Required keywords and variables are surrounded by grouped brackets. Required keywords and variables are those components that are required to be entered as part of the command syntax.</td>
</tr>
<tr>
<td><code>[keyword or variable]</code></td>
<td>Optional keywords or variables, or those that a user may or may not choose to use, are surrounded by square brackets.</td>
</tr>
</tbody>
</table>

|  | With some commands there may be a group of variables from which the user chooses one. These are called alternative variables and are documented by separating each variable with a vertical bar (also known as a pipe filter). Pipe filters can be used in conjunction with required or optional keywords or variables. For example: |
|  | `{ nonce | timestamp }` |
|  | OR |
|  | `[count number_of_packets | size number_of_bytes ]` |
Contacting Customer Support

Use the information in this section to contact customer support.

**For New Customers:** Refer to the support area of http://www.cisco.com for up-to-date product documentation or to submit a service request. A valid username and password is required to this site. Please contact your local sales or service representative for additional information.

**For Existing Customers with support contracts through Starent Networks:** Refer to the support area of https://support.starentnetworks.com/ for up-to-date product documentation or to submit a service request. A valid username and password is required to this site. Please contact your local sales or service representative for additional information.

---

**Important:** For warranty and repair information, please be sure to include the Return Material Authorization (RMA) tracking number on the outside of the package.
Chapter 1

Affected Document(s)

This addendum provides additions and modifications to filters, keywords, and commands in various configuration modes specific to Release 9.0 command line interface for the Cisco ASR 5000 SGSN.

Documentation updates provided in this addendum pertain to the documents listed in the following table and correspond to the stated release date(s):

<table>
<thead>
<tr>
<th>Document</th>
<th>Part Number</th>
<th>Release Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco ASR 5000 Series Command Line Interface Reference: Version 8.x and 9.0</td>
<td>OL-22947-02</td>
<td>September 30, 2010</td>
</tr>
<tr>
<td>Release 8.x to Release 9.0 Change Reference</td>
<td>OL-22957-02</td>
<td>09-30-2010</td>
</tr>
</tbody>
</table>
Chapter 2
Card Configuration Mode Commands

A new keyword has been added to the `framing` command. Details are provided in this section.
framing

The **ss-bits** keyword has been added to this command.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
framing sdh [ ds1 | e1 ] [ ss-bits ]
```

- **sdh [ ds1 | e1 ] [ ss-bits ]**
  - **ss-bits** - use this keyword to include ss bits in the message headers.

**Usage**

This new keyword enables/disables the use of ss bits in the AU pointer (per ITU 1997 G.783 specification) for an SDH configured line card - either an OLC2 or a CLC2. The ss-bits identify payload for transmissions via an SDH card.

**Example**
Enable the use of ss bits for signaling over all E1 interfaces on this SDH-configured line card:

```
framing sdh e1 ss-bits
```
Chapter 3
GPRS Service Configuration Mode Commands

Two new keywords have been added to the `llc` command in this configuration mode. Details for each of these new keywords are provided in this section.
Two new keywords, documented below, have been added to this command.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
llc { nu-overflow-detection high-watermark high_num low-watermark low_num
increment-oc  | reset-vur }
[ default | no ] { nu-overflow-detection | reset-vur }
```

- **default**
  - Resets the configuration to the default values.

- **no**
  - Disables the specified timer.

- **nu-overflow-detection high-watermark high_num low-watermark low_num
increment-oc**
  - Enables/disables overflow detection for the N(U) counter and setting overflow high/low thresholds facilitates ciphering synchronization between the MS and SGSN.
  - `high_num`: Enter an integer between 1 and 511.
  - `low_num`: Enter an integer between 0 and 510.
  - If the expected value of nu(Vur) is greater than or equal to the configured high-watermark, and the received nu(LFN) is less than or equal to the configured low-watermark, the SGSN increments the overflow counter (VurOC).
  - The recommended overflow settings are as follows: `llc nu-overflow-detection high-watermark 496 low-watermark 15 increment-oc` While expecting a packet with 496 &lt;= nu &lt;= 511 and a packet with 0 &lt;= nu &lt;= 15 is received, overflow is detected and VurOC is incremented.

- **reset-vur**
  - Enables/disables the mechanism to reset the Vur value maintained at LLC if the intra RAU request is received with N(U) = 0
  - Default: Disabled

**Usage**

This command configures the Vur (expected N(U) value and the VurOc (overflow counters for Vur) for the logical link control (LLC) sub-layer.

When these two new keywords are configured, statistics for related traffic can be viewed in the output of the `show llc statistics verbose` command.

**Example**

Use this command to reset the default for the N(U) overflow detection:
default llc nu-overflow-detection

Change the N(U) overflow thresholds to have counters increment when the low-watermark threshold of 12 is crossed:

```
llc nu-overflow-detection high-watermark 496 low-watermark 12 increment-oc
```
Chapter 4
Gs Service Configuration Mode Commands

Keywords, for commands `pool-area` and `non-pool-area` in this configuration mode, have been modified since the last release of the 8.x and 9.0 CLI Reference. Details for each of these changes are provided in this section.
non-pool-area

The `lac` keyword has been added to the `no` command and the maximum number of definable LACs has been increased.

### Product
SGSN

### Privilege
Security Administrator, Administrator

### Syntax

```plaintext
non-pool-area non_pool_name { use-vlr vlr_name lac lac_num }
no non-pool-area non_pool_name [ lac lac_num ]
```

- **no**
  Removes the configured non-pool area from this Gs service.

- **lac lac_num**
  This keyword can now be included with the `no` form of the command to enable operators to remove a specific configured LAC from the non-pool area configuration.
  `lac_num` is the LAC value and must be an integer value from 1 through 65535.

### Usage
This command creates a non-pool area for a set of subscriber location area codes (LACs) that can be used with a specific VLR for the Gs service.

It is now possible to define up to 128 LACs to be configured for the combined `non-pool-area` and `pool-area` configurations per Gs service.

### Example
Use this command to remove LAC 355 from a specific non-pool-area configuration:

```plaintext
no non-pool-area 2 lac 355
```
**pool-area**

This command creates a pool area configuration for a set of subscriber location area codes (LAC) that can be used with a specific VLR for the Gs service.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
pool-area pool_name
```

**Usage**

It is now possible to define up to 128 LACs to be configured for the combined `non-pool-area` and `pool-area` configurations per Gs service.
Chapter 5
HLR Configuration Mode Commands

A new filter has been added to the `mobile-global-title` keyword in the `imsi` command. Details for the change are provided in this chapter.
imsi

The **max-gt-address-len** filter has been added to the **mobile-global-title** keyword in this command.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] imsi { any | starts-with prefix_number mobile-global-title mgt_number [ max-gt-address-len max_gt_address ]
```

Defines the mobile global title address that the MCC/MNC portion of the IMSI will be converted to. If the maximum GT address length is specified (optional) and if the length of the MGT string is greater than defined, then the least significant digits will be omitted.

`mgt_number` is a string of digits, up to 18 digits in length.

`max_gt_address_len` is an integer from 1 to 32.

**Usage**

The new **max-gt-address-len** sets the maximum length of the global title address for the mobile global title (MGT) format. If the converted MGT string (replacement of the MCC/MNC portion of the IMSI with the mgt-string) length is greater than the length specified by the **max-gt-address-len**, then the least significant digits are omitted from the newly converted MGT address.

**Example**

Use this command to limit the GT address length to 26 digits:

```
imsi starts-with 20243 mobile-global-title123456789 max-gt-address-len 26
```
Chapter 6
IuPS Service Configuration Mode Commands

One new timer has been added and several timers have had their ranges expanded and their defaults increased. Details are available in this chapter.
relocation-alloc-timeout

This new command defines the amount of time the SGSN waits for a Relocation Request message.

**Product**  
SGSN

**Privilege**  
Security Administrator, Administrator

**Syntax**

```
relocation-alloc-timeout timeout_value
```

default relocation-alloc-timeout

---

default

 Resets the configuration to a 5 second wait time.

---

timeout_value

Time in seconds that the SGSN waits to receive a Relocation Request message.  
**timeout_value**: Must be an integer from 1 to 60. Default: 5 seconds.

**Usage**

Use this command to configure the number of seconds the SGSN will wait for a Relocation Request message to be received. This timeout needs to be set with sufficient time so that SRNS procedure aborts can be avoided if the peer fails to respond in a timely fashion in the case of a hard handoff.

**Example**

The following command sets the wait time to 10 seconds.

```
relocation-alloc-timeout 10
```
reset

The two timers listed below have had their timeout ranges expanded.

**Product**  
SGSN

**Privilege**  
Security Administrator, Administrator

**Syntax**

```plaintext
reset { ack-timeout time | guard-timeout time }  
default reset { ack-timeout | guard-timeout }
```

**default**
Returns to the default settings for the Reset procedure.

**ack-timeout time**
Configures the interval (in seconds) for which the SGSN waits for RESET-ACK from the RNC.  
`time` must be an integer and the range has expanded from 5 - 10 to 5 - 60. 
Default: has been increased to 20 seconds.

**guard-timeout**
Configures the interval (in seconds) after which the SGSN sends RESET-ACK to the RNC.  
`time` must be an integer and the range has expanded from 5 - 10 to 5 - 60. 
Default: 10

**Usage**
This command defines the configuration for various timers used as part of the the Reset procedure. The command can be repeated to set each of the timers separately.

**Example**
The following command sets a maximum wait time of 10 seconds for an acknowledgement from the RNC:

```plaintext
reset ack-timeout 10
```
tigoc-timeout

This command configures the TigOc interval. The interval options have increased to the new values indicated below.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
tigoc-timeout time
```

- `time`
  
  Set the number of seconds the SGSN is to wait.
  
  `time` must be an integer and the range has expanded from 1 - 10 to 1 - 60.

**Usage**

Define the amount of time that the SGSN ignores any overload messages for TigOc interval after receiving one overload message from the RNC.

**Example**

Use the following command to change the default TigOc interval to 4 seconds:

```
tigoc-timeout 4
```
**tintc-timeout**

This command configures the TinTc interval. The interval options have increased to the new values indicated below.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
tintc-timeout time
```

*time*

Set the number of seconds to wait. 
*time* must be an integer and the range has expanded from 1 - 10 to 1 - 60. Default: has been increased to 30 seconds.

**Usage**
Define the number of seconds that the SGSN waits before decrementing (by one) the traffic level of the RNC.

**Example**
Use the following command to set the TinTc interval to 4 seconds:

```
tintc-timeout 4
```
Chapter 7
SCCP Network Configuration Mode Commands

The hop-count command has been modified. Details are available in this chapter.
hop-count

The maximum number of hop counts possible has been increased.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

gop-count hop_cnt

hop_cnt

Define the maximum number of hop counts to allow for this SCCP network.

hop_cnt must be an integer; the range has been expanded (from 1 - 5) to 1 - 15.

Usage
This command specifies the maximum number of hops, for processing by network elements, for SCCP messages to avoid message looping.

Example
The following sets the maximum hop count to 10:

hop-count 10
Chapter 8
SGSN Global Configuration Mode Commands

Four new commands have been added to this configuration mode since the last release of the 8.x and 9.0 CLI Reference. Details for each of these new commands are provided in this section.
aggregate-ipc-msg

Enables/disables aggregation of IPC messages in the linkmgr and sessmgr.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

aggregate-ipc-msg { linkmgr | sessmgr } { flush-frequency frequency | num-msgs number_msgs }

default aggregate-ipc-msg { linkmgr | sessmgr }

default
Resets the managers to default values for flushing.

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.

flush-frequency frequency
Configure the frequency, in 100-millisecond intervals, that the aggregated IPC messages will be flushed. 

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.

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

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

Example
Configure the SGSN to buffer 45 messages before flushing the linkmgr IPC messages:

aggregate-ipc-msg linkmgr flush-frequency 45
bssgp-message

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

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
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**

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
```
max-pending-attaches

Configure the maximum length of the pending attach queue.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

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 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

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
**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

**Syntax**

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

Including `no` with the command disables the authentication.

**Usage**
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 from the HLR.

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

```
no umts-aka-r99
```
Chapter 9
SGSN Operator Policy

This chapter identifies the changes to the commands and keywords in the SGSN Operator Policy configuration mode since the last 8.x/9.0 CLI Reference publication.
access-restriction-data

This new command enables the operator to assign a failure code to be included in reject messages if attach rejection is due to access restriction data (ARD) checking in incoming subscriber data (ISD) messages. As well, the operator can disable the ARD checking behavior.

Product  
SGSN

Privilege  
Security Administrator, Administrator

Syntax

access-restriction-data { failure-code cause_code | no-check }

remove access-restriction-data failure-code

remove

Removes the failure code setting for the reject message that could result from ARD checking.

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 (information has been taken 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.

**Usage**

By default, the SGSN checks access restriction data (ARD) in 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.

**Example**

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

```
access-restriction-data no-check
```
gtp send

A new optional filter has been added to the imeisv keyword in this command.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
gtp send imeisv [ derive-imeisv-from-imei ]
no gtp send imeisv
```

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disables the configuration specified with the new optional filter.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>imeisv</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instructs the SGSN to include the IMEISV (international mobile equipment identity (and software version) of the mobile when sending GTP messages of the type “Create PDP Context Request”.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>derive-imeisv-from-imei</th>
</tr>
</thead>
<tbody>
<tr>
<td>This is a new 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.</td>
</tr>
</tbody>
</table>

Usage
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 operator policy is applied.

Example
The following command instructs the SGSN to send the GGSN the IMEI-SV based on the IMEI:

```
imeisv derive-imeisv-from-imei
```
rau-inter-plmn

This new command enables/disables restrictions for all RAUs occurring between different PLMNs, 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

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```bash
rau-inter-plmn access-type { all | location-area-list instance instance } { failure-code fail_code | user-device-release { before-r99 | 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 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 (information has been taken 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 - Sync 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. 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

Use this command to configure the restrictions and function of the inter-RAU procedure.

Example

default rau-inter allow access-type gprs location-area-list instance 1
**srns-intra**

The `default` command has been modified. The `failure-code` filter has been added to the `all` keyword.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
default srns-intra { all failure-code | location-area-list instance }
```

```
default srns-intra all failure-code
```

Resets the configuration to use a single default failure-code for all intra-SRNS relocations.

**Usage**

This command configures parameters relevant to the intra-SRNS (Serving Radio Network Subsystem) relocation procedure. With the `failure-code` filter appended to the `all` keyword in the `default` command, it is possible to reset the configuration to use a single failure-code for all intra-SRNS relocations.

**Example**

Set the default failure-code:

```
default srns-intra all failure-code
```
Chapter 10
SGTP Service Configuration Mode Commands

A new command has been added to the SGTP service configuration mode. Details are provided in this chapter.
ignore-remote-restart-counter-change

This new command can instruct the SGSN to ignore (not process) restart counters received from remote nodes.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
ignore-remote-restart-counter-change
[ default | no ] ignore-remote-restart-counter-change
```

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Default is to process restart counters received from remote nodes.</td>
</tr>
<tr>
<td>no</td>
<td>Disables the ignore change instruction.</td>
</tr>
</tbody>
</table>

**Usage**
This command is an on-off switch to instruct the SGSN to refrain from taking specific action (ignore) when there is a change in the restart counter at a remote node. Whether or not the changes to the remote node restart counters are processed, restart counters are tracked and the results are viewable in the output of the `show sgtp-service ggsn-table`. 

**Example**
Use the following command to instruct the SGSN not to process changes in the remote node’s restart counter:

```
ignore-remote-restart-counter-change
```
A new filter has been added to the `mobile-global-title` keyword in the `smsc-routing` command. Details for the change are provided in this chapter.
smsc-routing

The max-gt-address-len filter has been added to the mobile-global-title keyword in this command.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
smsc-routing { any | imsi-starts-with prefix_number mobile-global-title
    mgt_number [ max-gt-address-len max_gt_address ]
```

```
mobile-global-title mgt_number [ max-gt-address-len max_gt_length ]
```

Defines the mobile global title address that the MCC/MNC portion of the IMSI will be converted to. If the maximum GT address length is specified (optional) and if the length of the MGT string is greater than defined, then the least significant digits will be omitted.

mgt_number is a string of digits, up to 18 digits in length.

max_gt_address_len is an integer from 1 to 32.

Usage

The new max-gt-address-len sets the maximum length of the global title address for the mobile global title (MGT) format. If the converted MGT string (replacement of the MCC/MNC portion of the IMSI with the mgt-string) length is greater than the length specified by the max-gt-address-len, then the least significant digits are omitted from the newly converted MGT address.

Example

Use this command to limit the GT address length to 26 digits:

```
smsc-routing imsi-starts-with 20243 mobile-global-title123456789 max-gt-address-len 26
```