Cisco ASR 5000 Series Command Line Interface Reference Addendum

Version 12.0

Last Updated December 15, 2011

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

Reorient or relocate the receiving antenna.

Increase the separation between the equipment and receiver.

Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB’s public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco ASR 5000 Series Command Line Interface Reference Addendum

CONTENTS

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.

Icon	Notice Type	Description
i	Information Note	Provides information about important features or instructions.
!	Caution	Alerts you of potential damage to a program, device, or system.
⚡	Warning	Alerts you of potential personal injury or fatality. May also alert you of potential electrical hazards.
⚠	Electro-Static Discharge (ESD)	Alerts you to take proper grounding precautions before handling a product.

Typeface Conventions	Description
Text represented as a `screen display`	This typeface represents displays that appear on your terminal screen, for example: `Login:`
Text represented as **`commands`**	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.
Text represented as a **`command`** *`variable`*	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.
Text represented as menu or sub-menu names	This typeface represents menus and sub-menus that you access within a software application, for example: Click the **File** menu, then click **New**

Command Syntax Conventions	Description
{ **`keyword`** or *`variable`* }	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.

Command Syntax Conventions	Description
[**keyword** or *variable*]	Optional keywords or variables, or those that a user may or may not choose to use, are surrounded by square brackets.
|	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 Documents

This addendum provides new and/or expanded information pertaining to the CLI command documentation delivered as part of the 12.0 releases.

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

Document	Part Number	Release Date
Cisco ASR 5000 Series Command Line Interface Reference: Version 12.x	OL-25190-02	September 30, 2011

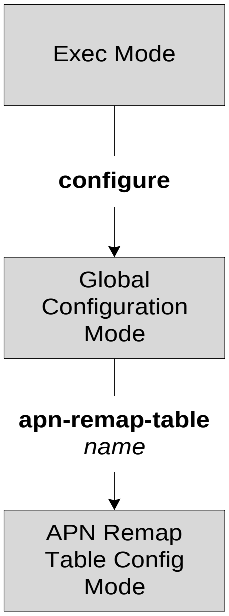
Chapter 2
APN Remap Table Configuration Mode

APN Remap Table configuration mode provides the commands to configure parameters for multiple features related to APN handling. A new set of keywords, for the **cc** command, have been added to enable APN remapping based on charging characteristics. Command and syntax details are available in this section.

APN remap table is a key element of the Operator Policy feature and a table is not usable (valid) until it has been associated with an operator policy (see *Operator Policy Configuration Mode Commands* chapter.)

When this mode is accessed, the command prompt should be similar to:

```
[local]asr5000(apn-remap-table<table_id>)#
```



cc

This command defines APN remapping behavior so that remapping occurs based on the charging characteristics value.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
cc behavior bit_value profile index_bit apn-remap network-identifier apn_net_id
new-ni new_apn_net_id

no cc behavior bit_value profile index_bit apn-remap network-identifier
apn_net_id
```

no

Disables the configured remapping behavior.

behavior*bit_value*

Specify the bit value for the behavior bit for the charging characteristic.
bit_value must be a hex value from 0x0 to 0xFFFF.

profile *index_bit*

This keyword sets the SGSN operator policy to use a profile index for the charging characteristics when the HLR does not provide a value for this.
index_bit must be an integer value from 1 through 15.
Some of the index values are predefined according to 3GPP standard:

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

apn-remap network-identifier *apn_net_id*

Identifies the 'old' APN network identifier that is being mapped for replacement.
apn_net_id : Enter a string of 1 to 62 alphanumeric characters, including dots (.) and dashes (-) .

new-ni *new_apn_net_id*

Identifies the 'new' APN network identifier that is being mapped to.
new_apn_net_id : Enter a string of 1 to 62 alphanumeric characters, including dots (.) and dashes (-) .

Usage

Use this command to enable APN remapping only when the charging characteristic value in the subscription record associated with the requested APN matches the value configured for the **new-ni** .

The new APN NI must be part of the subscription data so that the charging characteristic associated with the new APN NI will be used for activating the context and if there isn't one associated then the general charging characteristic will be used.

Example

The following command associates a new APN NI 'locals1' with a set of charging characteristics:

```
cc behavior 0xF  profile 4 apn-remap network-identifier homer1 new-ni
locals1
```

Chapter 3
DHCP Service Configuration Mode Commands

A new CLI has been introduced to skip the client hardware address (chaddr) validation performed on DHCPACK Message. This is required because some of the corporate DHCP servers in the field are not compliant with RFC 2131 and are not sending exact chaddr in DHCPACK message as it has received in DHCPREQUEST message. Configuring "**`no dhcp chaddr-validate`**" CLI will ensure that the chaddr field in DHCPACK is not validated and call is successfully established. Existing default behaviour is to perform chaddr validation and if mismatch is detected call is gets rejected.

Important: DHCPACK message is the response message sent from the server selected in the DHCPREQUEST message and is the combination of CHADDR (also known as client identifier) and assigned network address.

dhcp chaddr-validate

This command configures behavior of the client hardware address (chaddr) validation in DHCP messages.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

```
[ default | no ]dhcp chaddr-validate
```

`default`

This keyword enables the default functionality of validating chaddr value received in DHCPACK message with chaddr value sent in DHCPREQUEST message.

`no`

This keyword disables the functionality of validating the chaddr value received in DHCPACK message with chaddr value sent in DHCPREQUEST message.

Important: Chaddr information value in the DHCPACK message will be parsed and not be validated against the value maintained with client. Chaddr information value in DHCPACK will be ignored and will not be stored internally anywhere.

Usage

Use this command to configure behavior relating to the validation of chaddr information validation in the DHCPACK messages.

Example

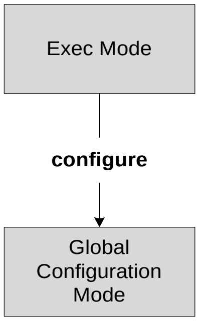
The following command specifies that the chaddr will not be validated in the DHCP messages:

```
no dhcp chaddr-validate
```

Chapter 4 Global Configuration Mode Commands

The SGSN's **`network-overload-protection`** command has been modified. New keywords define the queue size for buffering and message age-out wait-time for optimized network overload protection. This section contains command and syntax details.

The Global Configuration Mode is used to configure basic system-wide parameters.



network-overload-protection

This command configures an attach rate throttle mechanism to control the number of new connections (attaches or inter-SGSN RAUs), through the SGSN, on a per second basis.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
network-overload-protection sgsn-new-connections-per-second #_new_connections
action { drop | reject with cause { congestion | network failure } } [ queue-
size queue_size ] [ wait-time wait_time ]

default network-overload-protection sgsn-new-connections-per-second
```

default

Using **default** in the command, disables this attach rate throttle feature that provides network overload protection.

sgsn-new-connections-per-second *#_new_connections*

Define the number of new connections to be accepted per second.
#_new_connections: Must be an integer from 50 to 5000.

action

Specifies the action to be taken by the SGSN when the attach rate exceeds the configured limit on the number of attaches. Select one of the following actions:

- **drop:** Drop the new connection request.
- **reject-with-cause:** Reject the new connection request. Include one of the following as the cause in the reject message:
- **congestion**
- **network failure**

queue-size *queue_size*

Defines the maximum size of the pacing queue used for buffering the packets. If configured, the queue-size should be greater than or equal to the *#_new_connections* value and less than or equal to the optimal value (the *wait_time* * *#_new_connections*). This validation is done in the CLI.
queue_size Must be an integer from 250 to 25000.
Default: unconfigured. The default value is the *#_new_connections * wait-time*. This will be the optimal value.

wait-time *wait_time*

Defines the maximum life-time (number of seconds) of the packets in the queue beyond which the packets are considered to be “stale”.
wait_time Must be an integer from 1 to 15

Default: 5

Usage

Use this command to configure the rate at which the SGSN must process new connection requests. The rate is the number of new connections to be accepted per second.

With basic network overload protection, the incoming new connection rate is higher than this configured rate. When this occurs, all of the new connection requests cannot be processed. This command can also be used to configure the action to be taken when the rate limit is exceeded. The new connection requests, which cannot be processed, can be either dropped or rejected with a specific reject cause.

The SGSN's *optimized* network overload protection performs attach-rate throttling to avoid overloading Gr, Gn and Gf interfaces. This is enabled with **queue-size** and **wait-time** keywords so that the IMSIMgr throttles the attach rate to values configured with these keywords.

If the SGSN receives more than the configured number of attaches in a second, then the attaches are buffered in the pacing queue and requests are only dropped when the buffer overflows due to high incoming attach rate. Messages in the queue are processed (FIFO) until they age-out when the queued message's lifetime crosses the configured wait-time. The wait-time and the attach rate decide the optimal size of the queue.

Counters for this feature are available in the **show gmm-sm statistics** command display in the Network Overload Protection portion of the table.

Example

Configure the throttle rate or limit to 2500 attaches per second and to drop all requests if the limit is exceeded.

```
network-overload-protection sgsn-new-connections-per-second 2500 action
drop
```

Disables the network-overload protection feature and set the default queue size to 1000 and the wait time to 5 seconds:

```
default network-overload-protection sgsn-new-connections-per-second
```

Set the attach rate to 500 per second, the action to drop, the wait time to 5 seconds, and the queue size to be calculated (as follows: *wait_time* * *#_new_connections* - i.e., 2500)

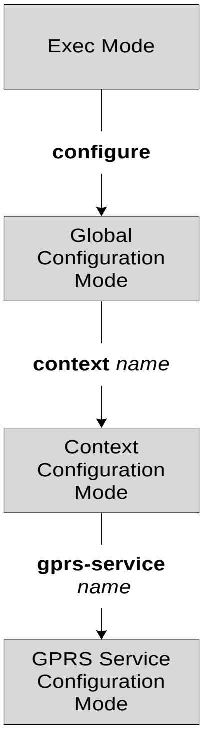
```
network-overload-protection sgsn-new-connections-per-second 500action
drop wait-time 5
```

Chapter 5
GPRS Service Configuration Mode Commands

The new **`gmm attach ptmsi-signature-mismatch`** command has been added to the GMM command set of the GPRS Service Configuration Mode. Details for the command and syntax are available in this section.

The prompt for this mode appears as:

```
[context_name]hostname(config-gprs-service)#
```


Exec Mode
configure
Global Configuration Mode
context name
Context Configuration Mode
gprs-service name
GPRS Service Configuration Mode

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

gmm

gmm actually provides a set of commands used to define the GPRS mobility management parameters for the SGSN service.

Important: The **gmm** commands can be repeated as needed to set each timer.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
gmm { accept-procedure [ new-tlli | old-tlli ] | attach ptmsi-signature-mismatch
send-reject failure-code cause_code | ciph-gmm-msg-from-unknown-ms { detach |
ignore } | mobile-reachable-timeout mins | negotiate-t3314-timeout secs | purge-
timeout mins | T3302-timeout mins | T3312-timeout mins | T3313-timeout secs |
T3350-timeout secs | T3360-timeout secs | T3370-timeout secs | trau-timeoutsecs
}

default gmm { attach ptmsi-signature-mismatch | ciph-gmm-msg-from-unknown-ms |
mobile-reachable-timeout | negotiate-t3314-timeout | purge-timeout | T3302-
timeout | T3312-timeout | T3313-timeout | T3350-timeout | T3360-timeout | T3370-
timeout | trau-timeout }

no gmm negotiate-t3314-timeout
```

default

Disables the specified function or resets the specified timer to system defaults.

no

Removes the specified GMM definition from the configuration.

accept-procedure [new-tlli | old-tlli]

Default: new-tlli
This keyword enables the use of either a new TLLI (temporary logical link identifier) or an old TLLI for attach-accept or RAU-accept messages sent by the SGSN to the MS during related procedures.

attach ptmsi-signature-mismatch send-reject failure-code *cause_code*

Default: disabled
This keyword enables the SGSN to validate the P-TMSI signature, present in the Attach Request, against the PTMSI-SIGNATURE stored at the SGSN. The SGSN then sends an Attach Reject to the MS if the PTMSI-SIGNATURE does not match.
The P-TMSI signature validation functionality only works if the feature is enabled. But even if it is enabled, the feature does not validate in the following situations:

- when the PTMSI-SIGNATURE is absent from the 2G Attach Request.

- if the first subscriber being in DETACHED state or is purged with FREEZE-PTMSI. In both the scenarios PTMSI-SIGNATURE cannot be validated.
- when the 2G subscriber(MS2) attaches with the same P-TMSI and a different P-TMSI_Signature as previously attached 2G subscriber (MS1), both the subscriber profiles are cleared from the system. This is relevant where the old RAI for MS-2 is the same as the current RAI for MS-1.

Optionally, a GMM failure *cause_code* can be configured to include in the Attach Reject if one is sent. 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

`ciph-gmm-msg-from-unknown-ms { detach | ignore }`

Configures how the SGSN will behave when it receives a ciphered GMM message from an unknown MS.

`detach` - Instructs the SGSN to send a Detach message to the MS.
`ignore` - Instructs the SGSN to send an Ignore (drop) message to the MS.
Default: **`ignore`**

`mobile-reachable-timeout` *`mins`*

Default: 58 minutes
Timer value for the mobile reachability timer.
`mins` must be an integer from 4 to 1440.

`negotiate-T3314-timeout` *`secs`*

Set the number of seconds for the T3314-timeout ready timer value. Value sent out from SGSN so MS can negotiate ready timer.
`secs` must be an integer from 0 to 11160. Default is 44 seconds.

- If the MS does not send the ready timer in the Attach/RAU request, then the SGSN sends this T3314-timeout (ready timer) value.
- If the MS sends the requested value of the ready timer in the Attach/RAU Request, and if the requested value is less than or equal to the value of the negotiate-T3314-timeout timer, then the SGSN sends Att/RAU Accept with the requested T3314 value.
- If the MS sends the requested value of the ready timer in the Attach/RAU Request, and if the requested value is greater than the value of the negotiate-T3314-timeout timer, then the SGSN sends Att/RAU Accept with the negotiate-T3314-timeout value.

Important: This is the only GMM timer that can be disabled by entering **`no`** at the beginning of the command syntax. **`no gmm negotiate-t3314-timeout`** By disabling negotiation of the T3314-timeout value, if the MS sends the requested value of the ready timer in the Att/RAU Request, then the SGSN sends the T3314-timeout value in the Att/RAU Accept.

`purge-timeout` *`mins`*

Default: 10080 minutes
Value defines the mm-context lifetime in minutes.
`mins` must be an integer from 1 to 20160.

`T3302-timeout` *`mins`*

Default: 12 minutes
Defines the number of minutes for timer to send to MS.
`mins` is an integer from 1 to 186.

`T3312-timeout` *`min`*

Default: 54 minutes
Periodic RAU update timer to send to MS.
`mins` is an integer from 0 to 186.

`T3313-timeout` *`secs`*

Default: 5 seconds
Initial page timeout timer for retransmission for Paging Requests.
`secs` is an integer from 1 to 60.

T3314-timeout *secs*

Default: 44 seconds
Ready Timer for controlling Cell Update Procedure.
secs must be an integer from 0 to 11519.

T3350-timeout *secs*

Default :6 seconds
Retransmission timer for Attach Accept/RAU Accept/P-TMSI Realloc Command.
secs must be an integer from 1 to 20.

T3360-timeout*secs*

Default :6 seconds
Retransmission timer for Authentication Request.
secs must be an integer from 1 to 20.

T3370-timeout *secs*

Default :6 seconds
Retransmission timer for Identity Request.
secs must be an integer from 1 to 20.

trau-timeout *secs*

This timer is available in releases 9.0 and higher.
Default: 30
Specifies the number of seconds the "old" 3G SGSN waits to purge the MS's data. This timer is started by the "old" SGSN after completion of the inter-SGSN RAU.
secs : Must be an integer from 5 to 60.

Usage

Use this command to set GMM timers.

Example

Set the t3370 timer expiration for 15 seconds:

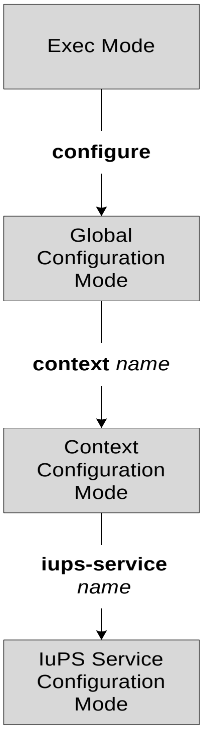
```
gmm t3370-timeout 15
```

Chapter 6
IuPS Service Configuration Mode Commands

A new command facilitates handling of empty Connection Request messages. The command and syntax are detailed in this section.

In this mode, the prompt will appear similar to:

```
[<context_name>]hostname(config-ctx-iups-service)#
```


Exec Mode
configure
Global Configuration Mode
context name
Context Configuration Mode
iups-service name
IuPS Service Configuration Mode

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

empty-cr

This command allows the operator to determine how empty Connection Request messages will be handled.

Product

SGSN

Privilege

Security Administrator, Administrator

Syntax

```
empty-cr procedure reject

[ default | no ] empty-cr procedure reject
```

`default | no`

Using either **`default`** or **`no`** with the command disables the rejection function and returns the system to the default behavior, which is to ignore receipt of the empty CRs.

Usage

Use this command to enable/disable the procedure for handling empty (not containing dataparameters) Connection Request (CR) messages.

This feature can be used in the following scenario: During 4G to 3G handovers, some Connection Requests from mobile subscribers might be ignored by the SGSN, even though their UE would display that the WCDMA was available. The RNC would send an SCCP Connection Request (CR) over the Iu interface to the SGSN. Normally, this message contains a RANAP message and GMM, but according to 3GPP and ITU Q.713 standards, it is permissible to send an SCCP CR without any data parameters. In such a situation, normally the SGSN would ignore these SCCP CR messages, because without these data parameters the SGSN would be unable to derive the DeMux key which is the basis for determining the Session Manager instance to be used for a subscriber. Using this feature allows the SGSN to send a Reject to the mobile subscriber when an “empty” SCCP CR is sent from their UE.

Fields have been added to the output of the following CLI show commands to track the receipt and rejection of Connect Request (CR) messages:

- show demux-mgr statistics imsimgr full
- show gmm-sm statistics
- show gmm-sm statistics verbose

Example

The following command enables the empty CR handling procedure:

```
empty-cr procedure reject
```

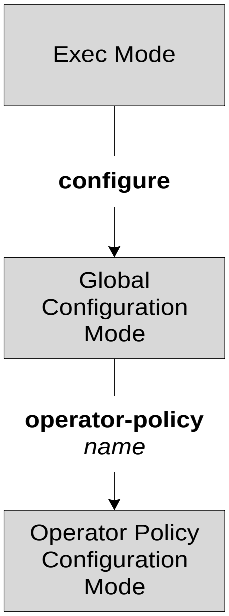
The following command disables the empty CR handling procedure:

```
default empty-cr procedure reject
```

Chapter 7
Operator Policy Configuration Mode

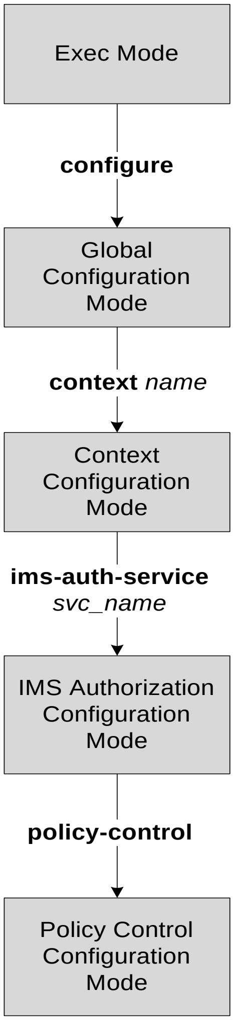
Operator Policy configuration mode associates APNs, APN profiles, IMEI ranges, IMEI profiles, an APN remap table and a call control profile to an operator policy. New maximum APN profile and IMEI range associations have been defined.

- A maximum of 1000 operator policies can be defined, this includes the ‘default’ operator policy.
- A maximum of 128 APN profiles can be associated with a single operator policy - this is an increase from 50.
- A maximum of 128 IMEI profiles can be associated with a single operator policy - this is an increase from 10.



Chapter 8
Policy Control Configuration Mode Commands

Policy Control Configuration mode is used to configure the Diameter dictionary, origin host, host table entry and host selection algorithm for IMS Authorization service.


Exec Mode
configure
Global Configuration Mode
context name
Context Configuration Mode
ims-auth-service svc_name
IMS Authorization Configuration Mode
policy-control
Policy Control Configuration Mode

cc-profile

This command enables to configure value of the **Offline** AVP sent to the PCRF based on the Charging Characteristics (CC) profile received from the SGSN.

Product

GGSN

Privilege

Security Administrator, Administrator

Syntax

```
cc-profile cc_profile_number [ to cc_profile_number_range_end ] map-to offline-
avp { 0 | 1 }

{ default | no } cc-profile
```

`default`

Configures the default setting for this command.
Default: Deletes all previously configured mappings.

`no`

Deletes all previously configured mappings.

`cc_profile_number`

Specifies the CC profile number to map.
For example, 1 for Hot Billing.
`cc_profile_number` must be an integer from 0 through 15.

`cc_profile_number_range_end`

Specifies, for a range of CC profile numbers to map, the end number. That is, from *`cc_profile_number`* through *`cc_profile_number_range_end`*.
`cc_profile_number_range_end` must be an integer from 1 through 15.

`map-to offline-avp { 0 | 1 }`

Specifies to map the CC profile number(s) to the **Offline** AVP value sent to the PCRF.

- **`0`**: Corresponds to the value DISABLE_OFFLINE (0).
- **`1`**: Corresponds to the value ENABLE_OFFLINE (1).

Usage

Use this command to configure the CC Profile to **Offline** AVP value mapping. The **Offline** AVP's value (DISABLE_OFFLINE (0), ENABLE_OFFLINE (1)) is derived based on the CC profile received from the SGSN as specified by this mapping.
The following example shows how this command can be configured multiple times:

```
cc-profile 1 to 2 map-to offline-avp 1
```

```
cc-profile 4 map-to offline-avp 0

cc-profile 8 map-to offline-avp 1
```

On configuring the above set of commands, the Offline AVP value is sent as 1 (Offline enabled) for the CC profiles 1 (Hot Billing), 2 (Flat Rate), and 8 (Post-Paid). And, as 0 (Offline disabled) for the CC profile 4 (Pre-paid).

When configuring this command, overlapping of CC profile numbers is not permitted. In the following example, after configuring the first command, which specifies to send the **Offline** AVP's value as 1 (Offline enabled) for the CC profiles 1 through 15, the second command, which specifies to map CC profile 7, is not permitted:

```
cc-profile 1 to 15 map-to offline-avp 1

cc-profile 7 map-to offline-avp 0
```

Example

The following command specifies to send **Offline** AVP value as 1 (Offline enabled) for the CC profile 1 (Hot Billing):

```
cc-profile 1 map-to offline-avp 1
```

The following command specifies to delete all previously configured mappings:

```
no cc-profile
```