

IuPS Service Configuration Mode Commands

Command Modes

The IuPS Service configuration mode is used to define properties for the IuPS service which controls the Iu-PS interface connections to Radio Network Controllers (RNCs) of the UMTS Terrestrial Radio Access Network (UTRAN).

Exec > Global Configuration > Context Configuration > IuPS Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service)#
```

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

Note From R15.0 onwards, License Control is implemented on all Network Sharing related commands.

Important For information on common commands available in this configuration mode, refer to the Common Commands chapter.

- access-protocol, on page 2
- associate, on page 3
- blockedlist-timeout-gtpu-bind-addresses, on page 4
- empty-cr, on page 5
- force-authenticate consecutive-security-failure , on page 6
- gtpu, on page 7
- inter-rnc-procedures, on page 9
- iu-hold-connection, on page 10
- iu-recovery, on page 11
- iu-release-complete-timeout, on page 11
- loss-of-radio-coverage ranap-cause, on page 12
- mbms, on page 13

- network-sharing cs-ps-coordination, on page 13
- network-sharing failure-code, on page 14
- network-sharing non-shared, on page 16
- network-sharing stop-redirect-reject-cause, on page 16
- plmn, on page 17
- rab-assignment-response-timeout, on page 19
- radio-network-controller, on page 20
- rai-skip-validation , on page 21
- relocation-alloc-timeout, on page 21
- relocation-complete-timeout, on page 22
- reset, on page 23
- rnc, on page 24
- security-mode-complete-timeout, on page 25
- service-request-follow-on, on page 26
- srns-context-response-timeout, on page 27
- tigoc-timeout, on page 27
- tintc-timeout, on page 28

access-protocol

This command configures the access protocol parameters for the IuPS service.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IuPS Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service)#
```

Syntax Description

access-protocol sccp-network *sccp_net_id*
no access-protocol sccp-network

no

Removes a previously configured access protocol value.

sccp-network *sccp_net_id*

Specifies the Signaling Connection Control Part (SCCP) for this IuPS service to use.

sccp_net_id must be an integer from 1 to 16.

Usage Guidelines

Use this command to configure access protocol parameters for the current IuPS service.

Example

The following command specifies that the current Iu-PS service should use SCCP *1*:

```
access-protocol sccp-network 1
```

associate

This command associates a configured DSCP marking template with this IuPS service and associated Iu interface.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IuPS Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service)#
```

Syntax Description

associate dscp-template downlink *dscp_template_name*
no associate dscp-template downlink

no

Removes a previously configured association.

dscp_template_name

Specifies a DSCP marking template that was previously configured with the commands in the DSCP Template configuration mode.

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

Usage Guidelines

Use this command to associate a specific DSCP marking template with this IuPS service and associated Iu interface. The DSCP template provides a mechanism for differentiated services code point (DSCP) marking of control packets and signaling messages at the SGSN's M3UA level on the Iu interface. This DSCP marking enables the SGSN to perform classifying and managing of network traffic and to determine quality of service (QoS) for the interface to the IP network.

Example

The following command associates a DSCP marking template named *dscptemp1* with the Iu interface:

```
associate dscp-template downlink dscptemp1
```

The following command disassociates a previously associated DSCP marking template named *template4* with this IuPS service configuration:

```
no associate dscp-template downlink
```

blockedlist-timeout-gtpu-bind-addresses

This command specifies the time period that a GTP-U bind address (loopback address) will not be used (is blacklisted) in RAB-Assignment requests after a RAB assignment request, with that GTP-U bind address, has been rejected by an RNC with the cause - Unspecified Error. This is a failure at the RNC's GTP-U IP interface.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IuPS Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service)#
```

Syntax Description

In releases prior to StarOS 21.26:

```
blacklist-timeout-gtpu-bind-addresses seconds
default blacklist-timeout-gtpu-bind-addresses
no blacklist-timeout-gtpu-bind-addresses
```

From StarOS 21.26 and later releases:

```
blockedlist-timeout-gtpu-bind-addresses seconds
default blockedlist-timeout-gtpu-bind-addresses
no blockedlist-timeout-gtpu-bind-addresses
```

no

Disables the Blockedlisting timeout configuration.

default

Resets the blockedlist time to 60 seconds.

seconds

Number of seconds that the GTP-U bind (loopback) address will not be used in a RAB-Assignment request.

seconds : Must be an integer from 1 to 1800.

Usage Guidelines

Use this command to configure the blockedlist period.

Example

In releases prior to StarOS 21.26:

The following command specifies a 15 minutes (*460 seconds*) blacklist period.

blacklist-timeout-gtpu-bind-addresses 460

From StarOS 21.26 and later releases:

The following command specifies a 15 minutes (*460 seconds*) blacklist period.

blockedlist-timeout-gtpu-bind-addresses 460

empty-cr

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

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IuPS Service Configuration

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

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ctx-iups-service)#`

Syntax Description

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 Guidelines

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 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

force-authenticate consecutive-security-failure

Disable/enable authentication when the MS/UE security fails and configures the procedures and frequency for authentication

Product

SGSN

Privilege

Security Administrator, Administrator, Operator

Command Modes

Exec > Global Configuration > Context Configuration > IuPS Service Configuration

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

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx-iups-service)#

Syntax Description

force-authenticate consecutive-security-failure { inter-sgsn-rau | local-messages count *frequency* **| non-local-messages count** *frequency* **}**
[default | no] force-authenticate consecutive-security-failure { inter-sgsn-rau | local-messages | non-local-messages }

default

Resets the values to defaults. Forced authentication is enabled for all the types of event procedures with the default values for determining frequency for authentication.

no

Disables the specified authentication configuration.

inter-sgsn-rau

Default: enabled

Enables/disables authentication for inter-SGSN RAU.

The SGSN does not remember previous inter-SGSN-RAU failures for a P-TMSI/RAI because the SGSN clears all contexts on the occurrence of an inter-SGSN-RAU security failure. So the next inter-SGSN-RAU can only be authenticated forcefully if it comes before the previous context is cleared. This type of forced authentication is enabled by default because this type of failure is fairly common.

local-messages count *frequency*

Default: 5

Enables/ disables authentication for local messages (such as local RAUs, Service Requests, Detach Requests, etc) . Consecutive security failures is fairly rare for local messages so the default count frequency is fairly

high, 5. Setting the count frequency enables the feature and sets the number of consecurity local message security failures that must occur prior t o authentication being forced.

frequency: Enter an integer from 1 to 10.

non-local-messages count *count*

Default: 1

Enables/ disables authentication for non-local messages (such as inter-RAT RAUs and all types of attaches) . Consecutive security failures for non-local messages is fairly common so the default count frequency is 1. Setting the count frequency enables the feature and sets the number of consecurity non-local message security failures that must occur prior t o authentication being forced.

frequency: Enter an integer from 1 to 10.

Usage Guidelines

GMM authentication is optional for UMTS. When GMM authentication is skipped, the SGSN and the MS continue to re-use the latest keys exchanged during the most recent GMM authentication procedure. This can result in the SGSN and the MS going out of sync with the CK and IK currently in use. If a mismatch occurs when the MS continues to use the correct parameters (e.g., cksn or P-TMSI signature) in the next Iu and if the SGSN skips authentication on the Iu, then, usually, the security mode will timeout or be rejected because the MS will not be able to decipher or perform an integrity check on the network messages. This scenario results in a lot of useless signaling in the network. This command allows the operator to enable a forced GMM authentication that will either resolve this type of problem or avoid it. As well, the operator can configure a frequency of authentication that best meets their needs.

Example

The following command enables forced authentication after every *3rd* local message security failure:

```
force-authenticate consecutive-security-failure local-messages count 3
```

gtpu

This commands configures parameters for the GTP user (GTP-U) dataplane.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IuPS Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service)#
```

Syntax Description

```
gtpu { bind ip_addr | echo-interval seconds | max-retransmissions number |
retransmission-timeout seconds | sync-echo-with-peer }
no gtpu { bind address ip_addr | echo-interval | max-retransmissions |
retransmission-timeout | sync-echo-with-peer }
```

```
default gtpu { echo-interval | max-retransmissions | retransmission-timeout
 | sync-echo-with-peer }
```

no

Removes the configured parameter value.

default

Sets the specified parameter to its default setting.

bind address *ip_addr*

This command binds the specified IP address to the Iu-PS GTP-U endpoint.

ip_addr: Must be an IP v4 IP address in dotted decimal notation.

echo-interval *seconds*

Default: 60

Configures the rate, in seconds, at which GTP-U echo packets are sent to the UTRAN over the Iu-PS interface.

seconds : Must be an integer from 60 through 3600.

max-retransmissions *number*

Default: 5

Configures the maximum number of transmission retries for GTP-U packets.

number : Must be an integer from 0 through 15.

retransmission-timeout *seconds*

Default: 5

Configures the retransmission timeout for GTPU packets in seconds.

seconds : Must be an integer from 1 through 20.

sync-echo-with-peer

This keyword is applicable to the SGSN only.

This keyword enables the SGSN to synchronize path management procedures with the peer after a GTP service restart recovery.

After GTP service recovery, the SGSN restarts the timers for GTP echo transmission, hence a drift in echo request transmission time (from the pre-recovery time) can occur causing the SGSN to be out of sync with the peer. By using this keyword, when the SGSN receives the first Echo Request (GTPC or GTPU) from the peer after the GTP service restart, in addition to replying with an ECHO Response, the SGSN transmits an ECHO Request to the peer and the SGSN restarts the timers associated with the path management procedures. This causes the path management procedure at SGSN to synchronize with the peer node.

Default: Enabled

Usage Guidelines

Use this command to configure GTP-U parameters for the Iu-PS interface.

Example

The following command binds the IP address *192.168.0.10* to the Iu-PS interface for communication with the UTRAN:

```
gtpu bind address 192.168.0.10
```

inter-rnc-procedures

This command enables the processing of SRNS relocation when the source RNC is behaving as the target RNC

Product

SGSN

Insert product and tag this paragraph appropriately.

Command Modes

Exec > Global Configuration > Context Configuration > IuPS Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service)#
```

Syntax Description

```
[ no ] inter-rnc-procedures [ source-rnc-as-target-rnc |
use-old-location-info ]
```

no

Disables SRNS relocation when the source RNC is behaving as the target RNC. This is the default behavior.

source-rnc-as-target-rnc

Configures the SGSN to complete SRNS relocation when the source RNC is behaving as the target RNC. For example, in the case of a Femtocell-to-Femtocell handoff - the femtocell gateway may act both as the source and target RNC to the femtocells, although from the SGSN's perspective it is the same RNC.

use-old-location-info

Selects and uses the old values of LAC, RAC and SAC for S-CDRs and ULI information sent to the GGSN during an intra-SRNS procedure.

Usage Guidelines

Use this command to enable/disable SRNS relocation when the source RNC is behaving as the target RNC.

Example

Enter this command to enable SRNS relocation for those scenarios where the source RNC is behaving as the target RNC.

```
inter-rnc-procedures source-rnc-as-target-rnc
```

iu-hold-connection

Defines the type and duration of the Iu hold connection.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IuPS Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service)#
```

Syntax Description

```
iu-hold-connection [ always | requested-by-ms ] [ hold-time seconds ]
default iu-hold-connection
no iu-hold-connection
```

default

Resets the Iu hold connection parameters to requested-by-ms and 100 second duration.

no

Removes the configuration information for the specified Iu hold connection parameter.

always

Specifies that there is always to be an Iu hold connection procedure.

requested-by-ms

Specifies that there is only an Iu hold connection procedure if requested by the MS/UE.

This is the default setting for Iu-hold-connection.

hold-time *time*

This variable configures the interval (in seconds) that the SGSN holds the Iu connection.

time: must be an integer from 1 to 3600.

time: must be an integer from 10 to 3600.



Important It is recommended to use a minimum value of "10" seconds. If a value less than "10" seconds is used, more collisions may be observed. If the minimum value of "1" is set, after a re-load, INTRA-RAU (with unknown ptmsi, old-rai known) will be released in "1" second if the Identity Rsp does not come within "1" second.

Default is 100.

Usage Guidelines Define the amount of time the Iu connection will be held open.

Example

Instruct the SGSN to hold the Iu connection open for 120 seconds

```
iu-hold-connection always hold-time 120
```

iu-recovery



Important This command has been deprecated and is no longer available.

Product SGSN

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

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service)#
```

iu-release-complete-timeout

Configures the SGSN's timer for waiting for an Iu Release Complete message from the RNC.

Product SGSN

Privilege Security Administrator, Administrator

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

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service)#
```

Syntax Description

```
iu-release-complete-timeout time
default iu-release-complete-timeout
```

default

Resets the timer to its default setting.

time

This variable defines the amount of time (in seconds) that the SGSN waits to receive an 'Iu Release Complete' message from the RNC.

Default: 10.

time: Must be an integer from 1 to 60.

Usage Guidelines Configure the number of seconds that the SGSN waits to receive the Iu Release Complete message.

Example

Set the SGSN to wait 20 seconds for Iu-Release-Complete:

```
iu-release-complete-timeout 20
```

loss-of-radio-coverage ranap-cause

This command sets the detection cause included in the Iu Release message. This command is unique to releases 9.0 and higher.

Product SGSN

Privilege Security Administrator, Administrator

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

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service)#
```

Syntax Description

```
loss-or-radio-coverage ranap-cause cause_number
default loss-of-radio-coverage ranap-cause
```

default

This keyword resets the configuration to the default cause ID number.

ranap-cause *cause_number*

This number identifies the reason the SGSN has detected, from Iu Release messages, for the loss of radio coverage (LORC). This value is included in the IE messages the SGSN sends to either the GGSN or the GGSN and the peer SGSN to indicate LORC state. The range of reasons is a part of the set defined by 3GPP 25413.

cause_number : Must be an integer from 1 to 512.

Default: 46 (MS/UE radio connection lost)

Usage Guidelines By defining a cause code, the SGSN knows to detect the LORC state of the mobile from Iu Release messages it receives for the subscriber. This configuration also instructs the SGSN to include the defined cause code for the LORC state in the IE portion of various messages sent to the GGSN and optionally the peer SGSN.

This command is one of the two commands required to enable the SGSN to work with the GGSN and, optionally the peer SGSN, to implement the Overcharging Protection feature (see the *SGSN Overview* in the *SGSN Administration Guide* for feature details. The other command needed to implement the Overcharging

Protection feature is the **gtp private extension** command explained in the *SGSN APN Policy Configuration Mode* chapter of the *Command Line Interface Reference*.

Example

Use the following command to set the cause code to indicate that there are no radio resources available in the target cell, cause *53*.

```
loss-or-radio-coverage ranap-cause 53
```

mbms

This command is in development for future use so the command and keywords that you might see are **not** currently supported.

network-sharing cs-ps-coordination

Enables/disables the SGSN service to perform a CS-PS coordination check.



Important With the release of 15.0, both 2G and 3G MOCN functionality is license controlled and the license is required to use all previously available network sharing SGSN configuration commands. For additional information, contact your Cisco Account Representative.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IuPS Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service)#
```

Syntax Description

```
network-sharing cs-ps-coordination [ homer | roamer ]
default network-sharing cs-ps-coordination
no network-sharing cs-ps-coordination
```

default

Including this keyword resets the SGSN service to allow the check to be performed.

no

Disables this CS-PS coordination checking for this IuPS service.

homer

Enables checking for CS-PS co-ordination for homers (UEs registered in the home network) only.

roamer

Enables checking for CS-PS co-ordination for roamers (UEs from outside the home network) only.

Usage Guidelines

Use this command to facilitate the network sharing functionality. With this command, the SGSN can be instructed to perform a check to determine if CS-PS coordination is needed.

3GPP TS 25.231 section 4.2.5 describes the functionality of the SGSN to handle CS-PS (circuit-switching/packet-switching) coordination for attached networks not having a Gs-interface. In compliance with the standard, the SGSN rejects an Attach in a MOCN configuration with cause 'CS-PS coordination required', after learning the IMSI, to facilitate the RNC choosing the same operator for both CS and PS domains.

Example

Use the following syntax to disable the CS-PS coordination check:

```
no network-sharing cs-ps-coordination
```

Use the following command to enable the CS-PS coordination check only for UEs from outside the home network:

```
no network-sharing cs-ps-coordination roamer
```

network-sharing failure-code

Configure the reject cause code to included in network-sharing Reject messages.



Important With the release of 15.0, both 2G and 3G MOCN functionality is now license controlled and the license is required to use all previously available network sharing SGSN configuration commands. For additional information, contact your Cisco Account Representative.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IuPS Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service)#
```

Syntax Description

network-sharing failure *failure_code*
default network-sharing failure

default

Resets the SGSN service to use the default cause code,14 (GPRS services not allowed in this PLMN).

failure_code

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

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

- 111 - Protocol error, unspecified

Usage Guidelines Use this command to determine which failure code will be included in Reject messages sent by the SGSN when there is a network-sharing failure.

Example

Use the following syntax to indicate that roaming is not allowed (*#13*) as the cause for the network-sharing failure:

```
network-sharing failure 13
```

network-sharing non-shared

This command allows non-shared area access when network-sharing is enabled.

Product SGSN

Privilege Security Administrator, Administrator

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

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service)#
```

Syntax Description

```
network-sharing non-shared
[ default | no ] network-sharing non-shared
```

default

Resets the default to disable non-shared access.

Usage Guidelines When non-shared area access is enabled, the SGSN sends the selected-plmn value in Attach/RAU accept if LAI is having one of the selected-plmn and "selected-plmn" or "Redirect-attempt flag" IEs are not included in the request message.

Example

Disable non-shared area access if it has already been configured:

```
no network-sharing non-shared
```

network-sharing stop-redirect-reject-cause

Enables the operator to disable the default behavior which sends Redirection Indication IE in RANAP Reject messages when reject is due to GMM cause #17 (network failure) related to System Failure or Unexpected

Data value MAP errors from the HLR. This change of the default behavior would only be applicable to 3G Roamers.

Product SGSN

Privilege Security Administrator, Administrator

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

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service)#
```

Syntax Description

```
network-sharing stop-redirect-reject-cause network-failure
{ default | no } network-sharing stop-redirect-reject-cause
```

default

Instructs the SGSN to use the default behavior and send redirect indication in Attach Reject or RAU Reject if reject is due to GMM cause 'network failure' which resulted from one of the MAP errors unexpected data value or system failure.

no

Disables this function and returns to the default behavior.

Usage Guidelines With this command, the operator would change the SGSN's default behavior (complies with 3GPP Release 11) for roaming subscribers and send Redirection Complete IE in Attach and RAU Reject messages when the reject is due to GMM cause #17 (network failure) in response to receiving System Failure or Unexpected Data value MAP errors from the HLR

Example

Configure the SGSN to send Redirect Indication IE in RANAP reject messages:

```
default network-sharing stop-redirect-reject-cause
```

plmn

Configures the PLMN (public land mobile network) related parameters for the IuPS service. This command is appicable to releases 8.1 and higher.

Product SGSN

Privilege Security Administrator, Administrator

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

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service)#
```

Syntax Description

plmn id mcc *mcc_num* **mnc** *mnc_num* **[network-sharing common-plmn mcc** *mcc_num* **mnc** *mnc_num* **[plmn-list mcc** *mcc_num* **mnc** *mnc_num* **[mcc** *mcc_num* **mnc** *mnc_num***+]]]**
no plmn id

no

Removes the PLMN ID from the configuration.

id

Creates a PLMN configuration instance based on the PLMN ID (comprised of the MCC and MNC). In accordance with TS 25.413, the SGSN supports up to 32 PLMN configurations for shared networks.

mcc *mcc_num*

Specifies the mobile country code (MCC) portion of the PLMN's identifier.

mcc_num: The PLMN MCC identifier and can be configured to any integer value between 100 and 999.

mnc *mnc_num*

Specifies the mobile network code (MNC) portion of the PLMN's identifier.

mnc_num: The PLMN MNC identifier and can be configured to any 2-digit or 3-digit value between 00 and 999.

network-sharing common-plmn mcc *mcc_num* mnc *mnc_num*

When network sharing is employed, this set of keywords is required to define the PLMN Id of the common PLMN. The common PLMN is usually not the same as the local PLMN.



Important With the release of 15.0, both 2G and 3G MOCN functionality is now license controlled and the license is required to use all previously available network sharing SGSN configuration commands. For additional information, contact your Cisco Account Representative.

plmn-list mcc *mcc_num* mnc *mnc_num*

When network sharing is employed and more than two PLMNs are available, then use the **plmn-list** keyword to begin a list of all additional PLMNs.

Usage Guidelines

Use this command to configure the PLMN associated with the SGSN. There can only be one PLMN associated with an SGSN unless one of the following features is enabled and configured: network sharing or multiple PLMN.

For network sharing, use of the **network-sharing** keywords make it possible to identify more than one PLMN. Including the PLMN identified initially. None have precedence. They are all treated equally but they must each be unique. In a MOCN configuration, the PLMN list will not be used as there would only be one local PLMN.

For multiple PLMN support, the SGSN can support up to 8 Iu-PS configurations for PLMNs. These Iu-PS service configurations must be associated with the SGSN via the **ran-protocol** command in the SGSN Service configuration mode.

Example

Use the following command to identify a PLMN by the MCC *313* and MNC *23* and instruct the SGSN to perform network sharing with a single *common PLMN* identified by MCC *404* and MNC *123*:

```
plmn id mcc 313 mnc 23 network-sharing common-plmn mcc 404 mnc 123
```

rab-assignment-response-timeout

Configures the RAB assignment timer.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IuPS Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service)#
```

Syntax Description

rab-assignment-response-timeout *time*
default rab-assignment-response-timeout

default

Resets the timer to its default setting.

time

This variable configures the amount of time (in seconds) that the SGSN waits to receive a RAB assignment from the RNC.

time: must be an integer from 1 to 60.

Default: 8.

Usage Guidelines

This command defines time the SGSN waits for the completion of the RAB assignment procedure.

Example

Change the timer setting to *11* seconds.

```
rab-assignment-response-timeout 11
```

radio-network-controller

This command creates an instance of an RNC configuration to associate with the IuPS service for the SGSN. This command is only available in release 8.0; use the **rnc** command for releases 8.1 and higher.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IuPS Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service)#
```

Syntax Description

`radio-network-controller id` *`rnc_id`* **`mcc`** *`mcc_num`* **`mnc`** *`mnc_num`*
`no radio-network-controller id` *`rnc_id`* **`mcc`** *`mcc_num`* **`mnc`** *`mnc_num`*

no

Removes the configuration information for the specified RNC.

id *rnc_id*

Define the instance number of the RNC configuration.

rnc_id : Must be an integer from 0 to 4095.

mcc *mcc_num*

Specifies the mobile country code (MCC).

mcc_num : Must be an integer between 100 and 999.

mnc *mnc_num*

Specifies the mobile network code (MNC).

mnc_num : Must be an integer between 00 and 999.

Usage Guidelines

Use this command to configure information for the IuPS service to use to contact specific RNCs.

This command also provides access to the RNC configuration mode.

Example

The following command creates or accesses RNC configuration instance *#1* with MCC of *131* and MNC of *22*:

```
radio-network-controller id 1 mcc 131 mnc 22
```

rai-skip-validation

Enable or disable if validation checks are done to verify the MCC and MNC fields received in the old RAI IE in Attach/RAU Requests.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IuPS Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service)#
```

Syntax Description

`[ no ] rai-skip-validation`

no

Disables skipping the validation of the old RAI MCC/MNC fields and enables the default behavior to validate.

Usage Guidelines

This command configures the SGSN to enable or disable rejection of RAU requests with invalid MCC/MNC values in the old RAI field. By default, this configuration is disabled allowing the default behavior to validate the old RAI MCC/MNC fields.

This command also impacts the PTMSI attaches where the old RAI field is invalid. If the OLD RAI field is invalid and if the validation is enabled, the identity of the MS is requested directly from the MS instead of the peer SGSN.

Validation checks are done per 3GPP TS 24.008 for the MCC/MNC fields of the old RAI IE in Attach/RAU Requests. RAU requests with invalid MCC/MNC values in the old RAI field are rejected. For Attach requests with invalid MCC/MNC values in the old RAI field, the identity of the MS is retrieved directly from the MS instead of sending an identity request to the peer Node where the MS identity is derived from the valid old-RAI.

Example

Use this command to configure rejection of RAU requests with invalid MCC/MNC values in the old RAI field:

`no rai-skip-validation`

relocation-alloc-timeout

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

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IuPS Service Configuration

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

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ctx-iups-service)#`

Syntax Description

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 Guidelines

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
```

relocation-complete-timeout

This command specifies the maximum time for the SGSN to wait for a Relocation Completion from the core network.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IuPS Service Configuration

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

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ctx-iups-service)#`

Syntax Description

relocation-complete-timeout *timeout_value*
default relocation-complete-timeout

default

Resets the configuration to a 5 second wait time.

timeout_value

Time in seconds that the SGSN waits for relocation to be completed.

timeout_value : Must be an integer from 1 to 60.

Default : 5 seconds.

Usage Guidelines

Use this command to configure the number of seconds the SGSN will wait for a relocation to be completed. 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 for *10* seconds.

```
relocation-complete-timeout 10
```

reset

Defines the configuration specific to the RESET procedure.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IuPS Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service)#
```

Syntax Description

```
reset { ack-timeout time | guard-timeout time | max-retransmissions retries
 | sgsn-initiated }
default reset { ack-timeout | guard-timeout | max-retransmissions |
sgsn-initiated }
no reset sgsn-initiated
```

default

Returns to the default settings for the Reset procedure.

no

Removes the SGSN-initiated reset procedure from the configuration.

ack-timeout *time*

Configures the interval (in seconds) for which the SGSN waits for RESET-ACK from the RNC.

time must be an integer from 5 to 60.

Default: 20.

guard-timeout

Configures the interval (in seconds) after which the SGSN sends RESET-ACK to the RNC.

time must be an integer from 5 to 60.

Default : 10

max-retransmissions

Configures maximum retries for RESET message.

retries must be an integer from 0 to 2.

Default: 1.

sgsn-initiated

Enables SGSN initiated RESET procedure.

Default: disabled.

Usage Guidelines

Configures the parameters that determine a RESET.

Example

Use the following to have the SGSN initiate the RESET procedure:

```
reset sgsn-initiated
```

rnc

This command creates or accesses an instance of an RNC (radio network controller) configuration.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IuPS Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service)#
```

Syntax Description

rnc id *rnc_id*
no rnc id *rnc_id*

no

Removes the configuration information for the specified RNC.

id *rnc_id*

Set the identification number of the RNC configuration instance.

rnc_id : Must be an integer from 0 to 4095 for 8.1 releases. Must be an integer from 0 to 65535 for releases 9.0 and higher.

Usage Guidelines

Use this command to configure information for the IuPS service to use to contact specific RNCs.

This command also provides access to the RNC configuration mode.

Example

The following command creates an RNC configuration instance *#3442*:

```
rnc id 3442
```

security-mode-complete-timeout

This command configures the security mode timer.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IuPS Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service)#
```

Syntax Description

security-mode-complete-timeout *time*
default security-mode-complete-timeout

default

Resets the timer configuration to the default settings.

time

Configures the interval (in seconds) the SGSN waits for the security mode from the MS to complete.

time must be an integer from 1 to 60.

Default is 5

Usage Guidelines

Use this command to configure the timer that determines how long the SGSN waits for a Security Mode Complete message from the MS (mobile station).

Example

Instruct the SGSN to wait *7* seconds:

security-mode-complete-timeout 7

service-request-follow-on

Instructs the SGSN not to release an Iu immediately.

Product

SGSN

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IuPS Service Configuration

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

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ctx-iups-service)#`

Syntax Description

[default | no] service-request-follow-on

default

Resets the configuration to the default, this function is enabled.

no

Disables this function so that Iu is released without waiting for the Iu-Hold-Timer to expire.

Usage Guidelines

For an Iu established as the result of a Service Request (signaling), the SGSN, by default, waits for the Iu-Hold-Timer to expire.

Use this command with the 'no' prefix to disable this function.

Use this command with the 'default' prefix or without any prefix if the configuration was modified previously with by **no service-request-follow-on**.

Example

Disable this function to wait for the Iu-Hold-Timer to expire:

no service-request-follow-on

Enable this function if it was previously disabled:

service-request-follow-on

srns-context-response-timeout

This command configures the SGSN context response timer.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IuPS Service Configuration

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

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ctx-iups-service)#`

Syntax Description

`srns-context-response-timeout` *`time`*
`default srns-context-response-timeout`

default

Resets the timer configuration to the default setting.

time

Configures the interval (in seconds) for which the SGSN waits for an SRNS Context Request message.

time must be an integer from 1 to 60.

Default: 5.

Usage Guidelines

Configures the time to wait before the SGSN sends a response to the SRNS Context-Request message.

Example

Configure the SGSN to wait *7* seconds for an SRNS Context-Request response:

`srns-context-response-timeout 7`

tigoc-timeout

This command configures the TigOc interval.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IuPS Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service)#
```

Syntax Description

tigoc-timeout *time*
default tigoc-timeout

default

Resets the timer configuration to the default setting.

time

This command sets the time in seconds.

time : Must be an integer from 1 to 60.

Default: 5.

Usage Guidelines

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..

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > IuPS Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service)#
```

Syntax Description

tintc-timeout *time*
default tintc-timeout

default

Resets the timer configuration to the default setting.

time

Set the number of seconds to wait.

time : Must be an integer from 1 to 60.

Default: 30.

Usage Guidelines

Define *4* as the number of seconds that the SGSN waits before decrementing (by one) the traffic level of the RNC.

Example

```
tintc-timeout 4
```