

HNB-GW Service Configuration Mode Commands

Important In Release 20 and later, HNBGW is not supported. Commands in this configuration mode must not be used in Release 20 and later. For more information, contact your Cisco account representative.

The 3G UMTS Home-NodeB Gateway Service Configuration Mode manages access to the UMTS core network in a 3G UMTS network through a Femto node.

Command Modes

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

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

- access-control-db, on page 2
- associate cbs-service, on page 3
- associate gtpu-service, on page 4
- associate rtp pool, on page 5
- authorised-macro-lai macro-info-ie-absent-action, on page 6
- authorised-macro-lai mcc, on page 7
- common-plmn, on page 8
- end, on page 9
- exit, on page 9
- handin, on page 9
- hnb override-vsa location-based-service, on page 10
- hnb-access-mode closed, on page 11
- hnb-access-mode hybrid, on page 12
- hnb-access-mode mismatch-action, on page 13
- hnb-access-mode open, on page 14
- hnb-aggregation, on page 15

- hnb-config-transfer, on page 16
- hnb-identity, on page 17
- ip iu-qos-dscp, on page 18
- ip iuh-qos-dscp, on page 20
- ipsec connection-timeout, on page 23
- iurh-handoff, on page 24
- iurh-handoff-guard-timer, on page 25
- mocn-max-reroute-attempts, on page 25
- mocn-reroute-timeout, on page 26
- paging cs-domain, on page 27
- paging imsi-purge-timer, on page 29
- paging ps-domain, on page 29
- paging open-hnb, on page 31
- radio-network-plmn, on page 33
- ranap reset, on page 34
- rtcp report, on page 35
- rtp address, on page 36
- rtp port, on page 37
- rtp mux, on page 38
- sctp bind, on page 39
- sctp checksum-type, on page 40
- sctp connection-timeout, on page 41
- sctp cookie-life, on page 42
- sctp heart-beat-timeout, on page 42
- sctp mtu-size, on page 43
- sctp rto, on page 44
- sctp sack-frequency, on page 45
- sctp sack-period, on page 46
- security-gateway bind, on page 46
- sessmgr-to-cbsmgr-pacing-timer, on page 48
- tnnsf-timer, on page 48
- ue registration-timeout, on page 49

access-control-db

Configures the access control database parameters in an HNB-GW service instance to control HNB and UE access to the HNB-GW node.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

Syntax Description

access-control-db imsi-purge-timeout { immediate | *dur* }
default access-control-db imsi-purge-timeout

default

Sets the default value to HNB-UE access control database on HNB-GW service instance.

The default timeout duration for purging of the IMSI White List from the HNB-GW Access Control database is 24 hours. The HNB-GW service waits for 24 hours after all referenced HNBs have de-registered before purging the records.

immediate

Sets the HNB-GW service to purge the HNB-UE access control database immediately after all referenced HNBs have de-registered.

imsi-purge-timeout *dur*

Sets the timeout duration (in minutes) for the access control database to wait before purging the IMSI values received as a White List from HMS/BAC.

After all HNBs have de-registered, the Access Control database on HNB-GW maintains the IMSI White List received from HMS/BAC during HNB registration procedure for the configured durations before purging the list.

dur is an integer from 1 through 1440.

Usage Guidelines

Use this command to configure the HNB-UE access control database parameters on HNB-GW service.

This command sets the timeout duration to maintain the IMSI White List received from HMS/BAC during HNB registration procedure in HNB-GW service for the configured *dur* in minutes after de-registration of all referenced HNBs from HNB-GW node and then purge the database.

Example

Following command sets the HNB-GW service instance to purge all IMSI records from HNB-UE access control database immediately after all referenced HNBs de-registered from HNB-GW service instance.

access-control-db imsi-purge-timeout immediate

associate cbs-service

Configures CBS service for this HNBGW service.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

Syntax Description

associate cbs-service *svc_name*
no associate cbs-service

no

Removes the configured CBS service from this HNB-GW service configuration.

svc_name

Identifies the name of the pre-configured CBS service to associate with an HNB-GW service.

svc_name is an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to configure CBS service for HNB-GW service.

Example

Following command configures CBS service named *cbs_hnb1* with specific HNB-GW service.

associate cbs-service cbs_hnb1

associate gtpu-service

Associates a previously configured GTP-U service to bind the HNB-GW service with an HNB towards the HNB side. A GTP-U service must be configured in Context Configuration mode before using this configuration.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

Syntax Description

associate gtpu-service *svc_name*
no associate gtpu-service

no

Removes the associated GTP-U service from this HNB-GW service configuration.

svc_name

Identifies the name of the pre-configured GTP-U service to associate with an HNB-GW service towards the Home-NodeB side.

svc_name is an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to configure GTP-U data plan between HNB-GW service and Home-NodeB. The service defined for GTP-U can be configured in Context configuration mode.



Important

Another GTP-U service can be used to bind the HNB-GW service towards the Core Network and can be configured in HNB-PS Configuration mode. For more information on GTP-U service configuration, refer *GTP-U Service Configuration Mode Commands*.

Example

Following command associates GTP-U service named *gtpu_hnb1* with specific HNB-GW service towards Home-NodeB side.

```
associate gtpu-service gtpu_hnb1
```

associate rtp pool

Associates a previously defined RTP pool (IP pool) with the HNB-GW service. This pool is used by HNB-GW to send an IP address to HNB where HNB uses it to map the RTP streams over Iuh interface. This command is used for RTP stream management on HNB-GW.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

Syntax Description

```
associate rtp pool pool_name
no associate rtp pool
```

no

Removes the associated RTP pool (IP pool) from this HNB-GW service configuration.

pool_name

Specifies the name of the pre-configured RTP IP pool that the HNB-GW uses to assign IP addresses when mapping RTP streams over the Iuh interface.

pool_name is an alphanumeric string of 1 through 31 characters.

Important For IP pool (RTP pool) configuration, refer **ip pool** command in *Context Configuration Mode Commands* chapter.

Usage Guidelines Use this command to associate an RTP pool (IP Pool) with an HNB-GW service for allotment of RTP IP address to HNB-GW node and send the same to HNB for RTP stream management support. The HNB maps the RTP streams with received IP address(es) while communicating with HNB-GW over Iuh interface where HNB-GW communicates with MSC/VLR through IuCS-over-IP tunnel.

This command is used for RTP stream management on HNB-GW.

Important This command must be used to provide IP address for mapping of RTP streams on Iuh interface between HNB and HNB-GW.

Example

Following command associates RTP pool named *rtp_1* with HNB-GW service for RTP stream end point from Home-NodeB:

```
associate rtp pool rtp_1
```

authorised-macro-lai macro-info-ie-absent-action

This command configures the Action if Macro Coverage information IE is absent in HNB Location Information. The HNB will be accepted for Action Accept and rejected for Action Reject.

Product HNB-GW

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

Syntax Description

```
authorised-macro-lai macro-info-ie-absent-action { accept | reject }
default authorised-macro-lai macro-info-ie-ab sent-action
```

default

Sets / Restores default value assigned for the Action if Macro Coverage information IE is absent in HNB Location Information. The default value is reject.

accept

Accepts HNB even if Macro Coverage information IE is absent in HNB Location Information.

reject

Rejects HNB if Macro Coverage information IE is absent in HNB Location Information.

Usage Guidelines

Use this command when Macro Coverage Info IE is absent in HNB Location information.

Example

The following command accepts HNB even if Macro Coverage inforamtion IE is absent in HNB Location Information:

```
authorised-macro-lai macro-info-ie-absent-action accept
```

authorised-macro-lai mcc

This command configures MCC of Pre-Configured macro lai range for HNB Authorisation.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

Syntax Description

`[ no ] authorised-macro-lai mcc` *`mcc`* **`mnc`** *`mnc`* **`lac range`** *`min`* **`to`** *`max`*

no

Removes the MCC of Pre-Configured macro lai range for HNB Authorisation.

mcc *mcc*

MCC of Pre-Configured macro lai range for HNB Authorisation.

mcc is a number ranging from 100 through 999.

mnc *mnc*

MNC of Pre-Configured macro lai range for HNB Authorisation.

mnc is a number ranging from 00 through 999.

lac range *min* to *max*

LAC of Pre-Configured macro lai range for HNB Authorisation.

LAC is configured as range, if single lac make min is equal to max.

Macro LAC from*min* to *max* integer values between 0 through 65535.

Usage Guidelines Use this command to configure the MCC of Pre-Configured macro lai range for HNB Authorisation.

Example

The following command configures the MCC of Pre-Configured macro lai range for HNB Authorisation with mcc *888*, mnc *44* and lac range from *10* to *1000*:

```
authorised-macro-lai mcc 678 mnc 788 lac range 10 to 1000
```

common-plmn

This command configures the Common PLMN along with rnc-id. This enables MOCN.

Product HNB-GW

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

Syntax Description

```
common-plmn mcc mcc mnc mnc rnc-id rnc_id
no common-plmn
```

no

Removes the configuration of Common PLMN service.

mcc *mcc*

Configures the MCC of Common PLMN.

mcc is a number ranging from 100 through 999.

mnc *mnc*

Configures the MNC of Common PLMN.

mnc is a number ranging from 00 through 999.

rnc-id *rnc_id*

Configures the RNC-id for this HNBGW service.

rnc_id is a decimal value of integer ranging from 0 through 4095.

Usage Guidelines Use this command to configure the Common PLMN along with rnc-id to HNB-GW service.

This enables MOCN.

Example

The following command configures Common PLMN with mcc *888*, mnc *44* and rnc-id *66*to HNB-GW service:

```
common-plmn mcc 444 mnc 56 rnc-id 56
```

end

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

Product All

Privilege Security Administrator, Administrator

Syntax Description

```
end
```

Usage Guidelines Use this command to return to the Exec mode.

exit

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

Product All

Privilege Security Administrator, Administrator

Syntax Description

```
exit
```

Usage Guidelines Use this command to return to the parent configuration mode.

handin

Allows or disallows the incoming hand-over of an MS in HNB-GW via the Serving Radio Network Subsystem (SRNS) Relocation procedure for the specified packet switched/circuit switched (PS/CS) core network (CN) domain.

Product HNB-GW

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

Syntax Description

`[ no | default ] handin cn-domain [ cs | ps ]`

no

Disallows the incoming MS hand-over for the particular CN domain via SRNS Relocation procedure in an HNB-GW service instance.

If hand-over is restricted the relocation request will be rejected with rejection cause "Relocation Not Supported In Target RNC Or Target System".

default

Sets the HNB-GW service instance to allow the incoming MS hand-over for the particular CN domain via SRNS Relocation procedure in an HNB-GW service instance.

cs

Sets the HNB-GW service instance to allow the incoming MS hand-over for the CS core network domain via SRNS Relocation procedure in an HNB-GW service instance.

ps

Sets the HNB-GW service instance to allow the incoming MS hand-over for the PS core network domain via SRNS Relocation procedure in an HNB-GW service instance.

Usage Guidelines

Use this command to set HNB-GW service instance for allowing/disallowing incoming hand-over of an MS in HNB-GW via SRNS Relocation procedure for PS or CS core network domain.

If hand-over is restricted the Relocation Request message will be rejected with rejection cause "Relocation Not Supported In Target RNC Or Target System".

Example

The following command configures the HNB-GW service instance to allow hand-over of an MS in HNB-W via SRNS Relocation procedure for PS core network domain:

`handin cn-domain ps`

hnb override-vsa location-based-service

This command enables / disables overriding of a particular vendor specific attribute of configured location based HNB Service.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

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

Entering the above command sequence results in the following prompt:

`[local]host_name(config-hnbgw-service)#`

Syntax Description

`[ no | default ] hnb override-vsa location-based-service`

no

Disables the overriding of vendor specific attribute for location based service.

default

When set to default, overriding of vendor specific attribute will be disabled.

Usage Guidelines

Use this command to enable / disable overriding of a particular vendor specific attribute of configured location based HNB Service.

Example

The following command enables overriding of a particular vendor specific attribute of configured location based HNB Service. :

`hnb override-vsa location-based-service`

hnb-access-mode closed

This command configures Closed Access Mode for HNB Access Mode Support.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HSGW Service Configuration

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

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-hsgw-service)#`

Syntax Description

`hnb-access-mode closed [ max-registered-ue` *`value`* **`]`**
`default hnb-access-mode closed`

default

Sets/Restores the default value assigned for Closed Access Mode.

max-registered-ue*value*

Maximum Registered UEs per Close HNB. Default is 64.

value is an integer ranging from 1 to 1000.

Important Maximum registered UEs depends on the aggregation factor configuration of HNBGW service. If aggregation is enabled then Maximum registered UEs is 1 to 10000 otherwise it is 1 to 1000.

Usage Guidelines Use this to configure Closed Access Mode for HNB Access Mode Support.

Example

Following command configures the Maximum Registered UEs per Close HNB as 15.

```
hnb-access-mode closed max-registered-ue 15
```

hnb-access-mode hybrid

This command configures the Hybrid HNB access mode in HNB-GW service instance and related parameters.

Product HNB-GW

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

Syntax Description

```
hnb-access-mode hybrid [ max-non-access-controlled-ue num ]
{ no | default } hnb-access-mode hybrid
```

no

Disables the Hybrid Access Mode of HNB service.

default

Sets the default configuration of Hybrid Access Mode support. The default value of Maximum Non-Access-Controlled UEs per Hybrid HNB is 64.

By default, HNB-GW allows registration of Non-Access-Controlled UEs per Hybrid HNB and a maximum of 16 UEs can register from a hybrid HNB in an HNB-GW service instance.

max-non-access-controlled-ue *num*

Maximum Non-Access-Controlled UEs per Hybrid HNB.

num is an integer from 0 through 64.

Usage Guidelines Use this command to configure the Hybrid HNB access mode in HNB-GW service instance and related parameters.

Example

The following command configures the Hybrid HNB access mode in HNB-GW service instance and related parameters. :

```
hnb-access-mode hybrid
```

hnb-access-mode mismatch-action

This command configures the mismatch action of HNB access mode in HNB-GW service instance and related parameters.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

Syntax Description

```
hnb-access-mode mismatch-action { accept-aaa-value | hnb-reg-rej }
default hnb-access-mode mismatch-action
```

default

Sets the default Hybrid Access Mode of HNB service. The default value of Maximum Non-Access-Controlled UEs per Hybrid HNB is 64.

accept-aaa-value

Supports the Accept AAA value.

hnb-reg-rej

Supports the HNB Registration Reject.

Usage Guidelines

Use this command to configure the mismatch action of HNB access mode in HNB-GW service instance and related parameters.

Example

The following command configures the mismatch action of HNB access mode in HNB Service to Accept AAA value:

```
hnb-access-mode mismatch-action accept-aaa-value
```

hnb-access-mode open

Configures the Open HNB access mode in HNB-GW service instance and related parameters.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

Syntax Description

hnb-access-mode open [max-registered-ue *reg_ue_open*]
{ no | default } hnb-access-mode open

no

Disables Open Access mode support.

If disabled and an Open HNB tries to register, the HNB-GW sends HNB-Registration-Reject message with "OAM Intervention" cause.

Important UE-Reg/CS-Call/PS-Call requests (both existing and future) is allowed from already registered Open HNBs even after operator has disabled the Open Access support. No new Open HNB registration is allowed once operator disables the Open Access support.

default

Sets the default configuration of Open Access mode support.

By default, HNB-GW allows registration of Open HNBs and a maximum of 64 UEs can register from an open HNB in an HNB-GW service instance.

max-registered-ue *reg_ue_open*

Sets the HNB-GW service instance to allow the maximum number of UEs through an open HNB under Open Access mode support.

reg_ue_open defines the maximum number of UEs that can register from an Open HNB as an integer from 1 through 64.

If a UE tries to register from an Open HNB which has already reached to the configured limit configured, the HNB-GW sends HNB-Registration-Reject message with "*ue not allowed in this hnb*" cause in an HNB-GW service instance.

Usage Guidelines

Use this command to configure the HNB-GW service instance for Open Access Mode support and related parameters.

This command enable Open Access mode support to allow the UEs that can register from an Open HNB. If a UE tries to register from an Open HNB with an HNB-GW service instance, which is already reached to the limit configured through **max-registered-ue** *reg_ue_open* the HNB-GW sends HNB-Registration-Reject message with "*ue not allowed in this hnb*" cause.



Important If Operator has reduced the maximum number of UEs allowed per Open HNB during the session, this will not have any effect on already registered UEs/CS-Calls/PS-Calls even if previously configured *reg_ue_open* is beyond the newly configured *reg_ue_open* value. Limits is respected while handling new requests.

Example

The following command configures the HNB-GW service instance to allow 16 UEs to register through an open HNB:

```
hnb-access-mode open max-registered-ue 16
```

hnb-aggregation

This command enables / disables HNB aggregation support for this hnbgw-service.

Product HNB-GW

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

Syntax Description

```
hnb-aggregation { handin-with-aggregator | max-registered-ues-per-hnb
value } [ -noconfirm ]
[ no | default ] hnb-aggregation handin-with-aggregator [ -noconfirm ]
```

no

Disables the HNB aggregation support for this hnbgw-service.

default

Sets the default value of HNB aggregation support for this hnbgw-service .

handin-with-aggregator

Enables or disables handin with the aggregators.

max-registered-ues-per-hnb

Configures the maximum number of UEs allowed per HNB.



Caution Once set, any change in this configuration will cause all HNBs in this HNBGW service to get disconnected.

value defines the maximum number of UEs allowed per HNB as an integer from 1 through 10000.

Usage Guidelines Use this command to enable / disable HNB aggregation support for this hnbgw-service.

Example

The following command configures the maximum number of UEs allowed per HNB:

```
hnb-aggregation max-registered-ues-per-hnb 16
```

The following command enables handin with aggregators:

```
hnb-aggregation handin-with-aggregator
```

hnb-config-transfer

This command enables/disables Inclusion of Inner IP Address in HNB Configuration Transfer Response for HNBGW-service.

Product HNB-GW

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

Syntax Description **`[ default | no ] hnb-config-transfer add-inner-ip`**

no

Disables the Inclusion of Inner IP Address in HNB Configuration Transfer Response for HNBGW-service.

default

Enables the default behavior of Inclusion of Inner IP Address in HNB Configuration Transfer Response for HNBGW-service. By default it is enabled.

add-inner-ip

Enables/Disables Inclusion of Inner IP Address in HNB Configuration Transfer Response for HNBGW-service.

Usage Guidelines Use this command to enable / disable the Inclusion of Inner IP Address in HNB Configuration Transfer Response for HNBGW-service.

Example

The following command enables the Inclusion of Inner IP Address in HNB Configuration Transfer Response for HNBGW-service:

```
hnb-config-transfer add-inner-ip
```

hnb-identity

Configures and also allows modification to the HNB ID before it is sent to the AAA server for authentation in HNB-GW service instance.

Product HNB-GW

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

Syntax Description **`[ default | no ] hnb-identity oui discard-leading-char`**

no

Disables discarding of leading character of HNB-id if it contains Organizationally Unique Identifier

default

Enables the default behavior of discarding of leading character of HNB-id if it contains Organizationally Unique Identifier. By default this feature is deactivated.

oui discard-leading-char

This CLI allows to modify the HNB ID before it is sent to the AAA server for authentication. By using this CLI, first character of the HNB-id can be removed if the HNB-id follows the format: '1<OUI>-<SerialNumber>@<realm>'.

Usage Guidelines Use this command to configure and allow modification to the HNB ID before it is sent to the AAA server for authentation in HNB-GW service instance.

Example

The following command configures the discarding of leading character of HNB-id if it contains Organizationally Unique Identifier:

```
hnb-identity oui discard-leading-char
```

ip iu-qos-dscp

Enables or disables the DSCP marking parameter for data packets carried over over an IuCS/IuPS interface towards MSC/SGSN. By default this command is **Disabled**.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

Syntax Description

ip iu-qos-dscp protocol udp payload { gtpu | rtcp | rtp } *dscp_code*
{ default | no } ip iu-qos-dscp protocol udp payload { gtpu | rtcp | rtp }

no

Use this keyword to place the configuration in **pass-through** mode (no marking of DSCP). Use of this keyword is allowed even when there is no previous DSCP parameter set.

Important In this configuration the **no** keyword does not disable or remove a previous configuration.

default

Enables the DSCP marking on HNB-GW and set/restores the QoS parameters to their default setting.

udp payload { gtpu | rtcp| rtp} ***dscp_code***

Specifies the QoS traffic pattern towards MSC/SGSN in SCTP protocol association over IuCS/IuPS interface.

By this keyword the Traffic classes specified by a user based on UDP protocol and GTPU, RTCP, and RTP type of payload identified based on the transport level port numbers.

Default DSCP code in UDP traffic are:

- **GTP-U**: cs1
- **RTCP**: ef
- **RTP**: af41

dscp_code

Specifies the QoS DSCP codes supported for SCTP and UDP traffic and its payloads towards MSC/SGSN over IuCS/IuPS interface.

following type of DSCP codes *dscp_code* are supported over IuH interface:

- **af11**: Marks traffic as Assured Forwarding 11 PHB (high throughput data)
- **af12**: Marks traffic as Assured Forwarding 12 PHB (high throughput data)
- **af13**: Marks traffic as Assured Forwarding 13 PHB (high throughput data)
- **af21**: Marks traffic as Assured Forwarding 21 PHB (low latency data)
- **af22**: Marks traffic as Assured Forwarding 22 PHB (low latency data)
- **af23**: Marks traffic as Assured Forwarding 23 PHB (low latency data)
- **af31**: Marks traffic as Assured Forwarding 31 PHB (multimedia streaming)
- **af32**: Marks traffic as Assured Forwarding 32 PHB (multimedia streaming)
- **af33**: Marks traffic as Assured Forwarding 33 PHB (multimedia streaming)
- **af41**: Marks traffic as Assured Forwarding 41 PHB (multimedia conferencing). This is the default DSCP code for RTP payloads in UDP protocol.
- **af42**: Marks traffic as Assured Forwarding 42 PHB (multimedia conferencing)
- **af43**: Marks traffic as Assured Forwarding 43 PHB (multimedia conferencing)
- **cs1**: Marks traffic with Class Selector 1 (low priority data). This is the default DSCP code for GTP-U payloads in UDP protocol.
- **cs2**: Marks traffic with Class Selector 2 (OAM)
- **cs3**: Marks traffic with Class Selector 3 (broadcast video)
- **cs4**: Marks traffic with Class Selector 4 (real-time interactive)
- **cs5**: Marks traffic with Class Selector 5 (signaling). This is the default DSCP code for all SCTP payloads.
- **cs6**: Marks traffic with Class Selector 6 (network control)
- **df** : Marks traffic as Default Forwarding (best effort: DSCP = 0)
- **ef**: Marks traffic as Expedited Forwarding PHB (telephony). This is the default DSCP code for RTCP payloads in UDP protocol.

Usage Guidelines

Use this command to enable/disable the DSCP marking for data packets over IuCS/PS interface. This command assigns the DSCP levels to specific traffic patterns in order to ensure that the packets are delivered according to the precedence with which they are tagged. The Diffserv markings are applied to the IP header of every subscriber data packet transmitted over IuCS/IuPs interface(s) towards MSC/SGSN.

This command adds DSCP marking on egress traffic going towards CN (CS/PS). To make the configuration **pass-through** mode or not marking DSCP at all in the packets, **no** variant of command is used. Use of **no** is allowed even when there is no previous DSCP configuration done.



Important By default this command is **Disabled**.



Important When DSCP configuration is not specified, the system works in **pass-through** mode and DSCP values in the ingress (from CN) and egress (to HNB) data packets remain unchanged. Multiple traffic classes can share the same code point value.

Following type shown in following tables respectively:

Table 1: Supported DSCP Codes and Service Class

Service Class	DSCP Code	Service Class	DSCP Code
high throughput data	af11 af12 af13	low priority data	cs1
low latency data	af21 af22 af23	OAM	cs2
multimedia streaming	af31 af32 af33	broadcast video	cs3
multimedia conferencing	af41 af42 af43	real-time interactive	cs4
best effort/ default forwarding, value zero	df	Signaling	cs5
telephony	ef	network control	cs6

The DSCP level can be configured for multiple traffic patterns within a single instance of this command.

Example

The following command configures the DSCP code for the SCTP IuCS/IuPS streaming traffic pattern for all payloads to be **ef**:

```
ip iu-qos-dscp protocol sctp payload all ef
```

ip iuh-qos-dscp

Enables or disables the DSCP marking parameter for control and data packets transmitted over an IuH interface towards HNB. By default this command is **Disabled**.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

Syntax Description

ip iuh-qos-dscp protocol { sctp payload all | udp payload { gtpu | rtcp | rtp } } *dscp_code*
{ default | no } ip iuh-qos-dscp protocol { sctp payload all | udp payload { gtpu | rtcp | rtp } }

no

Use this keyword to set the configuration in **pass-through** mode. Use of this keyword is allowed even when there is no previous DSCP parameter set.

Important In this configuration the **no** keyword does not disable/remove a previous configuration.

default

Enables the DSCP marking on HNB-GW and set/restores the QoS parameters to its default setting.

sctp payload all *dscp_code*

Specifies the QOS traffic pattern towards HNB in SCTP protocol association over IuH interface.

By this keyword the Traffic classes specified by a user based on SCTP protocol and all type of payload identified based on the transport level port numbers.

By default DSCP codes **cs5** is supported for **all** payloads in SCTP protocol.

udp payload { gtpu | rtcp| rtp} *dscp_code*

Specifies the QOS traffic pattern towards HNB in SCTP protocol association over IuH interface.

By this keyword the Traffic classes specified by a user based on UDP protocol and GTPU, RTCP, and RTP type of payload identified based on the transport level port numbers.

Default DSCP code in UDP traffic are:

- **GTP-U**: cs1
- **RTCP**: ef
- **RTP**: af41

dscp_code

Specifies the QOS DSCP codes supported for SCTP and UDP traffic and its payloads towards HNB over IuH interface.

following type of DSCP codes *dscp_code* are supported over IuH interface:

- **af11**: Marks traffic as Assured Forwarding 11 PHB (high throughput data)
- **af12**: Marks traffic as Assured Forwarding 12 PHB (high throughput data)
- **af13**: Marks traffic as Assured Forwarding 13 PHB (high throughput data)
- **af21**: Marks traffic as Assured Forwarding 21 PHB (low latency data)
- **af22**: Marks traffic as Assured Forwarding 22 PHB (low latency data)
- **af23**: Marks traffic as Assured Forwarding 23 PHB (low latency data)

- **af31**: Marks traffic as Assured Forwarding 31 PHB (multimedia streaming)
- **af32**: Marks traffic as Assured Forwarding 32 PHB (multimedia streaming)
- **af33**: Marks traffic as Assured Forwarding 33 PHB (multimedia streaming)
- **af41**: Marks traffic as Assured Forwarding 41 PHB (multimedia conferencing). This is the default DSCP code for RTP payloads in UDP protocol.
- **af42**: Marks traffic as Assured Forwarding 42 PHB (multimedia conferencing)
- **af43**: Marks traffic as Assured Forwarding 43 PHB (multimedia conferencing)
- **cs1**: Marks traffic with Class Selector 1 (low priority data). This is the default DSCP code for GTP-U payloads in UDP protocol.
- **cs2**: Marks traffic with Class Selector 2 (OAM)
- **cs3**: Marks traffic with Class Selector 3 (broadcast video)
- **cs4**: Marks traffic with Class Selector 4 (real-time interactive)
- **cs5**: Marks traffic with Class Selector 5 (signaling). This is the default DSCP code for all SCTP payloads.
- **cs6**: Marks traffic with Class Selector 6 (network control)
- **df** : Marks traffic as Default Forwarding (best effort: DSCP = 0)
- **ef**: Marks traffic as Expedited Forwarding PHB (telephony). This is the default DSCP code for RTCP payloads in UDP protocol.

Usage Guidelines

Use this command to enable/disable the DSCP marking for control and data packets carried by the IP protocols and their payloads on IuH. This command assigns the DSCP levels to specific traffic patterns in order to ensure that the packets are delivered according to the precedence with which they are tagged. The Diffserv markings are applied to the IP header of every subscriber data packet transmitted over IuH interface(s) towards HNB.

This command adds DSCP marking on egress traffic going towards HNB. To make the configuration **pass-through mode** or not marking DSCP at all in the packets, **no** variant of command is used. Use of **no** is allowed even when there is no previous DSCP configuration done.



Important By default this command is **Disabled**.



Important When DSCP configuration is not specified, system works in **pass-through** mode and DSCP value in the ingress (from CN) and egress (to HNB) control and data packets remain unchanged. Multiple traffic classes can share the same code point value.

Following type shown in following tables respectively:

Table 2: Supported DSCP Codes and Service Class 140

Service Class	DSCP Code	Service Class	DSCP Code
high throughput data	af11	low priority data	cs1
	af12		
	af13		

Service Class	DSCP Code	Service Class	DSCP Code
low latency data	af21 af22 af23	OAM	cs2
multimedia streaming	af31 af32 af33	broadcast video	cs3
multimedia conferencing	af41 af42 af43	real-time interactive	cs4
best effort/ default forwarding, value zero	df	Signaling	cs5
telephony	ef	network control	cs6

The DSCP level can be configured for multiple traffic patterns within a single instance of this command.

Example

The following command configures the DSCP code for the SCTP IuH streaming traffic pattern for all payloads to be **ef**:

```
ip iuh-qos-dscp protocol sctp payload all ef
```

ipsec connection-timeout

This command allows to configure IPSEC tunnel idle time out in hours. Default is 4 hours.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

Syntax Description

{ default | no } ipsec connection-timeout *ipsec_connection_timeout*

default

Sets the default value of idle time out as 4 hours.

no

Disbles IPSEC idle time out.

ipsec_connection_timeout

IPSEC tunnel idle time out in hours between 1 and 48. Default is 4 hours.

Usage Guidelines Use this command to configure IPSEC tunnel idle timeout in a specific HNB-GW service.

Example

The following command sets IPSEC tunnel idle time out to 3 hours:

```
ipsec connection-timeout 3
```

iurh-handoff

This command enables or disables the Femto To Femto Handover in a specific HNB-GW service.

Product HNB-GW

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

Syntax Description **[no | default]iurh-handoff**

default

Sets the default behavior of the Femto To Femto Handover in a specific HNB-GW service. By default, it is disabled.

no

Disables the Femto To Femto Handover option in a specific HNB-GW service.

Usage Guidelines Use this command to enable or disable the Femto To Femto Handover in a specific HNB-GW service.

Example

The following command sets the default value of Femto To Femto Handover in a specific HNB-GW service :

```
default iurh-handoff
```

iurh-handoff-guard-timer

This command is used to configure the IURH Relocation Guard Timer in a specific HNB-GW service. If F2F handover does not happen within the guard time, the procedure is aborted.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

Syntax Description

[default] iurh-handoff-guard-timer *timer_seconds*

default

Sets the default value of IURH Relocation Guard Timer. By default, the IURH Relocation Guard Timer value is 15 seconds.

timer_seconds

timer_seconds is the number of seconds, an integer ranging from 10 to 30.

Usage Guidelines

Use this command to configure the IURH Relocation Guard Timer in a specific HNB-GW service.

Example

The following command sets the default value of the IURH Relocation Guard Timer in a specific HNB-GW service:

```
default iurh-handoff-guard-timer  20
```

mocn-max-reroute-attempts

This command configures the maximum number of operators who can be attempted in the reroute procedure.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

Syntax Description

mocn-max-reroute-attempts *max_attempts*
default mocn-max-reroute-attempts

default

Sets / Restores default value assigned for maximum number of operators who can be attempted in the reroute procedure. The default value is 4.

max_attempts

max_attempts is an integer ranging from 1 through 8.

Usage Guidelines

Use this command to configure the maximum number of operators who can be attempted in the reroute procedure.

Example

The following command configures the maximum number of operators who can be attempted in the reroute procedure as 5:

mocn-max-reroute-attempts 5

mocn-reroute-timeout

This command configures the timeout for the individual reroute procedure with one operator.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

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

Entering the above command sequence results in the following prompt:

`[local]host_name(config-hnbgw-service)#`

Syntax Description

mocn-reroute-timeout *timeout_value*
default mocn-reroute-timeout

default

Sets / Restores default timeout value for the individual reroute procedure with one operator. The default value is 5.

timeout_value

timeout_value is an integer ranging from 1 through 5.

Usage Guidelines

Use this command to configure the timeout for the individual reroute procedure with one operator.

Example

The following command configures the timeout for the individual reroute procedure with one operator. *4*:

```
mocn-reroute-timeout 4
```

paging cs-domain

Configures paging optimization parameters for CS domain in the HNB-GW service instance.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

Syntax Description

```
paging cs-domain { handle-unknown-imsi { use-cn-paging-area | use-whitelist
 } | phase1 page-last-known-hnb timeout timeout_val1 | phase2
paging-grid-fan-out timeout timeout_val2 | phase3 paging-area-fan-out timeout
 timeout_val3 }
no paging cs-domain { handle-unknown-imsi [ use-cn-paging-area |
use-whitelist ] | phase1 page-last-known-hnb | phase2 paging-grid-fan-out
 | phase3 paging-area-fan-out }
default paging cs-domain { handle-unknown-imsi [ use-cn-paging-area |
use-whitelist ] | phase1 page-last-known-hnb timeout | phase2
paging-grid-fan-out timeout | phase3 paging-area-fan-out timeout }
```

default

Sets the default behavior of paging optimization configuration for the a specific HNB-GW service.

no

Removes paging optimization configuration for an appended option in a specific HNB-GW service.

handle-unknown-imsi

Handles Unknown IMSIs Options.

use-cn-paging-area

Uses paging area provided by Core Network for forwarding the Page Req to all open/hybrid HNBs.

use-whitelist

Uses whitelist of HNBs for forwarding the Page req to all closed/hybrid HNBs.

phase1

Paging Phase1 Configuration - Forwards Page Req to last-known-hnb.

page-last-known-hnb

Page the last known HNB for the call.

timeout*timeout_val1*

Sets the timeout value in seconds for the last-known-hnb paging configuration. It is an integer value ranging from 1 to 30.

phase2

Paging Phase2 Configuration - Forwards Page Req to all HNBs in the Grid of last-known-hnb.

paging-grid-fan-out

Pages the last known paging grid.

timeout_val2

Sets the timeout value in seconds for the grid fan-out paging configuration. It is an integer value ranging from 1 to 30.

phase3

Paging Phase3 Configuration - Forwards Page Req to all HNBs in the LAI of last-known-hnb.

paging-area-fan-out

Pages the last known paging area.

timeout_val3

Sets the timeout value in seconds for the area fan-out paging configuration. It is an integer value ranging from 1 to 30.

Usage Guidelines

Use this command to configure the CS domain paging optimization parameters for a specific HNB-GW service instance.

Example

The following command configures the CS domain paging optimization for grid fan-out timeout as 15 seconds for a specific HNB-GW service :

```
paging cs-domain phase2 paging-grid-fan-out timeout 15
```

paging imsi-purge-timer

Configures paging optimization based on the timer for purging the unregistered IMSIs in the HNB-GW service instance.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

Syntax Description

paging imsi-purge-timer timeout *timeout_val1*
default paging imsi-purge-timer timeout

default

Sets the default value for the IMSI purge timer as 3 hours.

timeout_val1

Sets the timeout value for the IMSI purge timer in hours. It is an integer ranging 1 to 12.

Usage Guidelines

Use this command to configure the timer value for purging the unknown IMSIs for paging optimization configuration in a specific HNB-GW service instance.

Example

The following command configures the IMSI purge timer as 4 hours for a specific HNB-GW service instance:

```
paging imsi-purge-timer timeout 4
```

paging ps-domain

Configures paging optimization parameters for PS domain in the HNB-GW service instance.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

Syntax Description

paging ps-domain { handle-unknown-imsi { use-cn-paging-area | use-whitelist } | phase1 page-last-known-hnb timeout *timeout_val1* **| phase2 paging-grid-fan-out timeout** *timeout_val2* **| phase3 paging-area-fan-out timeout** *timeout_val3* **}**
no paging ps-domain { handle-unknown-imsi [use-cn-paging-area | use-whitelist] | phase1 page-last-known-hnb | phase2 paging-grid-fan-out | phase3 paging-area-fan-out }
default paging ps-domain { handle-unknown-imsi [use-cn-paging-area | use-whitelist] | phase1 page-last-known-hnb timeout | phase2 paging-grid-fan-out timeout | phase3 paging-area-fan-out timeout }

default

Sets the default behavior of paging optimization configuration for the a specific HNB-GW service.

no

Removes paging optimization configuration for an appended option in a specific HNB-GW service.

handle-unknown-imsi

Handles Unknown IMSIs Options.

use-cn-paging-area

Uses paging area provided by Core Network for forwarding the Page Req to all open/hybrid HNBs.

use-whitelist

Uses whitelist of HNBs for forwarding the Page req to all closed/hybrid HNBs.

phase1

Paging Phase1 Configuration - Forwards Page Req to last-known-hnb.

page-last-known-hnb

Page the last known HNB for the call.

timeout*timeout_val1*

Sets the timeout value in seconds for the last-known-hnb paging configuration. It is an integer value ranging from 1 to 30.

phase2

Paging Phase2 Configuration - Forwards Page Req to all HNBs in the Grid of last-known-hnb.

paging-grid-fan-out

Pages the last known paging grid.

timeout_val2

Sets the timeout value in seconds for the grid fan-out paging configuration. It is an integer value ranging from 1 to 30.

phase3

Paging Phase3 Configuration - Forwards Page Req to all HNBs in the LAI of last-known-hnb.

paging-area-fan-out

Pages the last known paging area.

timeout_val3

Sets the timeout value in seconds for the area fan-out paging configuration. It is an integer value ranging from 1 to 30.

Usage Guidelines

Use this command to configure the PS domain paging optimization parameters for a specific HNB-GW service instance.

Example

The following command configures the PS domain paging optimization grid fan-out timeout as 20 seconds for a specific HNB-GW service :

```
paging ps-domain phase2 paging-grid-fan-out timeout 15
```

paging open-hnb

Configures paging optimization parameters for open HNBs connected through Open Access mode in the HNB-GW service instance. In this release it is used to configure paging optimization for Open Access mode support only. This command is depricated release 15.0 onwards. Paging optimization can be configured using other **paging** commands available in this chapter.



Important From Release14.0 and onward this command is part of *HNB-Global Configuration Mode*.



Important From Release 16 and later, this command has been deprecated.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

Syntax Description

```
paging open-hnb [hnb-where-ue-registered fallback ] {always | never |
only-if-with-paging-area}
default paging open-hnb
```

default

Sets the default behavior of paging optimization configuration for an open HNB while using Open Access mode support.

By default the HNB-GW pages open HNBs only if paging-area IE is received in the paging message.

{always | never | only-if-with-paging-area}

Sets the HNB-GW service instance to page open HNB for a paging message.

always: Sets the system to ALWAYS page the open HNBs irrespective of **paging-area** IE is received in paging messages.

never: Sets the system to NEVER page any open HNB.

only-if-with-paging-area: Sets the system to page the open HNBs only when **paging-area** IE is received in paging messages.

hnb-where-ue-registered fallback {always | never | only-if-with-paging-area}

Sets the HNB-GW service instance to page open HNB from where the UE is registered.

always: Sets the system to ALWAYS page the open HNBs from where the UE is registered. If the UE is not registered then it pages the open HNBs irrespective of **paging-area** IE is received in paging messages.

never: Sets the system to page the open HNBs from where the UE is registered. If the UE is not registered then it NEVER pages any open HNB.

only-if-with-paging-area: Sets the system to ALWAYS page the open HNBs from where the UE is registered. If the UE is not registered then it pages the open HNBs only when **paging-area** IE is received in paging messages.

Usage Guidelines

Use this command to configure the paging optimization parameters for open HNBs connected through Open Access mode in HNB-GW service instance.

Example

The following command configures the HNB-GW service instance to page an open HNB from where the UE is connected and paging-area IE is received in paging message:

```
paging open-hnb hnb-where-ue-registered fallback only-if-with-paging-area
```

radio-network-plmn

Creates, remove and enters the HNB-RN-PLMN Configuration mode. In this mode you can configure various parameters for radio network public mobile land networks (PLMNs). A maximum of 16 radio PLMN-IDs can be configured in an HNB-GW service.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

Syntax Description

radio-network-plmn mcc *mcc_num* **mnc** *mnc_num* **[-noconfirm]**
no radio-network-plmn mcc *mcc_num* **mnc** *mnc_num*

no

Removes the configured radio network PLMN identifier for an HNB-GW service.

Caution Removing the PLMN-ID is a disruptive operation; the HNB-GW service will be re-started.

mcc *mcc_num*

Specifies the mobile country code (MCC) part of radio network PLMN identifier as an integer value from 101 through 998.

mnc *mnc_num*

Specifies the mobile network code (MNC) part of radio network PLMN identifier as a 2- or 3-digit integer from 01 through 998.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage Guidelines

Use this command to configure the radio network PLMN identifier for an HNB-GW service. This command also creates a configuration mode to configure various parameters for defined radio network PLMN identifier in HNB-GW service.

Caution Changing or removing the PLMN-ID is a disruptive operation; the HNB-GW service will be re-started.

Entering this command results in the following prompt:

```
[context_name]hostname(config-radio-network-plmn)#
```

A maximum of 16 radio network PLMN identifiers are supported for an HNB-GW service.

Example

The following command configures the radio network PLMN identifier with MCC value as *102* and MNC value as *20* for an HNB-GW service:

```
radio-network-plmn mmc 102 mnc 20
```

ranap reset

Configures various Radio Access Network (RAN) Application Part reset procedure parameters in an HNB access network.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

Syntax Description

```
ranap reset {ack-timeout timer_value | guard-timeout g_timer | hnbgw-initiated
 | max-retransmissions retries}
default ranap reset {ack-timeout | guard-timeout | hnbgw-initiated |
max-retransmissions }
no ranap hnbgw-initiated
```

default

Resets the RANAP RESET parameters on HNB-GW service instance.

no

Disables the RANAP RESET procedure related parameters in an HNB-GW service instance.

ack-timeout *timer_value*

Sets the timer value (in seconds) to wait for Reset Acknowledge from SGSN/MSC. This is used during HNB-GW initiated RANAP RESET procedure in HNB-GW service instance.

timer_value is an integer value from 5 through 10. Default: 10

guard-timeout *g_timer_value*

Sets the timer value (in seconds) to send Reset Acknowledge to SGSN/MSC. After this duration the HNB-GW sends RESET-ACK to SGSN/MSC. This is used during SGSN/MSC initiated RANAP RESET procedure in HNB-GW service instance.

g_timer_value is an integer value from 5 through 10. Default: 10

hnbgw-initiated

Enables the HNB-GW Initiated RANAP RESET procedures. Default: Disabled

max-retransmission *retries*

Sets the maximum number of retires allowed for transmission of RESET-ACK message to SGSN/MSC. This is used during RANAP RESET procedure in HNB-GW service instance.

retries is an integer value from 0 through 2. When 0 is used retransmission is disabled. Default: 1

Usage Guidelines

Use this command to configure the RANAP RESET procedure related parameters in HNB-GW service.

Example

The following command configures the HNB-GW initiated RANAP RESET Procedure for an HNB-GW service:

```
ranap reset hnbgw-initiated
```

rtcp report

Enables or disables the generation of RTP Control Protocol (RTCP) packet/report types on a per HNB-GW service instance basis. It also sets the time interval in seconds between two consecutive RTCP reports.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

Syntax Description

```
rtcp report interval dur
{ no | default }  rtcp report interval
```

no

Disables the RTCP report generation on HNB-GW service. When RTP configuration is not explicitly mentioned, this is the default behavior.

default

Restores the report interval value to its default value of 5 seconds.

interval *dur*

Sets the time interval (in seconds) between two consecutive RTCP reports as an integer from 5 through 30. Default: 5

Usage Guidelines

Use this command to configure the enabling or disabling of the generation of RTCP packet/ report types on a per HNB-GW service instance basis and sets the specified time interval in seconds between two consecutive RTCP reports.

RTCP enables the receiver to detect if there is any packet loss and needs to compensate for any delay jitter. RTP and RTCP protocols work independently of the underlying Transport layer and Network layer protocols.

Whenever this command is disabled, RTCP report generation stops from the next expiry of the previously configured interval and after enabling, reports are generated only for the calls that established as new calls in the future. For existing calls reports generated as per configuration in place.

RTCP reports are generated for each RAB for RTP received from and sent to IuH interface.

Important The same interval is applicable for all kinds of RTCP packets/ reports across all sessions on an HNB-GW service.

Example

The following command configures the RTCP report generation interval to *15* seconds on an HNB-GW service for RTP stream:

```
rtcp report interval 15
```

rtp address

Configures the Real Time Protocol (RTP) address on HNB-GW used to map RTP streams while HNB-GW connects to MSC/VLR through an IuCSoIP (IuCS-over-IP) tunnel. This command is used for RTP stream management on HNB-GW.

This command is obsolete. Use **ip pool** or **ipv6 pool** command in Context Configuration mode for IP pool configuration for RTP stream management.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

Syntax Description

```
rtp address address
no rtp address
```

no

Removes the RTP IP address association to be used for communication between HNB and HNB-GW while communicating with MSC/VLR -GW through IuCS over IP tunnel.

address *address*

Specifies the IP address of HNB-GW to use as an end point by HNB and HNB maps the RTP streams with this IP address and HNB-GW communicates with MSC/VLR through IuCS-over-IP Tunnel.

address is the same IP address as assigned to HNB-GW to communicate with HNB and must be an IP address in IPv4 or IPv6 notation.

Important This command cannot be entered more than once. Only one RTP IP address can be configured for one HNB-GW service.

Usage Guidelines

Use this command to enable the HNB-GW IP address as RTP IP address and send the same to HNB to map RTP streams while HNB-GW communicates with MSC/VLR through IuCS-over-IP tunnel.

This command is used for RTP stream management on HNB-GW.

Example

The following command sets the RTP IP address *209.165.200.229* on HNB-GW to communicate with HNB while using IuCS-over-IP tunnel with CS network:

```
rtp address 209.165.200.229
```

rtp port

Configures the Real Time Protocol (RTP) port range to listen from HNB while connecting to MSC/VLR through an IuCSoIP (IuCS-over-IP) interface. This command is used for RTP stream management on HNB-GW.

This command is obsolete. Use **ip pool** or **ipv6 pool** command in Context Configuration mode for IP pool configuration for RTP stream management.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

Syntax Description

```
rtp port range port_start to port_end
default rtp port range
```

default

Sets the RTP port range to default range from 16384 to 65535.

port range *range_start* to *range_end*

Specifies the port number range to be used by HNB to map the RTP streams and HNB-GW listen on these ports while communicating with MSC/VLR through IuCS-over-IP tunnel.

range_start must be an integer between 16384 through 65535 and should be less than *range_end*.

range_end must be an integer between 16384 through 65535 and should be more than *range_start*.

Default: port 16384 through 65535

Important This command cannot be entered more than once. Only one range of RTP port can be configured for one HNB-GW service.

Usage Guidelines

Caution This command is NOT active now.

Use this command to assign the RTP port range to be used by HNB to map RTP streams and HNB-GW listen these ports for RTP streams while communicating with MSC/VLR through IuCS-over-IP tunnel.

This command is used for RTP stream management on HNB-GW.

Example

The following command sets the RTP port number *20000* to *21000* on HNB-GW to listen from HNB for RTP streams while connecting with MSC/VLR using IuCS-over-IP tunnel.

```
rtp port range 20000 to 21000
```

rtp mux

Configures the HNB-GW service to allow an Home-NodeB to multiplex multiple RTP streams in one IP packet. This support is provided for RTP stream management feature on HNB-GW.

Product HNB-GW

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

Syntax Description

[no | default] rtp mux

default

Sets the multiplexing option to default state of "disabled".

no

Removes the configured option to multiplex multiple RTP stream in one packet by Home-NodeB in HNB-GW configuration.

Usage Guidelines

Use this command to allow an Home-NodeB to multiplex multiple RTP streams in one IP packet. This configuration support is provided for RTP stream management feature on HNB-GW and it is disabled by default.

Example

The following command sets the HNB-GW to allow HNB to multiplex multiple RTP stream in one packet:

rtp mux

sctp bind

Configures the SCTP IP address and port that is used for binding the SCTP socket to communicate with the Home-NodeB over an Iuh interface within an HNB-GW service.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

Syntax Description

sctp bind { address *IPv4_address* **| port** *port_num* **}**
no sctp bind { address | port }

no

Removes the SCTP binding.

address *IPv4_address*

Specifies the IP address of the HNB-GW Iuh interface in IPv4 dotted-decimal.

port *port_num*

Specifies the SCTP port number to communicate with the Home-NodeBs using Iuh interface as an integer form 1 through 65535.

Usage Guidelines

Use this command to assign the SCTP IP address and port with SCTP socket on HNB-GW to communicate with the Home-NodeB using Iuh interface. This SCTP configuration provides the IP-address and listen port where HNB-GW service shall bind to listen for incoming SCTP associations from HNB.

Example

The following command sets the SCTP port number *999* on HNB-GW to listen from Home-NodeB over Iuh interface:

```
sctp bind port 999
```

The following command sets the SCTP address *209.165.200.229* of HNB-GW to use with Home-NodeB over Iuh interface:

```
sctp bind address 209.165.200.229
```

sctp checksum-type

Configures SCTP checksum-type.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Syntax Description

```
sctp checksum-type { adler32 | crc32 }
default sctp checksum-type
```

default

Sets the SCTP checksum-type.

adler32

Specifies the SCTP checksum-type ADLER32.

crc32

Specifies the SCTP checksum-type CRC32.

Usage Guidelines

Use this command to configure SCTP checksum-type.

Example

The following command sets the SCTP checksum-type to adler32 on HNB-GW:

```
sctp checksum-type adler32
```

sctp connection-timeout

Configures the SCTP connection timeout duration to explicitly remove the SCTP association with a non-responsive HNB in an HNB-GW service.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

Syntax Description

sctp connection-timeout *dur*
{ default | no } sctp connection-timeout

no

Disables the connection time out configuration on HNB-GW service.

default

Restores the connection timeout duration value to its default value of 10 seconds.

dur

Sets the connection timeout duration (in seconds) after which the association is explicitly removed. In case of an HNB de-registration scenario, the HNB-GW waits for configured amount time before initiating the procedure to clear the SCTP association.

dur is an integer from 5 through 30. Default: 10

Usage Guidelines

Use this command to configure the minimum duration value before removing the SCTP association between a non-responding HNB and HNB-GW. If HNB registration not happened within the configured period after the SCTP association is established then the SCTP association is explicitly removed. In a scenario where an HNB de-registered due to any reason, the HNB-GW waits for the configured amount of time before initiating the procedure to clear the SCTP association.

Example

The following command sets the SCTP connection timeout duration to *15* second on HNB-GW after expiry of which the SCTP association is removed:

```
sctp connection-timeout 15
```

sctp cookie-life

Configures the SCTP valid cookie-life, Min 5000ms and Max 120000ms with granularity of 100ms.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

Syntax Description

sctp cookie-life *dur*
default sctp cookie-life

default

Restores the SCTP cookie-life value.

dur

Sets the SCTP cookie-life (in seconds).

dur is an integer from 50 through 1200.

Usage Guidelines

Use this command to configure the SCTP valid cookie-life.

Example

The following command sets the SCTP cookie-life value to 55 on HNB-GW:

```
sctp cookie-life 55
```

sctp heart-beat-timeout

Configures the SCTP heartbeat timer parameters for SCTP connection over an IuH interface in an HNB-GW service instance.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

Syntax Description

sctp heart-beat-timeout *dur*
{ default | no } sctp heart-beat-timeout

no

Disables the heartbeat timer configuration for SCTP over IuH in HNB-GW service instance.

default

Restores the default time out value for heartbeat timer to 30 seconds.

dur

Sets the heartbeat timer timeout duration (in seconds) after which the next heartbeat command is sent to HNB from HNB-GW in SCTP over an IuH interface. In an HNB de-registration scenario, the HNB-GW waits for configured amount time before initiating the procedure to clear the SCTP association.

dur is an integer from 1 through 300. Default: 30

Usage Guidelines

Use this command to configure the minimum duration value before retransmitting the HEARTBEAT chunk to HNB from HNB-GW in SCTP transmission. By default HNB-GW monitors the reachability of the idle HNBs by sending a HEARTBEAT chunk periodically to the HNB address.

Each time the HEARTBEAT timer expires on any address, or when a HEARTBEAT sent to an idle address is not acknowledged within a Retransmission Timeout duration, the error counter of that HNB incremented.

When the value in the error counter exceeds the protocol parameter for maximum retransmission for that destination address, the HNB-GW mark the destination HNB as inactive and a notification is sent to the upper layer.

Example

The following command sets the SCTP HEARTBEAT timeout duration to *15* second on HNB-GW after expiry of which the HNB-GW retransmits the HEARTBAT chunk to HNB over SCTP association:

sctp heart-beat-timeout 15

sctp mtu-size

This command configures SCTP mtu-size, Min 508 bytes and Max is 65535 bytes with granularity of 1 byte.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

Syntax Description

sctp mtu-size { max | min | start } *size*
default sctp mtu-size { max | min | start }

default

Sets the SCTP mtu-size to its default value.

size

size is an integer from 508 through 65535.

Usage Guidelines

Use this command to configure the SCTP mtu-size.

Example

The following command configures the SCTP mtu-size max value to 555 on HNB-GW:

```
sctp mtu-size max 555
```

sctp rto

This command sets the SCTP Retransmission Timeout value.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

Syntax Description

sctp rto { initial *initial_value* **| max** *max_value* **| min** *min_value* **}**
default sctp rto { initial | max | min }

default

Sets the SCTP Retransmission Timeout value to default.

initial_value

initial_value is SCTP Retransmission Timeout initial value, which is an integer from 1 through 1200.

max_value

max_value is SCTP Retransmission Timeout max value (Min 500 ms and max 120000 ms with granularity of 100 ms) , which is an integer from 5 through 1200.

min_value

min_value is SCTP Retransmission Timeout max value (Min 100 ms and max 5000 ms with granularity of 100 ms) , which is an integer from 1 through 50.

Usage Guidelines

Use this command to set the SCTP Retransmission Timeout value.

Example

The following command sets the SCTP max Retransmission Timeout value to 555 on HNB-GW:

```
sctp rto max 555
```

sctp sack-frequency

This command configures the SCTP Selective Ack Frequency.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

Syntax Description

sctp sack-frequency *value*
default sctp sack-frequency

default

Sets the SCTP sack-frequency value to default.

value

Min value is 1 and Max value is 5.

value is an integer from 1 through 5.

Usage Guidelines

Use this command to configure the SCTP Selective Ack Frequency.

Example

The following command configure the SCTP Selective Ack Frequency to 5on HNB-GW:

```
sctp sack-frequency 5
```

sctp sack-period

This command is used to configure SCTP Selective Ack Period in Seconds.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

Syntax Description

sctp sack-period *value*
default sctp sack-period

default

Sets the SCTP sack-period value to default.

value

Min 0 ms and Max is 500ms with granularity of 100ms.

value is an integer from 0 through 5.

Usage Guidelines

Use this command to configure the SCTP Selective Ack Period in Seconds.

Example

The following command configures the SCTP Selective Ack Period in Seconds to 5 on HNB-GW:

```
sctp sack-period 5
```

security-gateway bind

Binds the SeGW in an HNB-GW service to a logical IP interface serving as an Iuh interface and associates an IPsec IKEv2 crypto-map template.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

Syntax Description

security-gateway bind address *IPv4_address* **crypto-template** *cryp_name* **[context** *ctxt_name*]
no security-gateway bind

no

Removes a previously configured IPSec IP address use for binding the IKEv2 IPSec tunnel (local bind address) to communicate with the Home-NodeBs using Iuh interface.

bind address *IPv4_address*

Specifies the IP address for the Iuh interface for the IPSec tunnel. This is the IP address where the HNB-GW service is bound and that is provided to the Home-NodeB during HNB-GW discovery.

The IP address is expressed in IPv4 dotted-decimal.

crypto-template *cryp_name*

Specifies the Crypto-map template to be used for IPsec IKEv2 tunneling for the interface configured as an Iuh.

cryp_name specifies the name of the pre-configured Crypto-map template which is configured in Crypto-Map Template Configuration mode and associated with the HNB-GW service to create an IPSec tunnel with a Home-NodeB during HNB-GW discovery procedure over an Iuh interface.

context *ctx_name*

Specifies the name of the pre-configured context in which the Security Gateway service is configured. By default this command uses the HNB-GW service context for the security Gateway configuration.

Usage Guidelines

Use this command to associate or tie the HNB-GW service to a specific logical IP address that is used for binding the Iuh socket to communicate with the Home-NodeB using IPSec tunnel. A maximum of one IP address can be configured with this command for one HNB-GW service.

The HNB-GW passes the IP address during setting up the HNB-GW discovery procedure with the Home-NodeB.



Caution This is a critical configuration. The HNB-GW service cannot be started without this configuration. Any change to this configuration would lead to restarting the HNB-GW service and removing or disabling this configuration stops the HNB-GW service.

Example

The following command binds the logical IP interface with the address of *209.165.200.229* to the HNB-GW service using existing IPsec Crypto-Map template *crypto1* to establish IPSec tunnel with Home-NodeB:

```
security-gateway bind address 209.165.200.229 crypto-template crypto1
```

The following command disables a binding that was previously configured:

security-gateway bind address 209.165.202.134

sessmgr-to-cbsmgr-pacing-timer

This command configures pacing timer value for SABP messages being sent from Sessmgr to CBSmgr. Default value is 100ms.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

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

Entering the above command sequence results in the following prompt:

[local]*host_name*(config-hnbgw-service)#

Syntax Description

sessmgr-to-cbsmgr-pacing-timer *milli_seconds*

milli_seconds

Pacing timer value in miliseconds which is an integer from 10 through 500.

Usage Guidelines

Use this command to configure pacing timer value for SABP messages being sent from Sessmgr to CBSmgr.

Example

The following command sets pacing timer value for SABP messages being sent from Sessmgr to CBSmgr to 50:

sessmgr-to-cbsmgr-pacing-timer 50

tnnsf-timer

Configures the NAS Node Selection Function (NNSF) timer (T-NNSF) which is used by the HNB-GW to store the IMSI and the relevant Global-CN-ID in the short term after Paging. This timer is used for Iu-Flex feature support.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

Syntax Description

tnnsf-timer *dur*
{ no | default } tnnsf-timer

no

Disables/removes the configured timer value of NNSF timer (T-NNSF) from HNB-GW service instance.

default

Sets the timer value of NNSF timer (T-NNSF) for HNB-GW service instance to default value of 30 seconds.

tnnsf-timer *dur*

Configures the NNSF timer (in seconds) which is used by the HNB-GW to store the IMSI and the relevant Global-CN-ID as an integer from 10 through 60. Default: 30

Usage Guidelines

Use this command to configure the NNSF timer value in seconds for Iu-Flex support.

Whenever the MSC sends the paging request with IMSI, the HNB-GW stores the Global_CN_ID of the node which issued the paging request message for the given IMSI and HNB-GW starts the **tnnsf-timer**. HNBGW stores the mapping of IMSI to Global_CN_ID until the **tnnsf-timer** expires

Example

The following command sets the NNSF timer value to *30* seconds in an HNB-GW service instance:

default tnssf-timer

ue registration-timeout

Configures the UE registration timeout duration to de-register the connected UE from an HNB-GW service.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

Syntax Description

ue registration-timeout *dur*
{ default | no } ue registration-timeout

no

Disables the UE registration timeout duration and explicitly de-registers UE from the HNB-GW service.

default

Restores the UE registration timeout duration value to its default value of 120 seconds.

dur

Sets the UE registration timeout duration (in seconds) after which the UE is de-registered from HNB-GW. In a scenario when all Iu connections are released for a subscriber, the HNB-GW service de-registers the UE after the configured duration only.

dur is an integer from 60 through 300. Default: 120

Usage Guidelines

Use this command to configure the minimum duration value before de-registering the UE when subscriber fails to establish the Iu connection. If subscriber's Iu session does not established before configured period then UE is de-registered. Also in a scenario where all Iu connections are released for a subscriber, the HNB-GW service waits for configured period before starting UE deregistration procedure.

Example

The following command sets the UE registration timeout duration to *150* second on HNB-GW after expiry of which the UE is de-registered:

```
ue registration-timeout 150
```