eGTP Service Configuration Mode Commands

The eGTP Service Configuration Mode is used to create and manage Evolved GPRS Tunneling Protocol (eGTP) interface types and associated parameters.

Command Modes

Exec > Global Configuration > Context Configuration > eGTP Service Configuration

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

Entering the above command sequence results in the following prompt:

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

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

Important The commands should be added or removed in the startup config only and not when the node is live.

- associate, on page 1
- allow-lte-m-rat, on page 3
- collision-handling, on page 3
- cups-enabled, on page 4
- end, on page 5
- exit, on page 6
- gtpc, on page 6
- interface-type, on page 13
- pool, on page 15
- ran-nas decode proto-type-spare cause-value-length, on page 17
- validation-mode, on page 17

associate

Configures an association with a GTP-U service where parameters are applied to the GTP-U data flow. For an SGSN being configured for S4 functionality, this command associates a configured GTP-U service that will enable communication with the SGW over the S4 interface.

Product

ePDG

P-GW

SAEGW

SGSN

SaMOG

Important For StarOS releases prior to 16, the ePDG and SGSN are only supported on the ASR 5500 platform.

Important It is recommended to execute the S4 SGSN configuration commands during the maintenance window. After configuring the node, re-start the node to activate the configuration commands. This will ensure that the node is in a consistent state and S4 SGSN service instability scenarios are avoided.

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > eGTP Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

associate gtpu-service *name*
no associate gtpu-service

no

Removes the association to the configured GTP-U service from this service.

gtpu-service *name*

Associates a GTP-U service with this eGTP service. *name* must be an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to associate a GTP-U service with this eGTP service.

Important If you modify this command, the parent service (service within which the eGTP/GTP-U service is configured) will automatically restart. Service restart results in dropping of active calls associated with the parent service.

Example

The following command associates this eGTP service with a GTP-U service named *gtpu3*:

```
associate gtpu-service gtpu3
```

allow-lte-m-rat

Enables **lte-m-rat** as a new RAT type.

Product

ePDG

P-GW

SAEGW

Important For StarOS releases prior to 16, the ePDG and SGSN are only supported on the ASR 5500 platform.

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > eGTP Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
allow-lte-m-rat
[ no ] gtpc node-feature lte-m
```

no

Disables the LTE-M configuration.

gtpc node-feature lte-m

The **gtpc node-feature lte-m** CLI command is disabled by default.

Usage Guidelines

Use this command to enable LTE-M as new RAT type.

collision-handling

Enables operators to configure the behavior of the P-GW for collision handling of the Delete Bearer command (DBcmd) message when the Modify Bearer Request (MBreq) message for the default bearer is pending at the P-GW or S-GW.

Product

P-GW

S-GW

Privilege

Administrator, Security Administrator

Command Modes

Exec > Global Configuration > Context Configuration > eGTP Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

collision-handling dbcmd-over-mbreq { drop | queue }
[default | no] collision-handling dbcmd-over-mbreq

default

Returns the collision handling for the DBcmd over MBReq transaction to the default behavior. The default behavior is to use pre-StarOS 19.0 behavior: abort the MBReq message and handle the DBcmd message.

no

Disables collision handling for the **dbcmd-over-mbreq** transaction.

collision-handling

Enables collision handling for the **dbcmd-over-mbreq** transaction.

drop

Configures the P-GW to drop the DBcmd message when the MBreq message is pending.

queue

Configures the P-GW to queue the DBcmd message when the MBreq is message is pending.

Usage Guidelines

Use this command when you want more flexibility in configuring the behavior of the P-GW for collision handling of the Delete Bearer command (DBcmd) message when the Modify Bearer Request (MBreq) message for the default bearer is pending at the P-GW.

An EGTP service must be configured in EGTP Service Configuration Mode in order to use this command.

Example

This command configures the P-GW to queue the DBcmd message when the MBreq is message is pending.

collision-handling dbcmd-over-mbreq queue

cups-enabled

Important This command is available in this release only for testing purposes. For more information, contact your Cisco Account representative.

Configures eGTPC service with CUPS mode that is applicable only for SAEGW service.

Product

SAEGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > eGTP Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] cups-enabled*name*

no

Removes the association to the configured GTP-U service from this service.

Usage Guidelines

The following services should be in STARTED state, and associated under SAEGW service for SAEGW service to move to STARTED state:

1. All eGTPC services should be configured with cups-enabled CLI.
   - S-GW Ingress Service (which is configured as part of SAEGW S-GW Service)
   - S-GW Egress Service (which is configured as part of SAEGW S-GW Service)
   - P-GW Ingress Service (which is configured as part of SAEGW P-GW Service)
2. Other dependent Services like:
   - Sx Service
   - GTP-U Service

There is no requirement to configure GTP-U service under eGTPC service, in case **cups-enabled** CLI is enabled. If GTP-U service is configured along with cups-enabled CLI, then it will not have any affect.

There is no change in non-CUPS behavior.

Any variation in the above mentioned configuration of SAEGW service will not get the Service in STARTED state. The same would be displayed in **show configuration errors** CLI command.

The **show egtp-service all** for eGTPC and **show saegw-service all** for SAEGW will display if the services are CUPS enabled.

The **cups-enabled** CLI command must not be used for standalone P-GW and S-GW service.

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.

gtpc

Configure the GPRS Tunneling Protocol Control (GTP-C) plane settings for this service.

Product ePDG

MME

P-GW

S-GW

SAEGW

SaMOG

SGSN

Privilege Administrator

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
gtpc { allow-on-congestion { apn-name apn_name | arp priority_level } | bind
 { ipv4-address ipv4_address [ ipv6-address ipv6_address ] | ipv6-address
ipv6_address [ ipv4-address ipv4_address ] }  | command-messages {
dual-ip-stack-support } | disable cause-source | echo-interval seconds [
dynamic [ smooth-factor multiplier ] ] echo-max-retransmissoins number |
echo-retransmission-timeout seconds | error-response-handling |
peer-salvation | ip qos-dscp { forwarding_type |
max-remote-restart-counter-change integer } | max-retransmissions num |
node-feature {  cellular-iot network-triggered-service-restoration |
pgw-restart-notification } | path-failure detection-policy { echo |
control-restart-counter-change | echo-restart-counter-change } |
```

private-extension overcharge-protection | reject s2b-ho-no-context | retransmission-timeout *seconds* **| retransmission-timeout-ms** *milliseconds* **}**
no gtpc { allow-on-congestion { apn-name *apn_name* **| arp** *priority_level* **} | bind { ipv4-address** *ipv4_address* [ipv6-address *ipv6_address*] **| ipv6-address** *ipv6_address* **[ipv4-address** *ipv4_address*] **} | command-messages { dual-ip-stack-support } | disable cause-source | echo-interval | error-response-handling | node-feature { cellular-iotnetwork-triggered-service-restoration | pgw-restart-notification } | path-failure detection-policy | private-extension overcharge-protection | reject s2b-ho-no-context }**
default gtpc disable cause-source |{ echo-interval | echo-max-retransmissons | echo-retransmission-timeout disable cause-source| ip qos-dscp | max-retransmissions | node-feature { cellular-iot network-triggered-service-restoration | pgw-restart-notification } | path-failure detection-policy | retransmission-timeout | retransmission-timeout-ms }

no

Disables or removes the configured GTP-C setting.

default

Resets the specified parameter to its default value.

allow-on-congestion { apn-name *apn_name* | arp *priority_level* }

Important ***P-GW, SAEGW, and S-GW only***. This functionality requires that a valid VoLTE license key be installed. Contact your Cisco account representative for information on how to obtain a license.

Enables the prioritized handling for calls under congestion conditions for the specified APN/ARP(s).

- If prioritized APN/ARP handling is enabled, and if the APN/ARP received in a CSReq at the EGTP demux matches any of the configured prioritized APN/ARP values, any valid CSReq will not be rejected at EGTP demux because of congestion control.
- This feature impacts only CSReq handling for new incoming calls.
- P-GW initiated dedicated bearer creation/updating is not changed due to this configuration.

apn-name *apn_name*: Configures the gateway to allow calls for this Access Point Name (APN), even under congestion. *apn_name* is an alphanumeric string of 1 through 64 characters. A maximum of 3 APNs can be configured.

arp *priority_level*: Configures the gateway to allow calls for this ARP, even under congestion. *priority_level* sets the priority value as an integer from 1 to 15. A maximum of 8 ARP values can be configured.

Important There is no APN-to-ARP mapping.

bind { ipv4-address *ipv4_address* [ipv6-address *ipv6_address*] | ipv6-address *ipv6_address* [ipv4-address *iv4p_address*] }

Binds the service to an interface with IPv4 address, IPv6 address, or both.

ipv4-address *ipv4_address* **[ipv6-address** *ipv6_address* **]**: Binds this service to the IPv4 address of a configured interface. Optionally, bind the service to a configured interface with an IPv6 address.

ipv4_address must be entered using IPv4 dotted-decimal notation.

ipv6_address must be entered using IPv6 colon-separated hexadecimal notation.

ipv6-address *ipv6_address* **[ipv4-address** *ipv4_address* **]**: Binds this service to the IPv6 address of a configured interface. Optionally, bind the service to a configured interface with an IPv4 address.

ipv6_address must be entered using IPv6 colon-separated hexadecimal notation.

ipv4_address must be entered using IPv4 dotted-decimal notation.

Important For binding GTP-C service on S2b interface, either IPv6 or IPv4 bind address shall be used. Binding both IPv4 and IPv6 address is not supported on ePDG.

The **ipv6-address** *ipv6_address* **[ipv4-address** *ipv4_address* **]** option is not currently supported on the SGSN.

cellular-iot

Enables the Cellular IoT features supported for eGTP Service.

command-messages dual-ip-stack-support

command-messages: Configuration related to MBC/DBC/BRC messages on S-GW and P-GW.

dual-ip-stack-support: Enables to handle command messages on both IPv4/IPv6 transport if supported. By default feature is enabled.

disable cause-source

disable: Disables functionality at eGTPC level.

cause-source: Disables cause source Bit in Cause IE.

echo-interval *seconds* [dynamic [smooth-factor *multiplier*]]

Configures the duration (in seconds) between the sending of echo request messages. *seconds* is an integer from 60 to 3600.

Default: 60

dynamic: Enables the dynamic echo timer for the eGTP service. The dynamic echo timer uses a calculated round trip timer (RTT) to support variances in different paths to peer nodes.

smooth-factor *multiplier*: Introduces a multiplier into the dynamic echo timer. *multiplier* is an integer from 1 to 5.

Default: 2

max-remote-restart-counter-change *integer*

Specifies the counter change after which the P-GW will detect a peer restart. Note that a peer restart will be detected only if the absolute difference between the new and old restart counters is less than the value configured. For example, if the **max-remote-restart-counter-change** is 10 and the current peer restart counter is 251, then eGTP will detect a peer restart only if the new restart counter is 252 through 255 or 0 through 5. Similarly, if the stored restart counter is 1, eGTP will detect a peer restart only if the new restart counter is 2 through 11.

Valid settings are from 1 to 255.

The recommended setting is 32.

The default setting is 255.

echo-max-retransmissions *number*

Configures the maximum retries for GTP Echo requests. *number* is an integer from 0 to 15. If **echo-max-retransmissions** option is not configured, then the **max-retransmissions** configuration will be used for maximum number of echo retries.

Default: 4

echo-retransmission-timeout *seconds*

Configures the echo retransmission timeout, in seconds, for the eGTP service. *seconds* is an integer ranging from 1 to 20.

If dynamic echo is enabled (**gtpc echo-interval dynamic**) the value set in this command serves as the dynamic minimum (if the RTT multiplied by the smooth factor is less than the value set in this command, the service uses this value).

Default: 3

error-response-handling

Enables error-response-handling on the S-GW. If this command is enabled in the eGTP service, then on receiving a bad response from the peer instead of dropping the message while doing validation eGTP-C informs the S-GW about the bad response received. The S-GW uses this notification from eGTP-C that a bad response is received to send a proper response to the other peer.

peer-salvation

Enables peer salvation for inactive GTPv2 peers for EGTP services in this context. When enabled, this functionality is enabled at the specific egtp-service level.

This functionality should be enabled at the context level if it is enabled at the egtp-service level. The configuration sequence is not dependent on enabling this functionality.

The parameter configured at the context level is used when peer-salvation is enabled. Ensure that peer-salvation is configured at all the configured services of a product. For example, sgw-services (egtp-service).

Note

- The parameter configured at the context level is used when peer-salvation is enabled. Ensure that peer-salvation is configured at all the configured services of a product. For example, sgw-services (egtp-service).
- All the information (peer statistics/recovery counter and so on) of the particular peer is lost after it is salvaged.
- The context level configuration is applied to egtpinmgr and egtpegmgr separately.

ip qos-dscp { *forwarding_type* }

Specifies the IP QoS DSCP per-hop behavior (PHB) to be marked on the outer header of signalling packets originating from the LTE component. This is a standards-based feature (RFC 2597 and RFC 2474).

Note that CS (class selector) mode options below are provided to support backward compatibility with the IP precedence field used by some network devides. CS maps one-to-one to IP precedence, where CS1 is IP precedence value 1. If a packet is received from a non-DSCP aware router that used IP precedence markings, then the DSCP router can still understand the encoding as a Class Selector code point.

The following forwarding types are supported:

- **af11**: Designates the use of Assured Forwarding 11 PHB.

  This is the default setting.
- **af12**: Designates the use of Assured Forwarding 12 PHB.
- **af13**: Designates the use of Assured Forwarding 13 PHB.
- **af21**: Designates the use of Assured Forwarding 21 PHB.
- **af22**: Designates the use of Assured Forwarding 22 PHB.
- **af23**: Designates the use of Assured Forwarding 23 PHB.
- **af31**: Designates the use of Assured Forwarding 31 PHB.
- **af32**: Designates the use of Assured Forwarding 32 PHB.
- **af33**: Designates the use of Assured Forwarding 33 PHB.
- **af41**: Designates the use of Assured Forwarding 41 PHB.
- **af42**: Designates the use of Assured Forwarding 42 PHB.
- **af43**: Designates the use of Assured Forwarding 43 PHB.
- **be**: Designates the use of Best Effort forwarding PHB.
- **cs1**: Designates the use of Class Selector code point "CS1".
- **cs2**: Designates the use of Class Selector code point "CS2".
- **cs3**: Designates the use of Class Selector code point "CS3".
- **cs4**: Designates the use of Class Selector code point "CS4".

- **cs5**: Designates the use of Class Selector code point "CS5".
- **cs6**: Designates the use of Class Selector code point "CS6".
- **cs7**: Designates the use of Class Selector code point "CS7".
- **ef**: Designates the use of Expedited Forwarding PHB typically dedicated to low-loss, low-latency traffic.

The assured forwarding behavior groups are listed in the table below.

	Class 1	Class 2	Class 3	Class 4
Low Drop	AF11	AF21	AF31	AF41
Medium Drop	AF12	AF22	AF32	AF42
High Drop	AF13	AF23	AF33	AF43

Traffic marked with a higher class is given priority during congestion periods. If congestion occurs to traffic with the same class, the packets with the higher AF value are dropped first.

max-retransmissions *num*

Configures the maximum number of retries for packets as an integer from 0 through 15.

After maximum retransmissions is reached, the path is considered to be failed.

Default: 4

node-feature pgw-restart-notification

Enables P-GW Restart Notification functionality. Node will start announcement of new supported features to peer nodes in echo as soon as configuration is added.

From release 17.0 onwards, the S4-SGSN and MME support receiving/advertising the P-GW Restart Notification (PRN). This command option must be configured in order to inform S-GW that S4-SGSN and/or MME supports receiving/advertising the PRN in eGTPC echo request/response messages.

Default: Disabled

node-feature network-triggered-service-restoration

This keyword applies to MME and S-GW only.

Enables Network Triggered Service Restoration (NTSR) functionality as per 3GPP TS 23.007 Release 11 for this eGTP service.

Upon receipt of a Downlink Data Notification (DDN) message including an IMSI, the MME will accept the request and initiate paging including the IMSI in order to force the UE to re-attach. IMSI-based DDN requests contain a zero TEID. Since the UE is not attached, the UE will be paged over the whole MME coverage area.

A different MME may be selected by the eNodeB to service the attach request. Since the MME that serviced the DDN will not be aware that the UE has responded with the attach request, it will stop paging upon a timeout.

path-failure detection-policy echo

Enables session cleanup upon path failure detected via ECHO timeout toward a peer.

Default: Enabled

If disabled, there is no session cleanup upon path failure detected via ECHO timeout toward a peer; however, SNMP trap/logs will continue to indicate path failure.

path-failure detection-policy control-restart-counter-change

Enables path failure detection policy when the restart counter in Echo Request/Echo Response messages changes. Used in conjunction with the **max-remote-restart-counter-change** command.

path-failure detection-policy echo-restart-counter-change

Enables path failure detection policy when the restart counter in Control Request/Control Response messages changes. Used in conjunction with the **max-remote-restart-counter-change** command.

private-extension overcharge-protection

Important From StarOS 19.0 and later releases, this command is obsolete.

Important Use of Overcharging Protection requires that a valid license key be installed. Contact your Cisco account representative for information on how to obtain a license.

Controls whether the PDU will contain overcharge-protection related data in the Indication information element or in the private extension.

- If this keyword is enabled in the eGTP service, then eGTP-C will encode/decode overcharge-protection related data in/from the private extension instead of the Indication IE.
- If this option is disabled in the eGTP service, then the eGTP-C layer will encode/decode overcharge-protection related data in the Indication IE.
- By default, this option is disabled.

reject s2b-ho-no-context

Allows handoff call on S2b interface, even when eGTP-C does not have a UE context.

retransmission-timeout *seconds*

Important In 17.3 and later releases, this option has been deprecated. Use the **retransmission-timeout-ms** option.

Configures GTPv2 control packets (non-echo) retransmission timeout (in seconds) as an integer from 1 to 20.

Default: 5

retransmission-timeout-ms *milliseconds*

Configures the control packet retransmission timeout in GTP, in milliseconds <in steps of 100>, ranging from 1000 to 20000.

Default: 5000

Usage Guidelines

Use this command to configure GTP-C settings for the current service.

This interface assumes the characteristics of an S11 reference point on the S-GW or MME.

For communication between the S4-SGSN and LTE S-GW, the interface assumes the characteristics of an S4 reference point on the S4-SGSN. Before using the **gtpc** command on the S4-SGSN, a new or existing service must be created or entered using the **egtp-service** command in the *Context Configuration Mode*. Once the eGTP service is configured, the service must be associated with the configured 2G and/or 3G services on the S4-SGSN using the **associate** command in the *SGSN Service Configuration Mode* and/or *GPRS Service Configuration Mode.*

Important If you modify this command, the parent service (service within which the eGTP/GTP-U service is configured) will automatically restart. Service restart results in dropping of active calls associated with the parent service.

Important For ePDG, IPv6 bind address must be used as ePDG supports IPv6 as transport on the S2b interface.

Example

The following command binds the service to a GTP-C interface with an IPv4 address of *112.104.215.177*:

```
gtpc bind ipv4-address 112.104.215.177
```

interface-type

Configures the interface type used by this service.

Product

ePDG

MME

P-GW

SAEGW

S-GW

SaMOG

SGSN

Important It is recommended to execute the S4 SGSN configuration commands during the maintenance window. After configuring the node, restart the node to activate the configuration commands. This will ensure that the node is in a consistent state and S4 SGSN service instability scenarios are avoided.

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > eGTP Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
interface-type { interface-cgw-egress | interface-epdg-egress |
interface-mme | interface-pgw-ingress [ s2a ] [ s2b ] | interface-sgsn |
 interface-sgw-egress | interface-sgw-ingress }
```

interface-cgw-egress

Specifies the SaMOG Gateway's EGTP interface for egress.

interface-epdg-egress

Specifies that the interface has the characteristics of an ePDG's egress EGTP interface.

interface-mbms-egress

This keyword is for future development.

interface-mme

Specifies that the interface has the characteristics of an eGTP MME S11 reference point to/from an S-GW or an eGTP MME Sv reference point to/from a Mobile Switching Center (MSC).

interface-pgw-ingress [s2a] [s2b]

Specifies that the interface has the characteristics of an eGTP P-GW S5/S8 reference point from an S-GW. The interface assumes the characteristics of either a GTP-C (control Plane) or GTP-U (user plane) reference point.

- **s2a**: P-GW supports the S2a interface. SAEGW does not support the S2a interface at this time.
- **s2b**: P-GW supports the S2b interface. S2b interface support is available on the SAEGW in 18.2 and later releases.

Note The **S2a** and **S2b** keywords will be available only if a valid license is installed. For more information, contact your Cisco account or support representative.

interface-sgsn

Specifies that the interface has the characteristics of an eGTP S-GW S4 reference point to/from an SGSN. On an S4-SGSN, this option specifies that the eGTP service is used for an S4-SGSN and gives the service the characteristics required for messaging towards an S-GW (S4) / MME (S3) / S4-SGSN (S16).

interface-sgw-egress

Specifies that the interface has the characteristics of an eGTP S-GW S5/S8 reference point to an eGTP P-GW. The interface assumes the characteristics of either a GTP-C (control Plane) or GTP-U (user plane) reference point.

interface-sgw-ingress

Specifies that the interface has the characteristics of:

- An eGTP-C S-GW S11 reference point from the MME.
- An eGTP-U S-GW S1-U reference point from the eNodeB.

Usage Guidelines

Use this command to specify the type of interface that this service uses. By configuring this command, the interface takes on the characteristics of the selected type.

Disable specific interface support for P-GW by entering the following command:

```
interface-type interface-pgw-ingress
```

Important If you modify this command, the parent service (service within which the eGTP/GTP-U service is configured) will automatically restart. Service restart results in dropping of active calls associated with the parent service.

Example

The following command configures the interface bound to this service to maintain the characteristics of an eGTP-C S-GW S11 reference point from an MME:

```
interface-type interface-sgw-ingress
```

The following command accepts or rejects Create Session Request (CSR) on GTP based S2a interface:

```
interface-type interface-pgw-ingress s2a
```

pool

This command enables the default S4-SGSN functionality for (flex) pooling and enables inclusion of the configured pool hop-counter count in new SGSN context/identity request messages. This command supports S4-SGSN pooling across the S16 interface. The S16 interface provides a GTPv2 path to a peer S4-SGSN.

Support for the S16 interface is provided as part of the S4 interface license. This command sets the S4-SGSN as the default SGSN within a pool. If the default S4-SGSN receives an inbound SGSN context request, it forwards it to the right SGSN in the pool based on the NRI bits of the P-TMSI.

Product

SGSN

Important It is recommended to execute the S4 SGSN configuration commands during the maintenance window. After configuring the node, restart the node to activate the configuration commands. This will ensure that the node is in a consistent state and S4 SGSN service instability scenarios are avoided.

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > eGTP Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
pool { default-sgsn | hop-counter count }
no pool default-sgsn
```

no

Disables the default SGSN pooling functionality or removes the SGSN pool hop-counter IE from the GTP Identity/context requests.

default-sgsn

Enables the default SGSN pooling functionality.

hop-counter *count*

Enables and configures the SGSN pool hop-counter to set the number of hops and to include the configured count in the **new** SGSN Context Requests or the **new** SGSN Identity Requests. *count* is an integer from 1 to 255.

If **default-sgsn** is enabled, then any messages relayed will have the default value of 4 for the counter if the message does not include this hop-counter ID.

Default: 4

Usage Guidelines

Use this command to enable the default flex functionality without exposing the pool (flex) structure. This functionality provides a means for SGSNs outside of the pool to reach a pooled SGSN on the basis of its NRI.

Once the pooling has been enabled, repeat the command using the **hop-counter** keyword to enable inclusion of the hop-counter IE in SGSN context/identity request messages and to configure the count for the pooling hop-counter. If the SGSN is behaving as the 'default SGSN', this SGSN will forward (relay) requests with the hop-count included to the target SGSN.

Example

The following command enables the default pooling functionality which allows an outside SGSN to reach a pooled SGSN:

```
pool default-sgsn
```

The following command sets *25* hops to be included in messages:

```
pool hop-count 25
```

ran-nas decode proto-type-spare cause-value-length

Configures the spare protocol types for the RAN/NAS IE. The cause value and length for the spare protocol type IE can also be configured.

Note

- This CLI configuration is supported only for the S2b interface.
- Spare protocol types are supported only for Failed Create Bearer Response/Failed Update Bearer Response messages.

Product

P-GW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > eGTP Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
ran-nas decode proto-type-spare cause-value-length <1 | 2>
```

cause-value-length

Specifies the length of cause value to be decoded.

<1 | 2>

The cause length value can be 1 octet or octets. The default value is 2 octets.

Usage Guidelines

Use this command to specify the spare protocol types for the RAN/NAS IE. If there is a mismatch between length of cause value IE and configured CLI value, the IE is ignored.

Example

The following command sets the length of the cause value to be decoded.

```
ran-nas decode proto-type-spare cause-value-length 2
```

validation-mode

Configures the type of validation to be performed on messages received by this service.

Product

ePDG

P-GW

SAEGW

SGSN

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > eGTP Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
validation-mode { custom1 | standard }
default validation-mode
```

default

Returns the command to the default setting.

Default: **standard**

{ custom1 | standard }

custom1: Specifies that the message should be validated based on a vendor-specific set of mandatory elements.

standard: Specifies that the message should be validated based on the set of mandatory elements as defined in 3GPP 29.274. This is the default option on an S4-SGSN.

Usage Guidelines

Use this command to specify the type of validation performed on messages received by this service. The information elements contained in messages have mandatory elements and conditional elements. The standard set of elements, as defined by 3GPP 29.274 is checked if this command is set to **standard**. The **custom1** setting is for a vendor-specific set of mandatory elements.

Example

The following command sets the validation mode for incoming messages to *standard*:

```
validation-mode standard
```