S-GW Service Configuration Mode Commands

The S-GW (Serving Gateway) Service Configuration Mode is used to create and manage the relationship between an eGTP service used for either ingress or egress control plane and user data plane network traffic.

Command Modes

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

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

Entering the above command sequence results in the following prompt:

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

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

accounting context

Configures the GTPP accounting context and group selection for S-GW service.

Product

S-GW

SAEGW

Privilege

Administrator

Command Modes

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

`accounting context` *`name`* **`[ gtpp group`** *`name`* **`]`**
`no accounting context`

no

Removes the configured accounting context from this service.

context *name*

Specifies the context where GTPP accounting is performed.

name must be an existing context configured on the system expressed as an alphanumeric string of 1 through 79 characters.

If an accounting context name is not configured in the S-GW service, the context where the S-GW service resides is considered the accounting context and the default GTPP group is used.

gtpp group *name*

Specifies a GTPP group used to perform GTPP accounting.

name must be an existing GTPP group configured on the system expressed as an alphanumeric string of 1 through 79 characters.

If a GTPP group is not configured, the system will use the default GTPP group in the specified accounting context. If the accounting context is not specified, the system will use default GTPP group in the context where the S-GW service resides.

Usage Guidelines

Use this command to specify the accounting context and/or GTPP accounting group the S-GW service will use to perform GTPP accounting.

Example

The following command specifies a GTPP accounting context named *acct-2* and a GTPP accounting group named *gtpp-grp-3* as the context and group the S-GW service will use:

`accounting context acct-2 gtpp group gtpp-grp-3`

accounting mode

Configures the mode to be used for accounting – GTPP (default), RADIUS/Diameter or None for S-GW service.

Product

S-GW

SAEGW

Privilege

Administrator

Command Modes

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ default ] accounting mode { gtpp | none | radius-diameter }`

default

Sets the accounting mode to GTPP.

gtpp

Specifies that GTPP accounting is performed. This is the default mode.

none

Specifies that no accounting will be performed for the S-GW service.

radius-diameter

Specifies that RADIUS/Diameter will be performed for the S-GW service.

Usage Guidelines

Use this command to specify the accounting mode for the S-GW service. However, an accounting mode configured for the call-control profile will override this setting. For additional information on accounting mode and its relationship to operator policy, refer to the *Serving Gateway Administration Guide*.

Example

The following command specifies that RADIUS/Diameter accounting will be used for the S-GW service:

`accounting mode radius-diameter`

accounting stop-trigger

Configures the trigger point for accounting stop CDR. Default is on session deletion request.

Product

S-GW

SAEGW

Privilege

Administrator

Command Modes

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
accounting stop-trigger custom
default accounting stop-trigger
```

default

Accounting stop CDR triggered once Delete Session/Delete Bearer Request is received at S-GW.

custom

Synchronizes the timestamp in the SGWRECORD CDR and PGWRECORD CDR if the MME cannot reach the UE. When configured, the SGW will also trigger the Accounting stop CDR after receiving the answer (accept for Delete session request) from the MME.

Usage Guidelines

Use this command to specify the trigger point for accounting stop CDR for this S-GW service.

Example

The following command specifies that accounting stop trigger would be at response of session deletion:

```
accounting stop-trigger custom
```

associate

Associates the S-GW service with QoS and policy control and charging configurations.

Product

S-GW

SAEGW

Privilege

Administrator

Command Modes

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

associate { access-peer-map | accounting-policy *name* **| egress-proto { gtp | gtp-pmip | pmip } [egress-context** *name* **| emps-profile** *emps_profile_name* **| gtpc-load-control-profile** *name* **| gtpc-overload-control-profile** *name* **[egtp-service** *name* **] [mag-service** *name* **]] | ims-auth-service** *name* **| ingress egtp-service** *name***| peer-map** *name* **| qci-qos-mapping** *name* **| subscriber-map** *name*

no associate { access-peer-map | accounting-policy | egress-proto [egress-context [egtp-service] [mag-service]] | emps-profile | ims-auth-service | ingress egtp-service | peer-map | qci-qos-mapping | subscriber-map }

no

Removes the specified association form the S-GW service.

access-peer-map*name*

Associates the access/ingress side of the peer-map to the configured S-GW service.

name must be an existing peer-map expressed as an alphanumeric string of 1 through 63 characters.

accounting-policy *name*

Associates the S-GW service with an accounting policy configured in the same context.

name must be an existing accounting policy expressed as an alphanumeric string of 1 through 63 characters.

Accounting policies are configured through the **policy accounting** command in the Context Configuration Mode.

egress-proto { gtp | gtp-pmip | pmip } [egress-context *name* [egtp-service *name*] [mag-service *name*]]

Associates and configures the egress protocol for this S-GW service.

gtp: Specifies that GTP is to be used for the S-GW service egress.

gtp-pmip: Specifies that either GTP or PMIP is to be used for the S-GW service egress.

pmip: Specifies that PMIP is to be used for the S-GW service egress.

egress-context *name*: Specifies that the context in this keyword is to be used for the S-GW service egress.

name must be an existing context on this system expressed as an alphanumeric string of 1 through 63 characters.

egtp-service *name*: Specifies that the service in this keyword is to be used for the S-GW service egress.

name must be an existing eGTP service on this system expressed as an alphanumeric string of 1 through 63 characters.

mag-service *name*: Specifies that the service in this keyword is to be used for the S-GW service egress.

name must be an existing MAG service on this system expressed as an alphanumeric string of 1 through 63 characters.

emps-profile*emps_profile_name*

Specifies that an eMPS profile is to be associated with an existing S-GW service in this context.

emps_profile_name must be a string of size 1 to 63 and treated as case insensitive.

gtpc-load-control-profile *name*

Associates a configured GTPC Load Control Profile with this S-GW service.

name must be an existing GTPC Load Control Profile on this system expressed as an alphanumeric string of 1 through 64 characters.

gtpc-overload-control-profile *name*

name must be an existing GTPC Overload Control Profile on this system expressed as an alphanumeric string of 1 through 64 characters.

ims-auth-service *name*

Associates the S-GW service with an IMS authorization service configured in the same context.

name must be an existing IMS auth service and be from 1 to 63 alphanumeric characters.

IMS authorization services are configured through the **ims-auth-service** command in the Context Configuration Mode.

ingress egtp-service *name*

Associates and configures the eGTP service ingress for this S-GW service.

name must be an existing eGTP service on this system expressed as an alphanumeric string of 1 through 63 characters.

peer-map *name*

Associates the access/ingress side of the peer-map to the configured S-GW service

name must be an existing peer-map configuration expressed as an alphanumeric string of 1 through 63 characters.

qci-qos-mapping *name*

Associates the S-GW service with QCI to QoS mapping parameters.

name must be an existing QCI-QoS mapping configuration expressed as an alphanumeric string of 1 through 63 characters.

QCI-QoS mapping is configured through the **qci-qos-mapping** command in the Global Configuration Mode.

subscriber-map *name*

Associates the S-GW service with subscriber map parameters.

name must be an existing subscriber map configuration expressed as an alphanumeric string of 1 through 63 characters.

Subscriber maps are configured through the **subscriber-map** command in the LTE Policy Configuration Mode.

Usage Guidelines

Use this command to select a pre-configured QoS mapping and/or policy control and charging configuration to be used by the S-GW service.

Example

The following command associates the S-GW service with an IMS authorization service named *ims-23*:

```
associate ims-auth-service ims-23
```

ddn failure-action

Configures a timer value to delay paging for this UE when the S-GW has initiated a Downlink Data Notification (DDN) to the MME and has received back a DDN failure.

Product

S-GW

SAEGW

Privilege

Administrator

Command Modes

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

ddn failure-action pkt-drop-time *seconds*
default ddn failure-action pkt-drop-time

default

Resets the command to its default setting of 300 seconds.

failure-action pkt-drop-time *seconds*

Default: 300

Configures a timer that determines how long the S-GW will discard downlink data packets so the MME has enough time to receive the Modify Bearer Request and prevent further errors being sent to the S-GW in the DDN Ack message.

seconds must be an integer value from 1 to 300.

Usage Guidelines

Use this command to set a timer value to delay the sending of excessive Downlink Data Notification messages to the MME (and receiving excessive DDN Ack message with errors from the MME) in cases when downlink data is arriving before the Modify Bearer Request is received. During the delay, downlink data packets are discarded until the timer has expired. This timer is triggered upon receiving the first error in a DDN Ack message from the MME.

Related Functionality

DDN Delay: By default, the S-GW supports the delay value IE included in a DDN acknowledgement message. The S-GW automatically multiplies this value by 50 ms, then applies the calculated delay for DDN for the UE.

Example

The following command configures the S-GW to discard downlink data packets for *200* seconds after the S-GW receives an error in a DDN Ack message from the MME :

```
ddn failure-action pkt-drop-time 200
```

ddn isr-sequential-paging

Configures the delay time in 100 millisecond increments between paging of different RAT types in support of the Intelligent Paging for ISR feature.

Product

S-GW

SAEGW

Privilege

Administrator

Command Modes

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

ddn isr-sequential-paging delay-time *delay*
default ddn isr-sequential-paging

default

Returns the delay time to its default value of 10 (10 * 100 ms = 1 second).

delay-time *delay*

Configures delay between paging of different RAT types.

delay must be an integer from 1 to 255, representing increments of 100 milliseconds (*delay* = 1-255 * 100 ms).

Default: 10 (10 * 100 ms = 1 second)

Usage Guidelines

Use this command to configure the delay time in (100 millisecond increments) between paging of different RAT types in support of the Intelligent Paging for ISR feature.

Example

The following command configures the delay timer to 5 seconds.

```
ddn isr-sequential-paging delay-timer 50
```

ddn success-action no-user-connect ddn-retry-timer

Use this command to resend DDN if no MBR or DDN Failure is received within the specified timer value.

Product

S-GW

SAEGW

Privilege

Administrator

Command Modes

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

ddn success-action no-user-connect ddn-retry-timer *value_sec*
default ddn success-action no-user-connect ddn-retry-timer

default

Resets the command to its default setting of 60 seconds.

ddn success-action no-user-connect ddn-retry-timer *value_sec*

Resends DDN if no MBR or DDN Failure is received within the specified timer value.

value_sec: Valid entries are from 60 to 300 seconds.

Usage Guidelines

After receiving DDN Ack, this timer is started and when it expires, S-GW sends one DDN and restarts the timer for same value. If no MBR is received within this time, S-GW clears the data buffers and waits for new data to trigger a new DDN.

This configuration is applicable only for non-ISR calls. If ISR is active, this configuration will be ignored. This extra DDN is sent under extreme circumstances. So, neither DDN delay nor throttling will be applied on it.

Example

The following command configures the DDN retry timer to 180 seconds.

```
ddn success-action no-user-connect ddn-retry-timer 180
```

ddn temp-ho-rejection mbr-guard-timer

Sets the guard timer to wait for a MBR when DDN Ack with Cause #110 temp-ho-rejection) is received.

If the guard timer expires and if no MBR of any type or DDN Failure Indication is received, all the buffered downlink data is flushed out and paging flags are reset. If the guard timer is running and any MBR is received, the timer is stopped and no further action is taken. If the guard timer is running and DDN Failure Indication is received, the timer is stopped and standard DDN failure action is taken. By default, this CLI command is always enabled.

Product

S-GW

SAEGW

Privilege

Administrator

Command Modes

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

ddn temp-ho-rejection mbr-guard-timer *time_in_seconds*

no

Disables the guard timer.

default

Enables the guard timer and sets it to the default value, 60 seconds.

temp-ho-rejection

Action to be taken when peer node indicates temporary rejection of paging due to handover-in-progress.

mbr-guard-timer

Sets the guard timer for a MBR when DDN Ack with Cause #110 (temp-ho-rejection) is received. When the timer expires, S-GW flushes all the buffered downlink data packets. The range of this timer is from 60 seconds to 300 seconds. Default timer value is 60 seconds.

Usage Guidelines

Use this CLI command to enable guard timer to wait for MBR once the DDN Ack with cause#110 (Temporary Handover In Progress) is received. If the guard timer expires and if no MBR of any type or DDN Failure Indication is received, all the buffered downlink data is flushed out and paging flags are reset. If the guard timer is running and DDN Failure Indication is received, the timer is stopped and standard DDN failure action is taken.

By default, this CLI command is always enabled.

Example

The following CLI command sets the guard timer for 200 seconds to wait for a MBR when DDN Ack with Cause #110 temp-ho-rejection) is received.

```
ddn temp-ho-rejection mbr-guard-timer 200
```

ddn throttle

Configures Downlink Data Notification throttle parameters.

Product

S-GW

SAEGW

Privilege

Administrator

Command Modes

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
ddn throttle arp-watermark arp_value [ rate-limit limit time-factor seconds
throttle-factor percent increment-factor percent [ poll-interval seconds ]
throttle-time-sec seconds [ throttle-time-min minutes ] [ throttle-time-hour
 hour ] stab-time-sec seconds [ stab-time-min minutes ] [ stab-time-hour hour
 ]
no ddn-throttle
```

no

Disables the DDN throttling feature.

throttle arp-watermark *arp_value*

If ARP watermark is configured and if an MME/SGSN sends the throttling factor and delay in a DDN ACK message, all the DDNs which have an ARP value greater than the configured value will be throttled by the throttle factor for the specified delay.

arp_value is an integer from 1 through 15.

rate-limit *limit*

Configures the rate limit (Use this and subsequent tokens to rate-limit only if the MME is a Non-Release 10 MME).

limit is an integer from 1 through 999999999.

time-factor *seconds*

Configures the time duration during which the S-GW makes throttling decisions.

seconds is an integer from 1 to 300.

throttle-factor *percent*

Configures the DDN throttling factor. Enter the percentage of the DDN to be dropped upon detecting a DDN surge.

percent is an integer from 1 through 100.

increment-factor *percent*

Configures the DDN throttling increment factor. Enter the percentage by which the DDN throttling should be increased.

percent is an integer from 1 through 100.

poll-interval *seconds*

Configures the polling interval in DDN throttling.

seconds is an integer from 2 through 999999999.

throttle-time-sec *seconds*

Configures the DDN throttling time in seconds. Enter time period in seconds over which DDN are throttled at the S-GW.

seconds is an integer from 0 through 59.

throttle-time-min *minutes*

Configures the DDN throttling time in minutes. Enter time period in minutes over which DDN are throttled at the S-GW.

minutes is an integer from 0 through 59.

throttle-time-hour *hour*

Configures the DDN throttling time in hours. Enter time period in hours over which DDN are throttled at the S-GW.

hour is an integer from 0 through 310.

stab-time-sec *seconds*

Configures the DDN throttling stabilization time in seconds. Enter a time period in seconds over which if the system is stabilized, throttling will be disabled.

seconds is an integer from 0 through 59.

stab-time-min *minutes*

Configures the DDN throttling stabilization time in minutes. Enter a time period in minutes over which if the system is stabilized, throttling will be disabled.

minutes is an integer from 0 through 59.

stab-time-hour *hour*

Configures the DDN throttling stabilization time in hours. Enter a time period in hours over which if the system is stabilized, throttling will be disabled.

hour is an integer from 0 through 310.

Usage Guidelines

Use this command to throttle DDNs to allow for the creation of the tunnel and avoid unnecessary DDNs.

For a UE in idle mode, S1U bearers are not established. In such a case, if a downlink packet arrives for the UE, the S-GW initiates a paging procedure towards the MME. The MME in turn pages the UE in its tracking area to search for the UE. Upon receiving the paging request, the UE establishes S1U bearers. Too many DDN requests towards the MME from the S-GW could overload the MME. To reduce this load, the MME can dynamically request S-GW to reduce a certain percentage of DDN messages sent towards it for a given period time.

The S-GW supports the following IEs for this feature:

- ARP IE in Downlink Data Notification
- DL Low Priority Traffic Throttling IE in DDN Acknowledge Message

More information is available in Release 10 of 3GPP 29.274, section 5.3.4.3.

The S-GW supports DDN throttling for up to 24 MMEs. DDNs for additional MMEs (25+) will be sent as normal and will not be throttled.

Throttling statistics can be viewed by issuing the Exec mode command:

show sgw-service statistics all

Example

The following command sets the ARP watermark lowest priority to *10* seconds:

```
ddn throttle arp-watermark 10
```

If the ARP value provided is 10, all bearers with ARP value between 10-15 are treated as low priority bearers and are given throttling treatment. Throttling would not be enabled if the ARP value is not provided through S-GW service configuration. Also, the ARP IE in DDN message towards MME would not be included unless DDN throttling is configured in S-GW service.

do show

Executes all **show** commands while in Configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax Description

```
do show
```

Usage Guidelines

Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.

Caution

There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

egtp

Configures the temporary failure response for Delete Bearer or for Update Bearer Request - Modify Bearer Command (UBR-MBC) collision for S-GW.

Product

S-GW

Privilege

Administrator

Command Modes

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

[default | no] egtp cause-code temp-failure { dbr-proc| ubr-mbc-collision }

no

Disables the specified parameter.

cause-code

Configures the collision-handling failure response.

temp-failure

Configures the service to handle temporary failure from peer.

dbr-proc

Configures the service to send cause code 110 (temporary failure) for Delete Bearer failure response. The default behavior is disabled.

ubr-mbc-collision

Configures the service to send cause code 110 (temporary failure) for UBR-MBC collision. The default behavior is disabled.

Usage Guidelines

Use this command to configure and to enable the temporary failure response for Delete Bearer or for UBR-MBC collision.

egtp-service

Configures an eGTP service to use as either an ingress (S1-U) or egress (S5/S8) service for the S-GW.

Product

S-GW

SAEGW

Privilege

Administrator

Command Modes

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

egtp-service { egress { context *name* **| service** *name* **} | ingress service** *name* **}**
no egtp-service { egress { context | service } | ingress service }

no

Removes the selected EGTP service from this service.

egress { context *name* | service *name* }

Specifies the egtp-service to be used as the egress eGTP service on a GTP-based S5/S8 interface.

context *name*: Specifies the name of the context where the eGTP service resides.

name must be an existing context name where an eGTP service resides expressed as an alphanumeric string of 1 through 63 characters.

service *name*: Specifies the name of the egress eGTP service.

name must be an existing eGTP service name expressed as an alphanumeric string of 1 through 63 characters.

ingress service *name*

Specifies the egtp-service to be used as the ingress eGTP service on the S11 interface.

name must be an existing eGTP service name expressed as an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to configure the eGTP service to use with this S-GW service. The eGTP service must be existing and be configured with the appropriate parameters supporting the intended service type.

Example

The following command configures the S-GW service to use an eGTP service named *s1u-egtp* as its ingress service:

egtp-service ingress service slu-egtp

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 handle-collision upc nrupc

This command helps in enabling or disabling collision handling between SGSN initiated UPC and NRUPC request.

Product

S-GW

Privilege

Security Administrator, Administrator

Command Modes

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ no | default ] gtpc handle-collision upc nrupc`

no

Disables collision handling between SGSN initiated UPC and NRUPC request.

default

Sets default collision handling behavior between SGSN initiated UPC and NRUPC request. By default, collision handling is enabled.

handle-collision upc nrupc

Enables/Disables collision handling between SGSN initiated UPC and network requested UPC. By default, collision handling is enabled.

Usage Guidelines

This command is used to enable or disable collision handling between SGSN initiated UPC and NRUPC request.

Example

The following example disables collision handling between SGSN initiated UPC and NRUPC request.

`no gtpc handle-collision upc nrupc`

gtpu-error-ind

Configures the actions to be taken upon receiving a GTP-U error indication from an RNC, eNodeB, SGSN, or P-GW.

Product

S-GW

SAEGW

Privilege

Administrator

Command Modes

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
gtpu-error-ind { { s12 | s1u | s11u } { local-purge | page-ue [
custom1-behavior ] } | { s4u | s5u } { local-purge | signal-peer } }
default gtpu-error-ind { s12 | s1u | s11u | s4u | s5u }
```

default

Resets the command to the default action for the specified interface. For S12 and S1-U, **page-ue** is the default action. For S4-U and S5-U, **local-purge** is the default action.

{ s12 | s1u | s11u }{ local-purge | page-ue [custom1-behavior] }

Specifies the action to take when a GTP-U error indication is received from a Radio Network Controller (RNC) over an S12 interface or from an eNodeB over the S1-U interface.

local-purge: The S-GW clears the affected bearer (or PDN if error-indication is received on default bearer) locally without informing peer.

page-ue [custom1-behavior]: The S-GW moves the complete UE state to S1-Idle and starts paging for this UE. If the custom1-behavior option is specified, the S-GW will guard the paging attempt with a timer of 60 seconds. Within this time the bearer must have the eNodeB TEID refreshed by an MME. Otherwise, the S-GW will clear the affected bearer with signaling. This is the default action for GTP-U error indication messages received on the S12 and S1-U interfaces.

{ s4u | s5u }{ local-purge | signal-peer }

Specifies the action to take when a GTP-U error indication is received from an SGSN over an S4-U interface or from a P-GW over the S5-U interface.

local-purge: The S-GW clears the affected bearer (or PDN if error-indication is received on a default bearer) locally without informing the peer. This is the default action for GTP-U error indication messages received on the S4-U and S5-U interfaces.

signal-peer: The S-GW initiates control signalling towards the peer MME and P-GW. When signalling:

- For a bearer deletion, the S-GW sends a Delete-Bearer-Command message to the P-GW and a Delete-Bearer-Request (with EBI) message to the MME.

- For PDN deletion, the S-GW sends a Delete-Session-Request message to the P-GW and a Delete-Bearer-Request (with LBI) message to the MME.
- The S-GW will not wait for Delete replies from the peer. The request will be sent only once and local resources will be reset.

Usage Guidelines

Use this command to specify the action to taken upon receiving a GTP-U error indication from an RNC over an S12 interface, an eNodeB across an S1-U interface, an SGSN over an S4-U interface, or from a P-GW across an S5-U interface.

Example

The following command sets the action to take upon receipt of a GTP-U error indication from the eNodeB to clear affected bearer:

```
gtpu-error-ind s1u local-purge
```

mag-service

Identifies the Mobile Access Gateway (MAG) egress service through which calls are to be routed for this S-GW service.

Product

S-GW

Privilege

Administrator

Command Modes

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

mag-service egress service *name*
no mag-service egress service

no

Removes the configured MAG egress service from this service.

egress service *name*

Specifies the MAG service name to be used as the egress MAG service on a Proxy Mobile IPv6 (PMIP) based S5/S8 interface.

name must be an existing MAG service expressed as an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to specify the name of the MAG service where calls are to be routed.

Example

The following command specifies that an existing MAG service named *mag3* is to be used to route call through for this S-GW service:

```
mag-service egress service mag3
```

ntsr session-hold timeout

Configures a timer to hold the session after path failure is detected at the MME (for Network Triggered Service Restoration).

Product

S-GW

Privilege

Administrator, Security Administrator

Command Modes

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] ntsr session-hold timeout *seconds*

no

Disables the NTSR session-hold timeout.

ntsr session-hold timeout *seconds*

Configures the timer duration, in seconds, that determines how long the session will be held after path failure is detected during MME restoration. Valid entries are from 1 to 3600 seconds.

Usage Guidelines

Use this command to configure the timer duration, in seconds, that determines how long the session will be held after path failure is detected during MME restoration.

Example

To configure the ntsr session-hold timeout for 10 seconds.

```
ntsr session-hold timeout 10
```

page-ue

Allows the S-GW to page the UE for P-GW-initiated procedures (Create Bearer Request (CBR)/Modify Bearer Request (MBR)/Update Bearer Request (UBR)) when the UE is idle, and sends a failure response to the P-GW with the cause code 110 (Temporary Failure) when the UE is idle or a collision is detected at the S-GW.

Product

S-GW

SAEGW

Privilege

Administrator

Command Modes

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

[default | no] page-ue pgw-initiated-proc

default

Returns the command to its default setting of disabled.

no

Disables the feature.

pgw-initiated-proc

Sets the command to page the UE for P-GW initiated MBR, UBR, and CBR procedures.

Usage Guidelines

Use this command to allow the S-GW to page a UE for P-GW-initiated procedures (CBR/MBR/UBR) when the UE is idle, and sends a failure response to the P-GW with the cause code 110 (Temporary Failure) when the UE is idle or a collision is detected at the S-GW.

Example

The following command enable the S-GW to page the UE

page-ue pgw-initiated-proc

paging-policy-differentiation

Controls Paging Policy Differentiation (PPD) functionality on the S-GW.

Product

S-GW

Privilege

Administrator, Security Administrator

Command Modes

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ default | no ] paging-policy-differentiation`

default

Restores the PPD functionality to its default setting of disabled.

no

Disables this option. This is the default setting.

paging-policy-differentiation

When S-GW supports the PPD feature, it shall include Paging and Service Information IE in the Downlink Data Notification message triggered by the arrival of downlink data packets at the S-GW. The Paging Policy Indication value within this IE will contain the value of the DSCP in TOS (IPv4) or TC (IPv6) information received in the IP payload of the GTP-U packet from the P-GW.

It is up to MME/S4-SGSN to use the Paging and Service Information IE of DDN message.

To support PPD feature in SAEGW, both S-GW and P-GW configuration is required.

Usage Guidelines

Use this command to enable/disable PPD functionality on S-GW.

Important

P-GW and S-GW should apply the PPD feature for both Default and Dedicated bearers. As per the specifications, P-GW transparently passes the user-datagram packet towards S-GW. This means, if PPD feature is enabled, operator can't apply different behavior for Default and Dedicated bearers.

Once the PPD feature is enabled, it is applicable for both existing and new calls.

If PPD feature is enabled at S-GW service, it is applicable for all calls irrespective of the APN profiles.

The PPD feature is license controlled under the license for S-GW Paging Profile. Once the license is enabled, both features co-exist together and work independently. That means, DDN message might carry both DSCP marking specified by PPD feature and Priority DDN value specified by S-GW Paging Profile feature.

At S-GW, the user-datagram packet DSCP value is used to send in DDN. S-GW can't change the DSCP, as per the local configuration (APN profile or service level). At eNodeB, the scheduling of the packet is based on the QCI instead of DSCP, however, any EPC node should not change/modify the inner DSCP value.

Important For the PPD feature to work, it must be enabled for P-GW and S-GW.

Both P-GW and S-GW services apply PPD configuration independently. Therefore, for any downlink data packet from an APN, there could be a case where P-GW does not have PPD configuration but S-GW has PPD configuration. To avoid such a conflict, you must configure the PPD functionality on both P-GW (APN level granularity) and S-GW (service level granularity).

See the *Paging Policy Differentiation* chapter in the *S-GW Administration Guide* for detailed information on PPD functionality.

Example

To enable PPD functionality on S-GW, enter the following command:

```
paging-policy-differentiation
```

path-failure

Configures the action to take upon the occurrence of a path failure between the S-GW and the MME, P-GW, RNC, SGSN, or eNodeB.

Product

S-GW

SAEGW

Privilege

Administrator

Command Modes

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
path-failure { s11 | s11u | s12 | s1u | s4 | s4u | s5 | s5u } ( local-purge
 | signal-peer }
default path-failure { s11 | s11u | s12 | s1u | s4 | s4u | s5 | s5u } (
local-purge | signal-peer }
```

default

Returns the command to the default setting of "local purge" for the selected interface.

{ s11 | s12 | s1u | s4 | s4u | s5 | s5u }

Specifies the interface to which the action will be applied.

s11: Applies the path failure action to the S11 interface between the S-GW and the MME.

s11u: Applies the path failure action to the S11-U interface between the S-GW and the MME.

s12: Applies the path failure action to the S12 interface between the S-GW and the RNC.

s1u: Applies the path failure action to the S1-U interface between the S-GW and the eNodeB.

s4: Applies the path failure action to the S4 control plane interface between the S-GW and the SGSN.

s4u: Applies the path failure action to the S4-U user plane interface between the S-GW and the SGSN.

s5: Applies the path failure action to the S5 interface between the S-GW and the P-GW.

s5u: Applies the path failure action to the S5-U user plane interface between the S-GW and the P-GW.

{ local-purge | signal-peer }

Specifies the action to apply to the selected interface.

local-purge: The S-GW clears the affected bearer (or PDN if path failure is received on a default bearer) locally without informing the peer. This is the default action for all interface.

signal-peer: The S-GW initiates control signalling towards the peer MME and P-GW. When signalling:

- For a bearer deletion, the S-GW sends a Delete-Bearer-Command message to the P-GW and a Delete-Bearer-Request (with EBI) message to the MME.
- For PDN deletion, the S-GW sends a Delete-Session-Request message to the P-GW and a Delete-Bearer-Request (with LBI) message to the MME.
- The S-GW will not wait for Delete replies from the peer. The request will be sent only once and local resources will be reset.

Usage Guidelines

Use this command to specify the type of action to take when a path failure occurs on one of the supported interfaces.

Example

The following command sets the path failure action for the S5 interface to "signal peer":

```
path-failure s5 signal-peer
```

pgw-fteid-in-relocation-cs-rsp

Controls the sending of the PGW Fully Qualified Tunnel Endpoint Identifier (FTEID) for relocation Create Session Response procedures with an S-GW change.

Product

S-GW

Privilege

Administrator, Security Administrator

Command Modes

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] pgw-fteid-in-relocation-cs-rsp

no

Disables the sending of the P-GW FTEID in Create Session Response procedures where there is an S-GW relocation change. This is the default setting.

pgw-fteid-in-relocation-cs-rsp

Enables the sending of the P-GW FTEID in Create Session Response procedures where there is an S-GW relocation change.

Usage Guidelines

Use this command to control the sending of the PGW Fully Qualified Tunnel Endpoint Identifier (FTEID) for relocation Create Session Response procedures with an S-GW change. For backward compatibility with earlier 3GPP release peer nodes requiring the P-GW FTEID in the Create Session Response procedures, this configurable can be enabled.

Example

To enable the sending of the FTEID for relocation Create Session REsponse procedures with an S-GW change:

pgw-fteid-in-relocation-cs-rsp

plmn

Configures the public land mobile network (PLMN) identifiers for this S-GW. service

Product

S-GW

SAEGW

Privilege

Administrator

Command Modes

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

`plmn id mcc` *`number`* **`mnc`** *`number`* **`[ primary ]`**
`no plmn id mcc` *`number`* **`mnc`** *`number`*

no

Removes the configured PLMN ID for this S-GW service.

mcc *number*

Configures the Mobile Country Code for this PLMN ID.

number must be an integer from 100 through 999.

mnc *number*

Configures the Mobile Network Code for this PLMN ID.

number must be a 2- or 3-digit integer from 00 through 999,

primary

Specifies that this is the primary PLMN ID for this S-GW service.

Usage Guidelines

The PLMN identifier is used by the S-GW service to determine whether or not a mobile station is visiting, roaming, or home. Multiple S-GW services can be configured with the same PLMN identifier. Up to five PLMN IDs can be configured for each S-GW Service. In Release 15.0 and later, up to 15 PLMN IDs can be configured.

Example

The following command configures a "primary" PLMN ID for this S-GW service with an MCC of *123* and an MNC of *12*:

`plmn id mcc 123 mnc 12 primary`

reporting-action

Configures the system to start reporting session events.

Product

S-GW

SAEGW

Privilege

Administrator

Command Modes

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ no ] reporting-action event-record [ trigger active-idle ]`
`default reporting-action event-record`

default

Returns the command to its default setting of disabled.

no

Disables session event reporting.

trigger active-idle

Specifies that the event is only to be reported upon the going from active to idle.

Usage Guidelines

Use this command to enable the session event reporting feature on the S-GW.

Example

The following command enables event reporting but does not limit it to events triggered by going active to idle:

`reporting-action event-record`

timeout idle

This command removes S-GW sessions that remain idle for longer than the configured time limit.

Product

S-GW

SAE-GW

Privilege

Administrator

Command Modes

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

`timeout idle` *dur_seconds* **`[ micro-checkpoint-periodicity`***time_in_seconds* **`| micro-checkpoint-deemed-idle`***time_in_seconds* **`]`**
`{ default | no } timeout idle`

default

Indicates the timeout specified is to be returned to its default behavior.

no

Disables the timeout idle functionality.

timeout idle

Enables the S-GW session idle timer.

dur_seconds

Specifies the time limit, in seconds, after which the S-GW session will be torn down. Valid entries are from 0 to 4294967295.

micro-checkpoint-periodicity*time_in_seconds*

Specifies the micro-checkpoint periodicity for idlesecs, in seconds.

time_in_seconds must be an integer from 10 to 10000 seconds.

Default: 10

Important

The **micro-checkpoint-periodicity** value should be less than **idle timeout** value.

micro-checkpoint-deemed-idle*time_in_seconds*

Specifies the time duration, in seconds, after which a session state is deemed to have changed from active to idle or idle to active, and a micro-checkpoint is then sent from the active to the standby chassis.

time_in_seconds must be an integer from 10 to 1000.

Default: 180

Important The **micro-checkpoint-deemed-idle** value should be less than the **timeout idle** value.

Usage Guidelines

The S-GW session idle timer removes stale sessions in those cases where the session is removed on the other nodes but due to some issue remains on the S-GW. Once configured, the session idle timer will tear down such sessions that remain idle for longer than the configured time limit. The implementation of the session idle timer allows the S-GW to more effectively utilize system capacity.

Optionally, ICSR micro-checkpoint periodicity for idlesecs is configurable instead of using the default periodicity of 10 seconds. Operators can configure this setting to a large value to suit their need to reduce the number of micro-checkpoints on the SRP link. When this CLI command is configured, idleseconds micro-checkpoints are sent at configured regular intervals to the standby chassis. If not configured, micro-checkpoints are sent at intervals of 10 seconds, which is the default.

Finally, the operator can choose to configure micro-checkpoint-deemed-idle. This process enables the active and standby chassis to be synchronized with respect to when a particular session became active or idle. Since this feature is event-based, it enables the chassis to send micro-checkpoints only when an event is deemed to have occurred, as opposed to sending micro-checkpoints based on a configured time duration, which sends the micro-checkpoints regardless of whether a session state change occurred or not. Using **micro-checkpoint-deemed-idle** results in a more efficient event-based sending of micro-checkpoints to the standby chassis and also increases SRP bandwidth.

Important Either the **micro-checkpoint-deemed-idle** or **micro-checkpoint-periodicity** value can be configured for idle time duration. Any change from **micro-checkpoint-deemed-idle** to **micro-checkpoint-periodicity**, or vice versa, requires removing the first configuration before adding the new configuration.

Example

The following example configures the S-GW session idle timer 3600 seconds (one minute).

```
timeout idle 3600
```