

SGTP Service Configuration Mode Commands

Command Modes

The SGSN GPRS Tunneling Protocol (SGTP) Service configuration mode provides the configuration of GTP-C and GTP-U related parameters.

Exec > Global Configuration > Context Configuration > SGTP Service Configuration

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

Entering the above command sequence results in the following prompt:

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

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

- direct-tunnel-disabled-ggsn, on page 1
- disable-remote-restart-counter-verification, on page 3
- do show, on page 4
- end, on page 4
- exit, on page 5
- ggsn-fail-retry-timer, on page 5
- gn-delay-monitoring , on page 6
- gtpc, on page 7
- gtpu, on page 12
- ignore-remote-restart-counter-change, on page 14
- max-remote-restart-counter-change, on page 14
- mbms, on page 15
- path-failure, on page 16
- pool, on page 16

direct-tunnel-disabled-ggsn

This command makes it possible for the operator to disable direct tunneling on the basis of a GGSN.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > SGTP Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

direct-tunnel-disabled-ggsn *ipv4/ipv6_address*
no direct-tunnel-disabled-ggsn [*ipv4/ipv6_address* **]**

no

Deletes the direct-tunnel-disabled-ggsn configuration which results in re-enabling direct tunneling to the GGSN.

- Including an IPv4 or IPv6 address for a specific GGSN, re-enables direct tunneling for that specific GGSN.
- Excluding any IPv4 or IPv6 address from this command removes all direct-tunnel-disabled-ggsn definitions from the SGTP service configuration.

Usage Guidelines

By default, GGSNs and RNCs are assumed to be capable of direct tunneling.

This command disables direct tunneling for a specified GGSN. The command can be repeated to disable direct tunneling for multiple GGSNs, thereby creating a 'disabled GGSN' list. Checking for a direct-tunnel-disabled GGSN is actually the last step in the PDP Activation procedure.

Restricting direct tunneling by a GGSN for an entire APN would be configured with the appropriate command in the APN profile configuration mode.

Restricting direct tunneling at the RNC level would be configured with the appropriate command in the IuPS service configuration mode.

This command can only be used if:

- The Direct Tunnel license has been purchased and applied.
- The Direct Tunnel feature is appropriately enabled via configurations of the IMEI profile and/or the Call-Control and APN profiles.
- The RNC does not restrict direct tunnel.
- The subscriber is not requesting CAMEL services.

Example

Use the following command to disable direct tunnel for the GGSN with the IP address of *141.21.4.20*:

```
direct-tunnel-disabled-ggsn 141.21.4.20
```

disable-remote-restart-counter-verification

This command disables the SGSN's default behavior for verification of the remote peer's (GGSN) restart counter change values.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > SGTP Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ default | no ] disable-remote-restart-counter-verification`

default

Enables the default behavior for verification of the GGSN's restart counter change values.

no

Disables the command configuration and enables the default behavior of verification.

Usage Guidelines

This command disables the default behavior used to minimize PDP deactivations resulting from path failure detection due to erroneous restart counter change messages.

With the execution of this command, the SGSN stops verifying restart counters received in Create PDP Context Response or Update PDP Context Response or Update PDP Context Request (CPCR, CPCR, and UPCQ) messages. When the SGSN detects GTP-C path failure between the SGSN and the GGSN, the SGSN assumes PDP sessions at the GGSN are lost and the SGSN deactivates those PDP sessions towards the UE with an indication that the UE should activate the PDP session again. Potentially, this scenario could cause unnecessary traffic increases within the operator's network.

The SGSN default behavior provides the ability to manage GTP-C path failures detected as a result of spurious restart counter change value messages received from the GGSN. With the default behavior, path failure detection is based on receipt of restart counter change values in CPCR, CPCR, and UPCQ messages. The session manager informs the SGTPC manager about a changed restart counter value. The SGTPC manager verifies the PDP context status by performing an echo request and echo response with the GGSN. Only then is the path failure confirmed if the echo response contains a new restart counter value. Then the SGTPC manager informs all session managers about the path failure and the session managers begin deactivation of the PDP contexts.

Related commands:

- **max-remote-restart-counter-change**, also part of the SGTP service configuration mode, allows the operator to set a maximum variance between stored and received values for restart counter changes coming from the GGSN.
- **pdp-deactivation-rate**, in the SGSN Global configuration mode, allows the operator to modify the rate the SGSN deactivates PDP connections when GPT-C path failure is detected.

- **ignore-remote-restart-counter**, also part of the SGTP service configuration mode.

Example

Disable the default behavior and stop verification with echo request/response process:

```
disable-remote-restart-counter-verification
```

Use either of the following commands to enable the default verification behavior:

```
no disable-remote-restart-counter-verification
default disable-remote-restart-counter-verification
```

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.
```

end

Exits the configuration mode and returns to the Exec mode.

Product All

Privilege Security Administrator, Administrator

Syntax Description

```
end
```

Usage Guidelines Changes the mode to the Exec mode.

exit

Exits the SGTP Service configuration mode and returns to the Context configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax Description

exit

Usage Guidelines

Return to the previous mode.

ggsn-fail-retry-timer

This command sets the amount of time that a GGSN will be unavailable.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > SGTP Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

ggsn-fail-retry-timer *value*
no ggsn-fail-retry-timer

no

Removes the timer setting and disables the Local DNS feature.

value

Defines the amount of time, in seconds, that the GGSN is to be considered unavailable.

Enter an integer from 60 to 600. Default is 300.

Usage Guidelines

Setting this timer to a valid value enables the Local DNS feature - described in the ***SGSN Administration Guide***. Setting this timer marks a GGSN in the primary GGSN pool as unavailable for PDP context creation and causes the SGSN to forward a PDP Context Activation Request to a remote pool GGSN, identified via a local (on the SGSN) DNS check. Marking a GGSN unavailable can be done if there is a reason to believe the GGSN is unavailable; for example, lack of response to GTP messages. Marking a GGSN as unavailable is usually done for a limited period to allow the GGSN time to recover.

Example

Enable the Local DNS feature and mark the GGSNs in the primary pool as unavailable for 4 minutes (*240 seconds*):

```
ggsn-fail-retry-timer 240
```

gn-delay-monitoring

This command configures monitoring of Gn/Gp interface to check for the delay of packets between the SGSN and the GGSN.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > SGTP Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

gn-delay-monitoring [num-delay *number_delayed* **| num-no-delay-for-clear** *number_normal* **| tolerance-seconds** *number_seconds* **]**
default gn-delay-monitoring [num-delay | num-no-delay-for-clear | tolerance-seconds]
no gn-delay-monitoring

default

Resets the specified parameter to the default value.

no

Disables Gn/Gp monitoring for delayed GTP-C packets.

num-delay *number_delayed*

Defines the number of response messages, coming from the GGSN, that can be delayed (delay time defined by tolerance-seconds parameter) before the delay is flagged to generate an SNMP trap.

number_delayed: Enter an integer from 1 to 500, default is 30.

num-no-delay-for-clear *number_normal*

Defines the number of consecutive response messages, coming from the GGSN, that must be received without delay (in normal response time) to clear the flag towards the GGSN.

number_normal: Enter an integer from 1 to 500, default is 15.

tolerance-seconds *number_seconds*

Defines the 'normal' number of seconds the SGSN should wait for a response from the GGSN. After this time, the response would be considered 'delayed'.

number_seconds: Enter an integer from 1 to 20, default is 4 seconds.



Important The value for this parameter should be less than the value set for the **retransmission-timeout** parameter of the **gtpc** command, also in this configuration mode.

Usage Guidelines

With this command, the SGSN can monitor the control plane packet delay for GTP-C signaling messages on the SGSN's Gn/Gp interface towards the GGSN. If the delay crosses this configurable threshold, an alarm will be generated to prompt the operator.

A delay trap is generated when the GGSN response to an ECHO message request is delayed more than a configured amount of time and for a configured number of consecutive responses. When this occurs, the GGSN will be flagged as experiencing delay.

A clear delay trap is generated when successive ECHO Response (number of successive responses to detect a delay clearance is configurable), are received from a GGSN previously flagged as experiencing delay.

This functionality can assist with network maintenance, troubleshooting, and early fault discovery.

Example

Enable Gn/Gp monitoring for GTP-C packets that arrive from the GGSN with a delay greater than *5* seconds:

```
gn-delay-monitoring tolerance-seconds 5
```

gtpc

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

Product

eWAG

MME

PDG/TTG

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > SGTP Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

gtpc { bind address *ipv4_address* **| dns-sgsn context** *context_name* **| echo-interval** *interval_seconds* **| echo-retransmission { exponential-backoff [[min-timeout** *timeout_seconds* **] [smooth-factor** *smooth_factor* **] +] | timeout** *timeout_seconds* **} | guard-interval** *interval_seconds* **| ignore response-port-validation | ip qos-dscp** *dscp_marking* **| max-retransmissions** *max_retransmissions* **| retransmission-timeout** *timeout_seconds* **| send { common flags | rab-context | target-identification-preamble } | sync-echo-with-peer }**
no gtpc { bind address | dns-sgsn context | echo-interval | send { common-flags | rab-context | target-identification-preamble } | sync-echo-with-peer }
default gtpc { echo-interval | echo-retransmission | guard-interval | ignore response-port-validation | ip qos-dscp | max-retransmissions | retransmission-timeout | send { common-flags | rab-context | target-identification-preamble } | sync-echo-with-peer }

no

Disables the configured GTP-C setting.

default

Resets the specified parameter to its default value.

bind address *ipv4_address*

Binds SGTP service to the IP address of the interface.

The bind address for the **gtpc** and **gtpu** commands should be the same.

ipv4_address must be a standard IPv4 address.

dns-sgsn context *context_name*

Identify the context where the DNS client is configured to send the DNS query to get the peer SGSN address. If nothing is configured, the system assumes the DNS client is configured in the same context where the SGTP service is configured.

context_name: Enter a string of 1 to 79 alphanumeric characters to identify the context.

There is a dns-sgsn command option in the call-control profile, which, if configured, would override the configuration in this SGTP service configuration.

echo-interval *interval_seconds*

Configures the duration between echoes.

seconds Enter an integer from 0 through 3600.

Default: 60

echo-retransmission { exponential-backoff [[min-timeout *timeout_seconds*] [smooth-factor *smooth_factor*] +] | timeout *timeout_seconds* }

Configures the retransmission parameters for GTP-C echo messages. The operator can choose to use either an "exponential-backoff" timers or a "fixed-retransmission" timer:

- The **exponential-backoff** timer uses an exponential backoff algorithm to better manage the GTP-C path during periods of network congestion and to perform exponential-backoff echo timing. The exponential-backoff timer uses a calculated round-trip time (RTT), as well as a configurable factor or a multiplier to be applied to the RTT statistic. Different paths can each have a different RTT, so the exponential-backoff timer can be configured for multiple paths. One or both of the following parameters can be configured to refine the exponential-backoff timer configuration:
  - **min-timeout** *timeout_seconds*: Specifies the minimum time period (in seconds) for the exponential-backoff echo timer. If the RTT multiplied by the smooth factor is less than this minimum timeout value, then the node uses the value set with this keyword. Range is 1-20. Default is 5.
  - **smooth-factor** *smooth_factor*: Specifies the multiplier that the exponential-backoff echo timer uses when calculating the time to wait to send retries, when the gateway has not received a response from the peer within value defined for the path echo interval. Range is 1-5. Default is 2.
- **timeout** *timeout_seconds*: Configures the number of seconds for the fixed retransmission timeout value for GTP-C echo messages. Range from 1 to 20. Default is 5.

guard-interval *interval_seconds*

Configures the interval (in seconds) for which the SGTP maintains responses sent to gateway. This optimizes the handling of retransmitted messages. This value should be configured to be greater than the gateway's configuration for max-retries multiple by retry-interval.

interval_seconds: Enter an integer from 10 to 3600.

Default: 100

ignore response-port-validation

This keyword is available in releases 8.1 and higher.

This keyword instructs the gateway to ignore the response port validation.

For the gateway to process incoming GTP responses to an *incorrect* port, this keyword must be entered, and the same **bind address** must be configured for GTPC and GTPU in the SGTP service.

Default: Disabled. To reset the default for this parameter, you must enter the following command: **no gtpc ignore response-port-validation**.

ip qos-dscp *dscp_marking*

Configures the diffserv code point marking to be used per hop behavior (PHB) when sending GTP-C messages originating from the session manager and SGTPC manager.

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, i.e., 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.

dscp_marking: Enter one of the following values:

- **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).
- **af42**: Marks traffic as Assured Forwarding 42 PHB (multimedia conferencing)
- **af43**: Marks traffic as Assured Forwarding 43 PHB (multimedia conferencing)
- **be** : Designates use of Best Effort forwarding PHB. This is the default value.
- **cs0** : Designates use of class selector mode 0 PHB.
- **cs1** : Designates use of class selector mode 1 PHB.
- **cs2** : Designates use of class selector mode 2 PHB.
- **cs3** : Designates use of class selector mode 3 PHB.
- **cs4** : Designates use of class selector mode 4 PHB.
- **cs5** : Designates use of class selector mode 5 PHB.
- **cs6** : Designates use of class selector mode 6 PHB.
- **cs7** : Designates use of class selector mode 7 PHB.
- **ef** : Designates use of Expedited Forwarding PHB

Default: **be** (best effort)

max-retransmissions *max_retransmissions*

Configures the maximum number of retries for packets.

max_retransmissions: Enter an integer from 0 to 15.

Default: 4

retransmission-timeout *timeout_seconds*

Configures the control packet retransmission timeout in GTP, in seconds.

timeout_seconds: Enter an integer value from 1 through 20.

Default: 5

send { common-flags | rab-context | target-identification-preamble }

- **common-flags** : This option configures the SGTP service to include or exclude the common flags IE during an Inter-SGSN RAU. When selected, the default is to send the common flags IE.



Important Sending of common flags must be enabled to configure dual PDP type (IPv4v6) addressing with the **dual-address-pdp** command in the SGSN global configuration mode.

- **rab-context** : This option configures the SGTP service to include/exclude the radio access bearer (RAB) context IE in SGSN 'context response' message during Inter-SGSN Routing Area Update procedure. Default is to send the RAB context IE.
- **target-identification-preamble** : This option configures the SGTP service to include the Target Identification IE preamble byte in the target-id of Relocation Requests that it sends. By default, the preamble is not included. In accordance with 3GPP TS 29.060, v9.2.0, if the preamble is included then multiple optional parameters, such as Extended RNC ID, are encoded. Extended RNC ID expands the ID range from 4095 to 65535.

  In situations of MME interaction with the SGSN during SRNS procedures via GTPv1, the SGSN can use this Extended RNC ID field to indicate the Target RNC ID associated with the MME and vice versa.

Default: sending RAB context IE.

sync-echo-with-peer

This keyword is applicable to the SGSN only.

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

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

Default: Enabled

Usage Guidelines

Use this command to configure GTP-C settings for the current SGTP service. Repeat the command as needed to configure all required GTP-C parameters.

Example

Following command excludes the radio access bearer (RAB) context IE in the SGSN Context Response message during the inter-SGSN RAU procedure:

```
no gtpc send rab-context
```

Configure the SGSN to send *common flags* with all GTP-C messages:

```
gtpc send common-flags
```

Set the SGSN to use GTPC echo-retransmission with exponential-backoff and both filters set for default:

```
gtpc echo-retransmission exponential-backoff
```

gtpu

This command configures the GPRS Tunneling Protocol user data plane parameters (GTP-U) for this SGTP service.

Product

eWAG

PDG/TTG

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > SGTP Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
gtpu { bind address ipv4_address | echo-interval interval_seconds |
echo-retransmission { exponential-backoff [ [ min-timeout timeout_seconds ]
 [ smooth-factor smooth_factor ] + ] | timeout timeout_seconds } |
max-retransmissions max_retransmissions | retransmission-timeout timeout_seconds
 | sync-echo-with-peer
no gtpu { bind address ipv4_address | echo-interval | sync-echo-with-peer}
default gtpu { echo-interval | echo-retransmission | max-retransmissions
 | retransmission-timeout | sync-echo-with-peer }
```

no

Removes the configuration for the specified parameter from the current SGTP service configuration.

default

Resets the specified GTP-U parameter to its factory default.

bind address *ipv4_address*

Defines the GTP-U Gn' interface IP address that binds to this SGTP service.

The **gtpu** and the **gtpc** commands should be configured with the same bind address.

ipv4_address: Enter a standard dotted-quad IPv4 address.

echo-interval *interval_seconds*

Configures the echo interval.

interval_seconds: Enter an integer from 60 through 3600.

Default: 60

echo-retransmission { exponential-backoff [[min-timeout *timeout_seconds*] [smooth-factor *smooth_factor*] +] | timeout *timeout_seconds*

Configures the retransmission parameters for GTP-U echo messages. The operator can choose to use either an "exponential-backoff" timers or a "fixed-retransmission" timer:

- The **exponential-backoff** timer uses an exponential backoff algorithm to better manage the GTP-U path during periods of network congestion and to perform exponential-backoff echo timing. The exponential-backoff timer uses a calculated round-trip time (RTT), as well as a configurable factor or a multiplier to be applied to the RTT statistic. Different paths can each have a different RTT, so the exponential-backoff timer can be configured for multiple paths. One or both of the following parameters can be configured to refine the exponential-backoff timer configuration:
  - **min-timeout** *timeout_seconds*: Specifies the minimum time period (in seconds) for the exponential-backoff echo timer. If the RTT multiplied by the smooth factor is less than this minimum timeout value, then the node uses the value set with this keyword. Range is 1-20. Default is 5.
  - **smooth-factor** *smooth_factor*: Specifies the multiplier that the exponential-backoff echo timer uses when calculating the time to wait to send retries, when the gateway has not received a response from the peer within value defined for the path echo interval. Range is 1-5. Default is 2.
- **timeout** *timeout_seconds*Configures the number of seconds for the fixed retransmission timeout value for GTP-U echo messages. Range from 1 to 20. Default is 5.

max-retransmissions *max_retransmissions*

Configures the maximum number of retries for retransmitting packets.

max_retransmissions: Must be an integer from 0 through 15.

Default: 4

retransmission-timeout *timeout_seconds*

Configures the retransmission timeout of packets, in seconds.

timeout_seconds: Must be an integer from 1 through 20.

Default: 5

sync-echo-with-peer

This keyword is applicable to the SGSN only.

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

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

Default: Enabled

Usage Guidelines

Use this command to configure the GTP-U settings for the SGTP service.

Example

Set the GTPU echo-interval for 5 seconds:

```
gtpu echo-interval 5
```

Set the gateway to use GTP-U echo-retransmission with exponential-backoff and the smooth-factor set for *4*:

```
gtpc echo-retransmission exponential-backoff smooth-factor 4
```

ignore-remote-restart-counter-change

With the inclusion of the **disable-remote-restart-counter-verification** command, this command has been deprecated.

max-remote-restart-counter-change

Use this command to set a restart counter change window to avoid service deactivations and activations that could cause large bursts of network traffic if the restart counter change messages from the GGSN are erroneous.

Product

eWAG

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > SGTP Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

max-remote-restart-counter-change *variance*
default max-remote-restart-counter-change

default

If this keyword is used or if a variance window is not configured, then the default value will be 255 and the default behavior will be to detect a restart on any change.

variance

Set a number (an 8-bit value) that will define the variance range for restart counter change values compared between the gateway's stored value and the value received in messages from the GGSN. Valid entry is an integer from 1 to 255; default is 255.

Value of 32 is recommended as it provides a sufficient window to allow the gateway to handle delayed messages with old restart counters.

Usage Guidelines

When the gateway detects GTP-C path failure between the gateway and the GGSN, the gateway assumes PDP sessions at the GGSN are lost and the gateway deactivates corresponding PDP sessions towards the UE with an indication that the UE should activate the PDP session again. Detection is based on receipt of restart counter change values in Create PDP Context Response or Update PDP Context Response or Update PDP Context Request (CPCR/UPCR/UPCQ) messages. Potentially, this scenario can cause major traffic increases within the operator's network. It is possible that the messages received from the GGSN are spurious.

The gateway default behavior provides the ability to verify possible GTP-C path failures detected as a result of spurious restart counter change messages received from the GGSN. With the default behavior, the session manager informs the SGTPC manager about a changed restart counter value. The SGTPC manager responds by verifying the PDP context status by performing an Echo Request / Echo Response with the GGSN. If the Echo Response includes a new restart counter change value, then the session manager considers the path failure confirmed and begins the PDP context deactivation sequence.

Use this command to avoid unnecessary path failures and deactivations by setting a restart counter change value 'window' or range of values. With this window, the gateway only accepts linearly increasing values for restart counter change values that are within the specified range of accepted changes before the SGTPC manager verifies. For example, if the allowed window for restart counter change value is set to 32 and the last learnt restart counter change value from the GGSN is 15, then the gateway should detect a restart only if the new restart counter value is between 16 and 47 (range of 32) and then the gateway would verify with the Echo Request/Response. If the received restart counter change value was 200 and the current learnt value was 15 with a window of 32, then the 200 would be ignored as a spurious value.

Also, use this command to set a restart counter change values window to avoid possible 'race conditions' (as defined in 3GPP TS 23.007 v8.7.0) where a new message arrives prior to an older message. This 'race condition' occurs when the gateway's stored restart counter value for the GGSN is larger than the restart counter value received in the messages received from the GGSN.

Related commands:

- **disable-remote-restart-counter-verification** - also part of the SGTP service configuration mode, this command allows the operator to disable the default behavior.
- **pdp-deactivation-rate**, in the SGSN Global configuration mode, this allows the operator to modify the rate the gateway deactivates PDP connections when GPT-C path failure is detected.
- **ignore-remote-restart-counter**, also part of the SGTP service configuration mode.

Example

Use the following command to configure an allowed restart counter change value window of *32*:

```
max-remote-restart-counter-change 32
```

mbms

Enables / disables the Multimedia Broadcast Multicast Service.



Important The **mbms** command and parameter-configuring keywords are under development for future release and should not be used or included in your configuration at this time.

path-failure

This command specifies the method for determining if path failure has occurred.

Product

eWAG

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > SGTP Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

`path-failure detection-policy gtp { echo | non-echo } + { default | no } path-failure detection-policy`

default

Resets the specified path failure parameter to default.

Default: echo (for both GTPC and GTPU)

no

Deletes the path-failure definition from the configuration.

echo

Path failure is detected when the retries of echo messages time out.

non-echo

Path failure is detected when the retries of non-echo messages time out.

Usage Guidelines

Use this command to define the policy to detect gtp path failure.

Example

Set *echo* as the polity detection type:

`path-failure detection-policy gtp echo`

pool

This command enables the default SGSN functionality for (flex) pooling and enables inclusion of the configured pool hop-counter count in new SGSN context/identify request messages.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > SGTP Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

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

no

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

default

Removes the SGSN pool hop-counter IE from the GTP Identity/context requests.

default-sgsn

Enables 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 Identify Requests.

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.

count: Enter an integer from 1 to 255.

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/identify 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

Enable the default pooling functionality which allows an outside SGSN to reach a pooled SGSN:

```
pool default-sgsn
```

Set the hop-count to be included in messages to *25*:

```
pool hop-count
```