Context Configuration Mode Commands E-H

Command Modes

This section includes the commands **edr-module active-charging-service** through **hss-peer-service**.

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Important

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

eap-profile

Creates a new, or specifies an existing, Extensible Authentication Protocol (EAP) profile and enters the EAP Configuration Mode.

Product

ASN-GW

ePDG

PDIF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] eap-profile *name*

no

Removes the specified EAP profile.

name

Specifies the name of a new or existing EAP profile as an alphanumeric string of 1 through 256 characters.

Usage Guidelines

Use this command to create a new or enter an existing EAP profile.

Entering this command results in the following prompt:

```
[context_name]hostname(config-ctx-eap-profile)#
```

EAP Configuration Mode commands are defined in the *EAP Configuration Mode Commands* chapter.

Example

The following command configures an EAP profile called *eap1* and enters the EAP Configuration Mode:

```
eap-profile eap1
```

edr-module active-charging-service

Enables the creation, configuration, or deletion of the Event Data Record (EDR) module for this context. In releases prior to 15.0, the SGSN re-used the existing 'EDR" module for generating event logs which is primarily used for charging records. But from release 15.0 onwards, the session-event module is used by SGSN for event logging. For more information see the **session-event-module** command.

Product

ACS

GGSN

HA

LNS

PDSN

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ no ] edr-module active-charging-service [ charging | reporting ]`

no

Removes the EDR module configuration for the current context.

charging

Enables the EDR module for charging EDRs that are stored in the /records/edr directory.

reporting

Enables the EDR module for reporting EDRs that are stored in the /records/redr directory.

Usage Guidelines

Use this command to create the EDR module for the context, and configure the EDR module for active charging service records. You must be in a non-local context when specifying this command, and you must use the same context when specifying the UDR module command.

If this CLI command is configured without the **charging** or **reporting** keywords, by default the EDR module is enabled for charging EDRs.

On entering the command with the **charging**keyword or without any keywords, the CLI prompt changes to:

[*context_name*]*hostname*(config-edr)#

On entering the command with the **reporting**keyword, the CLI prompt changes to:

[*context_name*]*hostname*(config-redr)#

Example

The following command creates the EDR module for the context for charging EDRs, and enters the EDR Module Configuration Mode:

`edr-module active-charging-service`

egtp-service

Creates an eGTP service or specifies an existing eGTP service and enters the eGTP Service Configuration Mode for the current context.

Product

MME

P-GW

SAEGW

SGSN

S-GW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ no ] egtp-service` *`service_name`* **`[ -noconfirm ]`**

egtp-service *service_name*

Specifies the name of the eGTP service as an alphanumeric string of 1 through 63 characters. If *service_name* does not refer to an existing service, the new service is created if resources allow.

Important

Service names must be unique across all contexts within a chassis.

-noconfirm

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

no egtp-service *service_name*

Removes the specified eGTP service from the context.

Usage Guidelines

Enter the eGTP Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.

A maximum of 256 services (regardless of type) can be configured per system.

Caution

Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following prompt:

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

eGTP Service Configuration Mode commands are defined in the *eGTP Service Configuration Mode Commands* chapter.

Use this command when configuring the following GTP SAE components: MME, P-GW, and S-GW. Also use this command when configuring an S4-SGSN. Once the eGTP service has been created on the S4-SGSN, the eGTP service must be configured using the **gtpc**, **validation-mode** and **interface-type** commands in *eGTP*

Service Configuration Mode. Once the service is created and configured, it then must be associated with the 2G and/or 3G services configured on the S4-SGSN using the**associate** command in *Call Control Profile Configuration Mode*.

Important If you modify the **interface-type** 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 enters the existing eGTP Service Configuration Mode (or creates it if it does not already exist) for the service named *egtp-service1*:

```
egtp-service egtp-service1
```

The following command will remove *egtp-service1* from the system:

```
no egtp-service egtp-service1
```

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.

epdg-service

Creates Evolved Packet Data GateWay service and enters EPDG service configuration mode.

Product

ACS

ePDG

GGSN

HA

LNS

PDSN

SGSN

Privilege Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] epdg-service *name* **[-noconfirm]**

no

Indicates the evolved packet data gateway service specified is to be removed.

name

Specifies the name of the ePDG service to configure as an alphanumeric string of 1 through 63 characters. If *name* does not refer to an existing service, the new service is created if resources allow.

Important Service names must be unique across all contexts within a chassis.

-noconfirm

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

Usage Guidelines

Enter the ePDG Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.

Example

The following command will enter the ePDG Service Configuration Mode creating the service *sampleService*, if necessary.

```
epdg-service sampleService
```

The following command will remove *sampleService* as being a defined ePDG service.

```
no epdg-service sampleService
```

event-report-conn

Configures a GMPC Event Report Connection.

Product

MME

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ no ] event-report-conn` *event_report_conn_name* **`[ -noconfirm ]`**

no

Indicates the event report connection name that is specified is to be removed.

name

Specifies the name of the event-report-conn to configure as an alphanumeric string of 1 to 32 characters. If *event-report-conn name* does not refer to an existing configuration, then new configuration is created if resources allow.

Important Service names must be unique across all contexts within a chassis.

Usage Guidelines

Enter the event-report-conn name for a newly defined configured connection. This command is also used to remove an existing connection.

Example

The following command will create the event-report-conn name Configuration Mode .

`event-report-conn name Config`

The following command will remove *event-report-conn name Config* as being a defined event-report-conn service.

`no event-report-conn name Config`

event-notif-endpoint

Enables creation, configuration or deletion of an Event Notification collection server endpoint.

Product

IPCF

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ no ] event-notif-endpoint` *en_node_name*

no

Removes the specified Event Notification collection server endpoint.

en_node_name

Specifies name of the Event Notification collection server endpoint as an alphanumeric string of 1 through 31 characters.

If the named endpoint does not exist, it is created, and the CLI mode changes to the Event Notification Interface Endpoint Configuration Mode wherein the endpoint can be configured.

If the named endpoint already exists, the CLI mode changes to the Event Notification Interface Endpoint Configuration Mode wherein the endpoint can be reconfigured.

Usage Guidelines

Use this command to create/configure/delete an Event Notification collection server endpoint.

Only 1 Event Notification interface across a chassis can be configured on a system.

Entering this command results in the following prompt:

```
[context_name]hostname(config-ntfyintf-endpoint)#
```

The commands configured in this mode are defined in the *Event Notification Interface Endpoint Configuration Mode Commands* chapter of *Command Line Interface Reference*.

Caution This is a critical configuration. The PCC Event notification can not be collected on a server without this configuration. Any change to this configuration would lead to the loss of event notifications from PCC service on IPCF node.

Example

The following command creates an Event Notification Interface Endpoint named *event_intfc_3*:

```
event-notif-endpoint event_intfc_3
```

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.

external-inline-server

This is a restricted command.

fa-service

Creates or deletes a foreign agent (FA) service or specifies an existing FA service for which to enter the FA Service Configuration Mode for the current context.

Product

ASN-GW

PDSN

FA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ no ] fa-service` *`name`* **`[ -noconfirm ]`**

no

Indicates the foreign agent service specified is to be removed.

name

Specifies the name of the FA service to configure as an alphanumeric string of 1 through 63 characters. If *name* does not refer to an existing service, the new service is created if resources allow.

Important Service names must be unique across all contexts within a chassis.

-noconfirm

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

Usage Guidelines

Enter the FA Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.

A maximum of 256 services (regardless of type) can be configured per system.

Caution Large numbers of services greatly increase the complexity of management and may impact overall system performance (i.e. resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Example

The following command will enter the FA Service Configuration Mode creating the service *sampleService*, if necessary.

```
fa-service sampleService
```

The following command will remove *sampleService* as being a defined FA service.

```
no fa-service sampleService
```

firewall max-associations

This command is obsolete.

fng-service

Creates a new, or specifies an existing FNG service and enters the FNG Service Configuration Mode. A maximum of 16 FNG services can be created. This limit applies per ASR 5000 chassis and per context.

Product FNG

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > **context** *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
fng-service name [ -noconfirm ]
no fng-service name
```

fng-service *name*

Specifies the name of a new or existing FNG service as an alphanumeric string of 1 through 63 characters that must be unique across all FNG services within the same context and across all contexts.

Important Service names must be unique across all contexts within a chassis.

no fng-service *name*

Deletes the specified FNG service.

Usage Guidelines

Use this command in Context Configuration Mode to create a new FNG service or modify an existing one. Executing this command enters the FNG Service Configuration Mode.

Example

The following command configures an FNG service named *fng1* and enters the FNG Service Configuration Mode:

```
fng-service fmg1
```

ggsn-service

Creates or deletes a Gateway GPRS Support Node (GGSN) service and enters the GGSN Service Configuration Mode within the current context to configure it.

Product

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

ggsn-service *svc_name* **[-noconfirm]**
no ggsn-service *svc_name*

no

Deletes a preciously configured GGSN service.

svc_name

Specifies the name of the GGSN service to create/configure as an alphanumeric string of 1 through 63 characters that is case sensitive.

Important Service names must be unique across all contexts within a chassis.

-noconfirm

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

Usage Guidelines

Services are configured within a context and enable certain functionality. This command creates and allows the configuration of services enabling the system to function as a GGSN in a GPRS or UMTS network. This command is also used to remove previously configured GGSN services.

A maximum of 256 services (regardless of type) can be configured per system.

Caution Large numbers of services greatly increase the complexity of management and may impact overall system performance (i.e. resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Example

The following command creates a GGSN service named *ggsn1*:

```
ggsn-service ggsn1
```

gprs-service

Creates a GPRS service instance and enters the GPRS Service Configuration Mode. This mode configures all of the parameters specific to the operation of an SGSN in a GPRS network.

Important For details about the commands and parameters for this mode, check the *GPRS Service Configuration Mode* chapter.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

gprs-service *srvc_name* **[-noconfirm]**
no gprs-service *srvc_name*

no

Removes the configuration for the specified IGPRS service from the configuration for the current context.

srvc_name

Specifies the name of the GPRS service as a unique alphanumeric string of 1 through 63 characters.

Important Service names must be unique across all contexts within a chassis.

-noconfirm

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

Usage Guidelines Use this command to create or remove a GPRS service. Entering this command will move the system to the GPRS Service Configuration Mode and change the prompt to:

```
[context_name]hostname(config-gprs-service)#
```

Example

The following command creates an GPRS service named *gprs1*:

```
gprs-service gprs1
```

The following command removes the GPRS service named *gprs1*:

```
no gprs-service gprs1
```

gs-service

Creates a Gs service instance and enters the Gs Service Configuration Mode. This mode configures the parameters specific to the Gs interface between the SGSN and the MSC/VLR.

Product SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > **context** *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
gs-service svc_name [ -noconfirm ]
no gs-service svc_name
```

no

Remove the configured Gs service from the current context.

svc_name

Specifies the Gs service as a unique alphanumeric string of 1 through 63 characters.

Important Service names must be unique across all contexts within a chassis.

-noconfirm

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

Usage Guidelines Use this command to create, edit, or remove a Gs service.

A maximum of 32 Gs service can be configured in one context/system. This limit is subject to maximum of 256 services (regardless of type) can be configured per system.

Important For details about the commands and parameters for this mode, refer *Gs Service Configuration Mode* chapter.

Example

The following command creates an Gs service named *gs1*:

```
gs-service gs1
```

The following command removes the Gs service named *gs1*:

```
no gs-service gs1
```

gtpc high-throughput-sub

This command enables the GTPC configuration for high throughput subscribers.

Product P-GW

SAEGW

S-GW

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description **[no] gtpc high-throughput-sub dcnr-based sessmgr-select round-robin**

no

Disables the GTPC configuration for high throughput subscribers.

dcnr-based

Applies this configuration to all Create Session Requests that have a DCNR flag.

sessmgr-select

Specifies the method to select a session manager for a DCNR session.

round-robin

Selects the session managers for a high throughput session using the round-robin method.

Usage Guidelines

Use this command to enable the GTPC configuration for high throughput subscribers.

The gateway – S-GW, SAEGW or P-GW, classifies a session as a high throughput session based on a DCNR flag present in the IE: FLAGS FOR USER PLANE FUNCTION (UPF) SELECTION INDICATION, in the Create Session Request. This DCNR flag is check-pointed and recovered by the gateway.

A high throughput session is placed on a session manager that has no other high throughput session. If all session manager are handling a high throughput session then these sessions are allocated using the Round-Robbin method.

gtpc overload-protection egress

Configures the overload protection of GGSN/P-GW by throttling outgoing GTPv1 and GTPv2 control messages over Gn/Gp(GTPv1) or S5/S8 (GTPv2) interface using rate-limiting-function (RLF) template for services configured in a context.

Product

GGSN

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

gtpc overload-protection egress [rlf-template *rlf_template_name* **| throttling-override-policy** *throttling_override_policy_name*
[no] gtpc overload-protection egress

no

Disables the GTP Outgoing Control Message Throttling for GGSN/P-GW services in this context.

rlf-template *rlf_template_name*

Associates a pre-configured Rate-Limiting-Function (RLF) template for throttling the GTP outgoing control messages for the GGSN/P-GW services in this context. This is a mandatory parameter to enable throttling.

Important Use the **rlf-template** command in Global Configuration mode to configure an RLF template.

throttling-override-policy*throttling_override_policy_name*

Associates a pre-configured GTP-C Throttling Override Policy to selectively bypass throttling for a specific message type. This is a mandatory parameter to bypass enabled throttling.

Important Use the **throttling-override-policy** command in Global Configuration mode to configure a GTP-C Throttling Override Policy.

Usage Guidelines

Use this command to enable the GTP Outgoing Control Message Throttling for GGSN/P-GW services configured in the same context. The RLF template associated with this command controls the throttling parameters.

Associating a GTP-C Throttling Override Policy determines which message types can bypass the rate limiting function.

Example

The following command enables the outgoing GTP control messages in a context using rlf-template *gtpc_1*:

```
gtpc overload-protection egress rlf-template gtpc_1
```

gtpc overload-protection ingress

Configures the over-load protection of GGSN/PGW/SAEGW/S-GW by throttling incoming new call GTPv1 and GTPv2 control messages over Gn/Gp (GGSN GTPv1) or S5/S8 (PGW GTPv2) or S4/S11 (S-GW GTPv2) interface with other parameters for GGSN/PGW/S-GW/SAEGW services configured in the same context.

Product

GGSN

P-GW

SAEGW

S-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
gtpc overload-protection ingress { msg-rate msg_rate  }  delay-tolerance
dur ] [ queue-size size ] [ exclude { sgw-interface [ priority-message ] }
 | { priority-message [ sgw-interface ] } ]
[default] gtpc overload-protection ingress
```

ingress

Configures throttling parameters for incoming new call GTPC messages for GGSN, PGW, SGW, and SAEGW services in this context.

default

Resets the GTP incoming control message throttling parameters of *msg-rate*, *delay-tolerance*, and *queue-size* to their default values for GGSN, P-GW, SAEGW, and S-GW services.

msg-rate *msg_rate*

Defines the number of GTP incoming messages that can be processed per second.

msg_rate is an integer with a minimum value of 100 and maximum value that is dependent on the chassis or card used as shown in the following table.

Value	Chassis/Card
2000	SSI SMALL
3000	SSI MEDIUM
20000	SSI LARGE
12000	SCALE MEDIUM
20000	SCALE LARGE
12000	ASR5000 PSC
20000	ASR5000 PSC2
20000	ASR5000 PSC3
20000	ASR5000 PPC
20000	ASR5500 DPC
20000	ASR5500 DPC2
3000	SSI FORGE

The default value of *msg_rate* is 0, which implies that it is disabled.

delay-tolerance *dur*

Defines the maximum number of seconds a incoming GTP message can be queued before it is processed. After exceeding this, the message is dropped.

dur is an integer between 1 through 10. The default value is 5.

queue-size *size*

Defines the maximum size of the queue to be maintained for incoming GTPC messages. If the queue exceeds the defined size *size*, any new incoming messages will be dropped.

size is an integer between 100 through 10000. The default value is 10000.

exclude

Excludes the specified interface.

sgw-interface resets the incoming throttling parameters "msg-rate" and "queue-size" to their default values for GTPC incoming new call messages at SGW ingress interface (S4, S11). “delay-tolerance” continues to be applied as the configured value for the GTPC messages on the SGW interface (S4, S11). The message queue size considered for Congestion Control feature for PGW/SGW/GGSN is reset to default value of 10K, if this keyword is configured.

priority-message enables bypassing of demux incoming throttling for incoming GTPC request messages that have the Message Priority (MP) flag set as “1” and Message Priority value set as “0” in the GTP header.

Note The priority-message" keyword is applicable only for the P-GW.

Usage Guidelines

Use this command to enable the GTP incoming control message throttling for GGSN/PGW/SAEGW/S-GW services configured in the same context.

New keywords **exclude** and **sgw-interface** have been added to the CLI command **gtpc overload-protection ingress** to disable throttling exclusively for S-GW ingress GTPC interfaces (S4, S11).

1. When **gtpc overload-protection ingress** CLI is configured without the **exclude sgw-interface** option, the configured values of msg rate, delay tolerance and queue-size are enabled on new call messages at S-GW ingress interface (S4, S11).
2. When **exclude sgw-interface**is configured for the GTPC messages on the S-GW interface (S4, S11), below are the values taken by different parameters:
3. If **exclude sgw-interface**is configured, GTPC ingress messages throttling is applied (with the configured values of **msg rate**, **delay tolerance** and **queue-size**) to the external interfaces of P-GW and GGSN such as S5, S8, S2b, Gn/Gp, only to the new call create messages incoming from outside of the ASR5k. GTPC ingress message throttling is also applied (with the configured values of *msg-rate*, *delay-tolerance*, and *queue-size*) to the internal interfaces of the SAEGW such as the S5/S8 interfaces, only to the new call create messages received at the local P-GW of the SAEGW.
4. If ingress throttling is configured using **gtpc overload-protection ingress** with **exclude sgw-interface**, then for congestion control calculation for P-GW/S-GW/GGSN/SAEGW demuxmgr based on message queue size, the default queue size value of 10K is used.

   If ingress throttling is configured using **gtpc overload-protection ingress** without **exclude sgw-interface**, then for congestion control calculation for P-GW/S-GW/GGSN/SAEGW demuxmgr based on message queue size, the configured queue-size value will be used.

   The following table describes various scenarios of the configuration:

GTPC Incoming Throttling Queue-size Configuration (100..10K)	If "exclude sgw-interface" configured	Queue-size used for GTPC Incoming Throttling for P-GW/GGSN	Queue-size used for GTPC Incoming Throttling for S-GW	Queue-size considered for Congestion Control Threshold for P-GW/GGSN/S-GW	Behaviour Change
No configuration/Default configuration	No	10K (Default)	10K (Default)	Configured_congestion_threshold * 10K (Default)	No
No configuration/Default configuration	Yes	10K (Default)	10K (Default)	Configured_congestion_threshold * 10K (Default)	No
5K (or any configured value from 100..10K)	No	5k (or the configured value)	5k (or the configured value)	Configured_congestion_threshold * 5k (or the configured value)	No
5k (or Any configured value from 100..10K)	Yes	5k (or the configured value)	10k (because "exclude sgw-interface" is configured)	Configured_congestion_threshold * 10k (this is the behaviour change for congestion control, if "exclude sgw-interface" is configured)	Yes

In Release 21.4, the **priority-message** keyword is added to the existing gtpc overload-protection ingress CLI to enable bypassing of demux incoming throttling for incoming GTPC request messages where the “MP” flag is set as 1 and Message Priority value set as 0 in the GTP header.

This keyword is disabled by default.

If the new **exclude priority-message** CLI keyword is configured, it applies the following behaviour to bypass incoming throttling for high priority messages:

- High priority messages, the default configuration for “msg-rate” and “queue-size” of demux are applicable (even if they are configured with a different value). The default value for “msg-rate” is 0, which implies that High Priority setting is disabled. The default value for “queue-size” is 10000.
- There is no throttling applied due to the “delay-tolerance” parameter for High Priority messages.
- Also High Priority Create Session Request (CSReq) messages are prioritized over other messages. However, High Priority CSReq messages are processed in sequence.
- When a High Priority message is received and the queue is overloaded then a Low Priority message is discarded from the queue to accommodate the High Priority message.
- In a rare scenario where all the messages in the queue are High Priority and the queue is overloaded, then the new High Priority message may get dropped.

- If ingress throttling is configured using "gtpc overload-protection ingress" with "exclude priority-message" option, then for congestion control calculation for P-GW, S-GW, GGSN, and SAEGW demux manager based on the demux message queue size, the default queue size value of 10,000 is used. (This is the same behaviour if **exclude sgw-interface** is selected.)
- If ingress throttling is configured using "gtpc overload-protection ingress" without the "exclude" option, then for congestion control calculation for P-GW, S-GW, GGSN, and SAEGW demux manager based on demux message queue size, the configured queue-size value is used.

  The following table describes the behavior when the **exclude priority-message** is configured:

GTPC Incoming Throttling Demux Queue-size Configuration (100 to 10000)	Is "exclude priority-message" configured	Demux Queue-size used for GTPC Incoming Throttling for S-GW/GGSN/ "Low Priority" P-GW messages	Demux Queue-size used for "High Priority messages" P-GW messages	Queue-size considered for Congestion Control Threshold for P-GW/GGSN/S-GW
No configuration/Default configuration	No	10000 (default)	10000 (default)	Configured_congestion_threshold * 10000 (default)
No configuration/Default configuration	Yes	10000 (default)	10000 (default)	Configured_congestion_threshold * 10000 (default)
5000 (or any configured value from 100 to10000)	No	5000 (or the configured value)	5000 (or the configured value)	Configured_congestion_threshold * 5000 (default)
5000 (or any configured value from 100 to10000)	Yes	5000 (or the configured value)	10000 (because "exclude priority-message" is configured)	Configured_congestion_threshold * 10000 (this is the behavior change for congestion control, if "exclude priority-message" is configured)

Example

The following command enables the throttling of incoming new call GTP control messages in a context using message rate *1000* per second with message queue size *10000* and delay tolerance of *1* second:

```
gtpc overload-protection ingress msg-rate 1000 delay-tolerance 1 queue-size
 10000
```

Example

The following command bypasses incoming throttling for high priority messages.

```
gtpc overload-protection ingress msg-rate 100 exclude priority-message
```

gtpc peer-salvation

Configures peer salvation for inactive GTPv2 peers for EGTP services in this context.

Product

P-GW

SAEGW

S-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ no ] gtpc peer-salvation { min-peers` *value* **| timeout** *value* **}**

no

Disables peer salvation for inactive GTPv2 peers for EGTP services in the context.

min-peers *value*

Configures the minimum number of accumulated GTPv2 peers across all EGTP services to start salvaging the inactive peers. The value ranges from 2000 to 12000.

timeout *value*

Configures the peer salvation timeout. The peer that is inactive for salvation time is salvaged, in hours. The value ranges from 1 to 48 hours.

Usage Guidelines

Use this command to enable peer salvation for inactive GTPv2 peers for EGTP services in this context. The **peer-salvation** keyword is introduced in the Context Configuration Mode. Minimum peers and timeout values can be provided with this CLI, which will be per egtpmgr (separate for egtpinmgr and egtpegmgr) and across all the egtp-services configured in that context.

This command is disabled by default.

Important

- When the **peer-salvation** keyword is enabled at the context level, but not enabled at egtp-service level, then peer salvation does not occur.
- 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.
- The **min-peers** value should be applied judiciously to ensure that the Session Manager in a fully loaded chassis does not go into warn/over state with many peer records. If the Session Manager goes into a warn/over state, then it is recommended to configure a lesser value for min-peers to ensure that the peers are salvaged.
- **min-peers** configuration is not considered during a new peer creation.
- Only peers with zero number of sessions are salvaged for the configured timeout value. Non-zero number of sessions is not salvaged even if there are few.

Example

The following command specifies the number of peers to be salvaged and the timeout value.

```
gtpc peer-salvation min-peers 4000 timeout 5
```

gtpc-system-param-poll interval

Sets the time period over which to monitor the chassis level CPU, Memory and Session count information from the resource manager.

Product

P-GW

SAEGW

S-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > **context** *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

gtpc-system-param-poll interval *seconds*
default gtpc-system-param-poll interval

default

Returns the GTP-C system parameter polling interval to the default setting of 30 seconds.

gtpc-system-param-poll interval *seconds*

Sets the time period over which to monitor the chassis level CPU, Memory and Session count information from the resource manager.

Valid entries are from 15 to 300 seconds.

The default setting is 30 seconds.

Caution Setting the time interval to a low value may impact system performance.

Usage Guidelines

In capacity testing and also in customer deployments it was observed that the chassis load factor for the R12 Load and Overload Support feature was providing incorrect values even when the sessmgr card CPU utilization was high. The root cause is that when the load factor was calculated by taking an average of CPU utilization of sessmgr and demux cards, the demux card CPU utilization never increased more than the sessmgr card CPU utilization. As a result, the system did not go into the overload state even when the sessmgr card CPU utilization was high.

This feature has been enhanced to calculate the load factor based on the higher value of similar types of cards for CPU load and memory. If the demux card's CPU utilization value is higher than the sessmgr card's CPU utilization value, then the demux card CPU utilization value is used for the load factor calculation.

This CLI command is introduced to configure different polling intervals for the resource manager so that the demuxmgr can calculate the load factor based on different system requirements.

Example

The following command sets the GTP-C system parameter polling interval to 40 seconds:

```
gtpc-system-param-poll interval 40
```

gtpp algorithm

Configures GTPP routing algorithms for the current context. This command is deprecated but available for backward compatibility.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description **gtpp algorithm { first-server | round-robin | first-n** *count* **}**

first-server

Specifies that accounting data is sent to the first available charging gateway function (CGF) based upon the relative priority of each configured CGF. Default: Enabled

round-robin

Specifies that accounting data is transmitted in a circular queue fashion such that data is sent to the highest priority CGF first, then to the next available CGF of the highest priority, and so on. Ultimately, the queue returns to the CGF with the highest configured priority. Default: Disabled

first-n *count*

Specifies that the AGW must send accounting data to *count* (more than one) CGFs based on their priority. Response from any one of the *count* CGFs would suffice to proceed with the call. The full set of accounting data is sent to each of the *count* CGFs.

count is the number of CGFs to which accounting data will be sent, and must be an integer from 2 through 65535. Default: 1 (Disabled)

Usage Guidelines Use this command to control how G-CDR/P-CDR accounting data is routed among the configured CGFs.

Example

The following command configures the system to use the round-robin algorithm when transmitting G-CDR/P-CDR accounting data:

```
gtpp algorithm round-robin
```

gtpp attribute

Allows the specification of the optional attributes to be present in the Call Detail Records (CDRs) that the GPRS/PDN/UMTS access gateway generates. It also defines that how the information is presented in CDRs by encoding the attribute field values.

Product GGSN

SGSN

P-GW

SAEGW

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
gtpp attribute { apn-ambr [ include-for-all-bearers |
include-for-default-bearer | include-for-non-gbr-bearers ] | apn-ni |
apn-selection-mode | charging-characteristic-selection-mode | camel-info
 | cell-plmn-id |  { ciot-cp-optind | ciot-unipdu-cponly } | diagnostics
 [ abnormal-release-cause ] | direct-tunnel | duration-ms | dynamic-flag
 | dynamic-flag-extension | furnish-charging-information | imei |
imsi-unauthenticated-flag | lapi last-ms-timezone | last-uli |
local-record-sequence-number | losdv | ms-timezone | msisdn | node-id |
node-id-suffix STRING | pdn-connection-id | pdp-address | pdp-type |
pgw-ipv6-addr | pgw-plmn-id | plmn-id | qos max-length | rat |
recordextension | record-extensions rat | record-type { sgsnpdprecord |
sgwrecord } | served-mnai | served-pdp-pdn-address-extension |
served-pdp-pdn-address-prefix-length | sgsn-change |  sms {
destination-number | recording-entity | service-centre } | sgw-ipv6-addr
 | sna-ipv6-addr | sponsor-id | start-time | stop-time | twanuli | uli |
 user-csg-information } +
default gtpp attribute { apn-ambr [ include-for-all-bearers |
include-for-default-bearer | include-for-non-gbr-bearers ] | apn-ni |
apn-selection-mode | charging-characteristic-selection-mode | camel-info
 | cell-plmn-id |  { ciot-cp-optind | ciot-unipdu-cponly } | diagnostics
 [ abnormal-release-cause ] | direct-tunnel | duration-ms | dynamic-flag
 | dynamic-flag-extension | furnish-charging-information | imei |
imsi-unauthenticated-flag | lapi last-ms-timezone | last-uli |
local-record-sequence-number | losdv | ms-timezone | msisdn | node-id |
node-id-suffix STRING | pdn-connection-id | pdp-address | pdp-type |
pgw-ipv6-addr | pgw-plmn-id | plmn-id | qos max-length | rat |
recordextension | record-extensions rat | record-type { sgsnpdprecord |
sgwrecord } | served-mnai | served-pdp-pdn-address-extension |
served-pdp-pdn-address-prefix-length | sgsn-change |  sms {
destination-number | recording-entity | service-centre } | sgw-ipv6-addr
 | sna-ipv6-addr | sponsor-id | start-time | stop-time | twanuli | uli |
 user-csg-information } +
no gtpp attribute { apn-ambr [ include-for-all-bearers |
include-for-default-bearer | include-for-non-gbr-bearers ] | apn-ni |
apn-selection-mode | charging-characteristic-selection-mode | camel-info
 | cell-plmn-id |  { ciot-cp-optind | ciot-unipdu-cponly } | diagnostics
 [ abnormal-release-cause ] | direct-tunnel | duration-ms | dynamic-flag
 | dynamic-flag-extension | furnish-charging-information | imei |
imsi-unauthenticated-flag | lapi last-ms-timezone | last-uli |
local-record-sequence-number | losdv | ms-timezone | msisdn | node-id |
node-id-suffix STRING | pdn-connection-id | pdp-address | pdp-type |
pgw-ipv6-addr | pgw-plmn-id | plmn-id | qos max-length | rat |
recordextension | record-extensions rat | record-type { sgsnpdprecord |
sgwrecord } | served-mnai | served-pdp-pdn-address-extension |
served-pdp-pdn-address-prefix-length | sgsn-change |  sms {
destination-number | recording-entity | service-centre } | sgw-ipv6-addr
 | sna-ipv6-addr | sponsor-id | start-time | stop-time | twanuli | uli |
 user-csg-information } +
```

default

Sets the default GTPP attributes in the generated CDRs. It also sets the default presentation of attribute values in generated CDRs.

no

Removes the configured GTPP attributes from the CDRs.

apn-ambr [include-for-all-bearers | include-for-default-bearer | include-for-non-gbr-bearers]

Default: Disabled

This keyword controls the inclusion of the optional field "apn-ambr" in the PGW-CDRs in the custom24 GTPP dictionary.

Important This keyword option will be available only if a valid license is installed. For more information, contact your Cisco account representative.

The APN Aggregate Maximum Bit Rate (AMBR) is a subscription parameter stored per APN. It limits the aggregate bit rate that can be expected to be provided across all non-GBR bearers and across all PDN connections of the same APN. Each of these non-GBR bearers potentially utilize the entire APN AMBR, e.g. when the other non-GBR bearers do not carry any traffic. The APN AMBR is present as part of QoS information.

In 15.0 and later releases, this CLI command should be configured along with the following additional options to support APN-AMBR reporting in SGW-CDRs in all GTPP dictionaries.

- **include-for-all-bearers**: Includes the APN-AMBR information in SGW-CDRs for all bearers (GBR and NON-GBR)
- **include-for-default-bearer**: Includes APN-AMBR information in SGW-CDRs only for default bearer.
- **include-for-non-gbr-bearers**: Includes APN-AMBR information for non-gbr-bearers.

This feature is required to enable post-processing of CDRs to verify MVNO subscribers actual QoS against invoicing systems.

Important This CLI command and the associated options are not available for products other than S-GW and P-GW. The option "**non-gbr-bearers-only**" is available in S-GW and P-GW but the other options are available in S-GW only.

In the P-GW implementation, if the CLI command "**gtpp attribute apn-ambr**" is configured, it will be treated as "**gtpp attribute apn-ambr non-gbr-bearers-only**". In case of S-GW/P-GW combo if any of the options is configured, it will be considered that the attribute is available.

apn-ni

Default: Enabled

This keyword controls the inclusion of the optional field "APN" in the x-CDRs.

apn-selection-mode

Default: Enabled

This keyword controls the inclusion of the optional field "APN Selection Mode" in the x-CDRs.

camel-info

SGSN only

Enter this keyword to include CAMEL-specific fields in SGSN CDRs. Default: Disabled

cell-plmn-id

SGSN only

Enter this keyword to enable the system to include the Cell PLMN ID field in the M-CDR. Default: Disabled

charging-characteristic-selection-mode

Default: Enabled

This keyword controls the inclusion of the optional field "Charging Characteristic Selection Mode" in the x-CDRs.

ciot-cp-optind

Includes optional field "CP CIoT EPS optimisation indicator" in the CDR.

ciot-unipdu-cponly

Includes optional field "UNI PDU CP Only Flag" in the CDR.

diagnostics [abnormal-release-cause]

Default: Disabled

Enables the system to include the Diagnostic field in the CDR that is created when PDP contexts are released. The field will include one of the following values:

- **26** - For GGSN: if the GGSN sends "delete PDP context request" for any other reason (e.g., the operator types "clear subscribers" on the GGSN). For SGSN: The SGSN includes this cause code in the S-CDR to indicate that a secondary PDP context activation request or a PDP context modification request has been rejected due to insufficient resources.
- **36** - For GGSN: this cause code is sent in the G-CDR to indicate the PDP context has been deactivated in the GGSN due to the SGSN having sent a "delete PDP context request" to the GGSN. For SGSN, this cause code is used to indicate a regular MS or network-initiated PDP context deactivation.
- **37** - when the network initiates a QoS modification, the SGSN sends in the S-CDR to indicate that the MS initiation deactivate request message has been rejected with QoS not accepted as the cause.
- **38** - if the GGSN sends "delete PDP context request" due to GTP-C/GTP-U echo timeout with SGSN. If the SGSN sends this cause code, it indicates PDP context has been deactivated due to path failure, specifically GTP-C/GTP-U echo timeout.
- **39** - SGSN only - this code indicates the network (GGSN) has requested a PDP context reactivation after a GGSN restart.

- **40** - if the GGSN sends "delete PDP context request" due to receiving a RADIUS Disconnect-Request message.

abnormal-release-cause: This keyword controls the inclusion of abnormal bearer termination information in diagnostics field of SGW-CDR. Note that the CLI command "**gtpp attribute diagnostics**" will disable **abnormal-release-cause** and enable the **diagnostics** field. The **no gtpp attribute diagnostics** command will disable both **abnormal-release-cause** and **diagnostics** field.

Important The Abnormal Bearer Termination feature is currently applicable only to custom34 and custom35 GTPP dictionaries. That is, the bearer termination cause is populated in SGW-CDR for custom34 and custom35 dictionaries, and PGW-CDRs for custom35 GTPP dictionary when the cause for record closing is "Abnormal Release".

direct-tunnel

Default: Disabled

Includes the Direct Tunnel field in PGW-CDR/eG-CDRs.

This keyword is applicable for GGSN, P-GW and S-GW only.

duration-ms

Specifies that the information contained in the mandatory Duration field be reported in milliseconds instead of seconds (as the standards require). Default: Disabled

dynamic-flag

Default: Enabled

This keyword controls the inclusion of the optional field "Dynamic Flag" in the x-CDRs.

dynamic-flag-extension

Default: Enabled

This keyword controls the inclusion of the optional field "Dynamic Address Flag Extension" in the x-CDRs.

This field is seen in the CDR when the IPv4 address is dynamically assigned for a dual PDP context. This extension field is required in the 3GPP Release 10 compliant CDRs so that the Dual Stack Bearer support is available.

furnish-charging-information

Default: Disabled

This keyword controls the inclusion of the optional field "pSFurnishChargingInformation" in the eG-CDRs and PGW-CDRs.

Important The Furnish Charging Information (FCI) feature is applicable to all GTPP dictionaries compliant to 3GPP Rel.7 and 3GPP Rel.8 except custom43 dictionary. This keyword option will be available only if a valid license is installed. For more information, contact your Cisco account representative.

PGW-CDR and eG-CDR will contain FCI only if it is enabled at command level, i.e. using the **gtpp attribute furnish-charging-information** command in GTPP Server Group Configuration mode.

Whenever FCI changes, a new Free-Format-Data (FFD) value is either appended to existing FFD or overwritten on the existing FDD depending on Append-Free-Format-Data (AFFD) flag. CDR is not generated upon FCI change.

FCI is supported in main CDR as well as in LOSDV. Whenever a trigger (volume, time, RAT, etc.) happens current available FFD at command level is added to the main body of the CDR. The same FFD at command level is added to the main body of the next CDRs until it is not appended or overwritten by next Credit-Control-Answer message at command level.

In the case of custom43 dictionary, the FCI implementation will be as follows:

- Whenever FCI changes PGW-CDR will generate CDR i.e close old bucket and will have old FCI details in the generated CDR.
- Translation for the PS-Free-Format-Data in CDR will be conversion of hexadecimal values in ASCII format (for numbers 0 to 9) to decimal values as integers.
- PS-Append-Free-Format-Data always OVERWRITE.

imei

Default: Disabled

For SGSN: includes the IMEI value in the S-CDR.

For GGSN: includes the IMEISV value in the G-CDR.

imsi-unauthenticated-flag

Default: Enabled

This keyword controls the inclusion of the optional field "IMSI Unauthenticated Flag" in the x-CDRs.

When the served IMSI is not authenticated, this field "IMSI Unauthenticated Flag" if configured, will be present in the P-GW CDR record for custom35 dictionary. This field is added per 3GPP TS 32.298 v10.7.

lapi

Default: Disabled

Includes the Low Access Priority Indicator (LAPI) field in the CDRs. This field is required to support MTC feature.

When UE indicates low priority connection, then the "lowPriorityIndicator" attribute will be included in the CDR.

last-ms-timezone

Default: Disabled

Sets the "Last MS-Timezone" in the CDR field. This option would be disabled when the default option is used.

last-uli

Default: Disabled

Sets the "Last ULI" in the CDR field. This option would be disabled when the default option is used.

local-record-sequence-number

Default: Disabled

This keyword provides both the local record sequence number and the Node ID. In the x-CDRs, this field indicates the number of CDRs generated by the node and is unique within the session manager.

The Node ID field is included in the x-CDR for any of several reasons, such as when PDP contexts are released or if partial-CDR is generated based on configuration. The field will consist of a AAA Manager identifier automatically appended to the name of the SGSN or GGSN service.

The name of the SGSN or GGSN service may be truncated, because the maximum length of the Node ID field is 20 bytes. Since each AAA Manager generates CDRs independently, this allows the Local Record Sequence Number and Node ID fields to uniquely identify a CDR.

Important If the **gtpp single-source centralized-lrsn** is configured, the 'Node-ID' field consists of only the specified NodeID-suffix. If NodeID-suffix is not configured, GTPP group name is used. For default GTPP groups, GTPP context-name is used. If the **gtpp single-source centralized-lrsn** is not configured, then node-id format for CDRs generated by Sessmgr is as follows: <1-byte Sessmgr restartvalue><3-byte Sessmgr instance number> <node-id-suffix>. If the **gtpp single-source centralized-lrsn** is not configured, then node-id format for CDRs generated by ACSmgr is as follows: <1-byte ACSmgr restart-value> <3-byte ACSmgr instance number> <Active charging service-name>.

losdv

Default: Enabled

This keyword controls the inclusion of the optional field "List of Service Data" in the x-CDRs.

ms-timezone

Default: Enabled

This keyword controls the inclusion of the optional field "MS-Timezone" in the x-CDRs.

msisdn

Default: Enabled

This keyword controls the inclusion of the optional field "MSISDN" in the x-CDRs.

node-id

Default: Enabled

This keyword controls the inclusion of the optional field "Node ID" in the x-CDRs.

node-id-suffix *STRING*

Default: Disabled

Specifies the configured Node-ID-Suffix to use in the NodeID field of GTPP CDRs as an alphanumeric string of 1 through 16 characters. Each Session Manager task generates a unique NodeID string per GTPP context.

Important The NodeID field is a printable string of the *ndddSTRING* format: *n*: The first digit is the Sessmgr restart counter having a value between 0 and 7. *ddd*: The number of sessmgr instances. Uses the specified NodeID-suffix in all CDRs. The "Node-ID" field consists of sessMgr Recovery counter (1 digit) *n* + AAA Manager identifier (3 digits) *ddd* + the configured Node-Id-suffix (1 to 16 characters) *STRING*. If the centralized LRSN feature is enabled, the "Node-ID" field will consist of only the specified NodeID-suffix (NodeID-prefix is not included). If this option is not configured, then GTPP group name will be used instead (For default GTPP groups, context-name will be used).

Important If this **node-id-suffix** is not configured, the GGSN uses the GTPP context name as the Node-id-suffix (truncated to 16 characters) and the SGSN uses the GTPP group named as the node-id-suffix.

pdn-connection-id

Default: Enabled

This keyword controls the inclusion of the optional field "PDN Connection ID" in the x-CDRs.

pdp-address

Default: Enabled

This keyword controls the inclusion of the optional field "PDP Address" in the x-CDRs.

pdp-type

Default: Enabled

This keyword controls the inclusion of the optional field "PDP Type" in the x-CDRs.

pgw-ipv6-addr

Default: Disabled

Specifying this option allows to configure the P-GW IPv6 address.

Important This attribute can be controllably configured in custom24 and custom35 SGW-CDR dictionaries.

pgw-plmn-id

Default: Enabled

This keyword controls the inclusion of the optional field "PGW PLMN-ID" in the x-CDRs.

plmn-id [unknown-use]

Default: Enabled

For SGSN, reports the SGSN PLMN Identifier value (the RAI) in the S-CDR provided if the dictionary supports it.

For GGSN, reports the SGSN PLMN Identifier value (the RAI) in the G-CDR if it was originally provided by the SGSN in the GTP create PDP context request. It is omitted if the SGSN does not supply one.

Normally when SGSN PLMN-id information is not available, the attribute sgsnPLMNIdentifier is not included in the CDR. This keyword enables the inclusion of the sgsnPLMNIdentifier with a specific value when the SGSN PLMN-id is not available.

unknown-use *hex_num*: is aa hexadecimal number from 0x0 through 0xFFFFFF that identifies a foreign SGSN that has not provided a PLMN-id. For GGSN only.

qos max-length

Default: Disabled

Specifying this option will change the parameters related to QoS sent in S-CDR and SaMOG CDR. The **max-length** option is used to modify the length of QoS sent in CDR. The **qos_value** must be an integer from 4 through 24.

This feature is introduced to support Rel.7+ QoS formats.

rat

Default: Enabled

For SGSN: includes the RAT (identifies the radio access technology type) value in the S-CDR.

For GGSN: includes the RAT (identifies the radio access technology type) value in the G-CDR.

recordextension

Default: Disabled

This keyword controls the inclusion of the optional field "RecordExtension" in the x-CDRs.

record-extensions rat

Default: Disabled

Enables network operators and/or manufacturers to add their own recommended extensions to the CDRs according to the standard record definitions from 3GPP TS 32.298 Release 7 or higher.

record-type { sgsnpdprecord | sgwrecord }

Important This keyword is available only when the SaMOG Mixed Mode license (supporting both 3G and 4G) is configured.

Default: sgwrecord

Specifies the SaMOG CDR type to use.

For an SaMOG 3G license, this keyword will not be available. However, sgsnpdprecord type will be used as the default record type.

served-mnai

Default: Disabled

This keyword controls the inclusion of the optional field "Served MNAI" in the x-CDRs.

served-pdp-pdn-address-extension

Default: Disabled

In support of IPv4v6 dual-stack PDP address types, this keyword causes the service to include IPv4v6 address information in the CDR. The IPv4 address goes in the Served PDP PDN Address Extension field and the IPv6 address goes in the Served PDP Address or Served PDP PDN Address field.

Important This attribute will not be displayed if the GTPP dictionary is set to custom34.

Note For SGSN, on enabling **served-pdp-pdn-address-extension** all custom S-CDR dictionaries will support the CDR field "Served PDP/ PDN Address extension" except for the following dictionaries:

- custom17
- custom18
- custom23
- custom42
- custom41

served-pdp-pdn-address-prefix-length

Default: Enabled

In support of IPv6 prefix delegation, this keyword causes the service to include this field "Served PDP PDN Address" in the x-CDRs.

If this field is configured, the servedPDPPDNAddress field will support reporting the IPv6 prefix length as outlined in 3GPP 32.298. The prefix length will only be reported if:

- it is configured
- it is not the default length of 64
- it is an IPv6 or IPv4v6 call

sgsn-change

Default: Enabled

This keyword is specific to SGSN and is license restricted.

This keyword controls the inclusion of the S-CDR attribute "SGSN Change" in the S-CDRs. It is enabled by default and the attribute "SGSN Change" is included in the S-CDRs by default.

Note For SGSN specific custom33 dictionary, it is recommended to disable this keyword before an upgrade to prevent billing issues.

sgw-ipv6-addr

Default: Disabled

Specifying this option allows to configure the S-GW IPv6 address.

Important This attribute can be controllably configured in custom24 and custom35 SGW-CDR dictionaries.

sms { destination-number | recording-entity | service-centre }

This keyword is specific to the SGSN.

Entering this keyword causes the inclusion of an SMS-related field in the SMS-MO-CDR or SMS-MT-CDR.

destination-number: Includes the "destinationNumber" field in the SMS-MO-CDR or SMS-MT-CDR.

recording-entity: Includes the "recordingEntity" field in the SMS-MO-CDR or SMS-MT-CDR.

service-centre: Includes the "serviceCentre" field in the SMS-MO-CDR or SMS-MT-CDR.

sna-ipv6-addr

Default: Disabled

Specifying this option allows to configure the Serving Node IPv6 Address (SNAv6).

Important This attribute can be controllably configured in custom24 and custom35 SGW-CDR dictionaries.

sponsor-id

Default: Disabled

Includes the Sponsor ID and Application-Service-Provider-Identity fields in PGW-CDR.

Note that the "Sponsor ID" and "Application-Service-Provider-Identity" attributes will be included in PGW-CDR if the PCEF supports Sponsored Data Connectivity feature or the required reporting level is sponsored connectivity level as described in 3GPP TS 29.212.

This feature is implemented to be in compliance with Release 11 3GPP specification for CDRs. So, this behavior is applicable to all GTPP dictionaries that are Release 11 compliant, i.e. custom35.

start-time

Default: Enabled

This keyword controls the inclusion of the optional field "Start-Time" in the x-CDRs.

stop-time

Default: Enabled

This keyword controls the inclusion of the optional field "Stop-Time" in the x-CDRs.

twanuli

Default: Disabled

This keyword controls the inclusion of the optional field "TWAN User Location Information" in the CDRs.

uli

Default: Enabled

This keyword controls the inclusion of the optional field "User Location Information" in the x-CDRs.

user-csg-information

Default: Disabled

This keyword controls the inclusion of the optional field "User CSG Information" in the x-CDRs.

Important Currently, UCI values are only supported for SGW-CDRs.

This attribute will not be displayed if the GTPP dictionary is set to custom11, custom34, or custom35.

+

Indicates that this command can be entered multiple times to configure multiple attributes.

Usage Guidelines

Use this command to configure the type of optional information fields to include in generated CDRs (M-CDRs, S-CDRs, S-SMO-CDR, S-SMT-CDR from SGSN and G-CDRs, eG-CDRs from GGSN) by the AGW (SGSN/GGSN/P-GW/SAEGW). In addition, it controls how the information for some of the mandatory fields are reported.

Fields described as optional by the standards but not listed above will always be present in the CDRs, except for Record Extensions (which will never be present).

Important This command can be repeated multiple times with different keywords to configure multiple GTPP attributes.

Example

The following command configures the system to present the time provided in the Duration field of the CDR is reported in milliseconds:

```
gtpp attribute duration-ms
```

gtpp charging-agent

Configures the IP address and port of the system interface within the current context used to communicate with the Charging Gateway Function (CGF).

Product

GGSN

SGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

gtpp charging-agent address *ip_address* **[port** *port* **]**
no gtpp charging-agent

no

Removes a previously configured charging agent address.

address *ip_address*

Specifies the IP address of the interface configured within the current context that is used to transmit CDR records (G-CDR/eG-CDR/M-CDR/S-CDR) to the CGF. *ip_address* must be entered using IPV4 dotted-decimal notation.

port *port*

Specifies the Charging Agent UDP port. as an integer from 1 through 65535.

If *port* is not defined, IP will take the default port number 49999.

Important

Configuring gtpp charging-agent on port 3386 may interfere with a ggsn-service configured with the same ip address.

Usage Guidelines

This command establishes a Ga interface for the system. For GTPP accounting, one or more Ga interfaces must be specified for communication with the CGF. These interfaces must exist in the same context in which GTPP functionality is configured (refer to the **gtpp** commands in this chapter).

This command instructs the system as to what interface to use. The IP address supplied is also the address by which the GSN is known to the CGF. Therefore, the IP address used for the Ga interface could be identical to one bound to a GSN service (a Gn interface).

If no GSN service is configured in the same context as the Ga interface, the address configured by this command is used to receive unsolicited GTPP packets.

Example

The following command configures the system to use the interface with an IP address of *192.168.13.10* as the accounting interface with port *20000* to the CGF:

```
gtpp charging-agent address 192.168.13.10 port 20000
```

gtpp data-record-format-version

Encodes the data record format version. The version indicates the 3GPP release version.

Product

Important In releases prior to 18, this is applicable only to custom24 and custom35 GTPP dictionaries for S-GW. In 18 and later releases, this command is applicable to all GTPP dictionaries for all products including GGSN, P-GW, S-GW and SGSN.

GGSN

P-GW

SGSN

S-GW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] gtpp data-record-format-version *string*

no

Specifies that the default data record format will be encoded based on the GTPP dictionary being used.

gtpp data-record-format-version *string*

Specifies the 3GPP release version to be encoded. *string* must be in the format a.b (for example 10.10). The entry can be from 1 to 1023 alphanumeric characters.

Usage Guidelines

Use this command to support a configurable multiple data record format version *only for custom24 and custom35 dictionaries* in releases prior to 18, and all GTPP dictionaries in release 18 and beyond. The entry can be from 1 to 1023 alphanumeric characters. This is useful when the value of the data record format version is taken according to the dictionary being used. If only the default configuration is used, a version mismatch causes the GTPP request to be discarded while using R10 attributes.

Example

This example configures the data record format version *10.10* to be encoded.

```
gtpp data-record-format-version 10.10
```

gtpp data-request sequence-numbers

Configures the range of sequence numbers to be used in the GTPP data record transfer record (DRT). Use this command to set the start value for the sequence number.

Product

GGSN

SGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
gtpp data-request sequence-numbers start { 0 | 1 }
default gtpp data-request sequence-numbers start
```

default

Default is 0 (zero).

{ 0 | 1 }

Specifies the value of the start sequence number for the GTPP Data Record Transfer Request. Default: 0

- **0**: Designates the start sequence number as 0.
- **1**: Designates the start sequence number as 1.

Usage Guidelines

When the GGSN/P-GW (SAEGW)/SGSN is configured to send GTPP echo request packets, the SGSN always uses 0 as the sequence number in those packets. Re-using 0 as a sequence number in the DRT packets is allowed by the 3GPP standards; however, this CLI command ensures the possibility of inter-operating with CGFs that can not properly handle the re-use of sequence number0 in the echo request packets.

Example

The following command sets the sequence to start at *1*.

```
gtpp data-request sequence-numbers start 1
```

gtpp dead-server suppress-cdrs

Enables or disables CDR archiving when a dead server is detected.

Important This command is customer specific. For more information please contact your local Cisco service representative.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[default | no] gtpp dead-server suppress-cdrs

default

Configures the default setting.

Default: Disabled

no

Re-enables CDR archiving.

Usage Guidelines

Use this command to enable/disable CDR archiving when a dead server is detected.With this CLI, once a server is detected as down, requests are purged.Also the requests generated for the period when the server is down are purged.

gtpp deadtime

Configures the amount of time to wait before attempting to communicate with a Charging Gateway Function (CGF) that was previously marked as unreachable.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

gtpp deadtime *time*
default gtpp deadtime

default

Configures this command with the default setting.

Default: 120 seconds

time

Specifies the amount of time (in seconds) that must elapse before the system attempts to communicate with a CGF that was previously unreachable. *time* is an integer from 1 through 65535.

Usage Guidelines

If the system is unable to communicate with a configured CGF, after a pre-configured number of failures the system marks the CGF as being down.

This command specifies the amount of time that the system waits prior to attempting to communicate with the downed CGF.

Refer to the **gtpp detect-dead-server** and **gtpp max-retries** commands for additional information on the process the system uses to mark a CGF as down.

Example

The following command configures the system to wait *60* seconds before attempting to re-communicate with a CGF that was marked as down:

gtpp deadtime 60

gtpp detect-dead-server

Configures the number of consecutive communication failures that could occur before the system marks a Charging Gateway Function (CGF) as down.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

gtpp detect-dead-server consecutive-failures *max_number*
default gtpp detect-dead-server consecutive-failures

default

Configures this command with the default setting.

Default: 0

consecutive-failures *max_number*

Specifies the number of failures that could occur before marking a CGF as down. *max_number* is an integer from 0 through 1000.

Usage Guidelines

This command works in conjunction with the **gtpp max-retries** parameter to set a limit to the number of communication failures that can occur with a configured CGF.

The gtpp max-retries parameter limits the number of attempts to communicate with a CGF. Once that limit is reached, the system treats it as a single failure. The gtpp detect-dead-server parameter limits the number of consecutive failures that can occur before the system marks the CGF as down and communicate with the CGF of next highest priority.

If all of the configured CGFs are down, the system ignores the detect-dead-server configuration and attempt to communicate with highest priority CGF again.

Important When the **gtpp detect-dead-server consecutive-failures** CLI command is used in the CDR streaming mode, the CDRs will not be written to the HDD even when all the CGF servers are inactive. The CDR records will be archived at AAA manager and then purged when the archival limit is reached.

If the system receives a GTPP Node Alive Request, Echo Request, or Echo Response message from a CGF that was previously marked as down, the system immediately treats it as being active.

Refer to the **gtpp max-retries** command for additional information.

Example

The following command configures the system to allow *8* consecutive communication failures with a CGF before it marks it as down:

```
gtpp detect-dead-server consecutive-failures 8
```

gtpp dictionary

Designates a dictionary used by GTPP for a specific context.

Product

GGSN

SGSN

PDG/TTG

P-GW

SAEGW

S-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
gtpp dictionary { custom1 | custom10 | custom11 | custom12 | custom13 |
custom14 | custom15 | custom16 | custom17 | custom18 | custom19 | custom2
 | custom20 | custom21 | custom22 | custom23 | custom24 | custom25 |
custom26 | custom27 | custom28 | custom29 | custom3 | custom30 | custom31
 | custom32 | custom33 | custom34 | custom35 | custom36 | custom37 |
custom38 | custom39 | custom4 | custom40 | custom41 | custom42 | custom43
 | custom44 | custom45 | custom46 | custom47 | custom48 | custom49 |
custom5 | custom50 | custom51 | custom52 | custom53 | custom54 | custom55
 | custom56 | custom57 | custom58 | custom59 | custom6 |  custom60 |
custom7 | custom8 | custom9 | standard }
default gtpp dictionary
```

default

Configures the default dictionary.

custom1

This is a custom-defined dictionary that conforms to TS 32.015 v 3.6.0 for R99. It supports the encoding of IP addresses in text format for G-CDRs.

custom2

Custom-defined dictionary.

custom3

This is a custom-defined dictionary that conforms to TS 32.015 v 3.6.0 for R99 except that it supports the encoding of IP addresses in binary format for G-CDRs.

custom4

This is a custom-defined dictionary that conforms to TS 32.015 v 3.6.0 for R99 except that:

- IP addresses are encoded in binary format.
- The Data Record Format Version information element contains 0x1307 instead of 0x1308.
- QoS Requested is not present in the LoTV containers.
- QoS negotiated is added only for the first container and the container after a QoS change.

custom5

Custom-defined dictionary.

custom6

This is a custom-defined dictionary for eG-CDR encoding.

custom7 ... custom30

These custom-defined dictionary have default behavior or "standard" dictionary.

custom31

This is a custom-defined dictionary for S-CDR encoding that is based on 3GPP TS 32.298 v6.4.1 with a special field appended for the PLMN-ID.

custom33

This ia a custom-defined dictionary for S-CDR encoding that is based on the 3GPP TS 32.298v6.4.1 with the following exceptions:

- Proprietary PLMN-ID field is present.
- It is a SEQUENCE and not a SET.
- Diagnostics and SGSN-Change fields are not supported.
- Indefinite length encoding is used.
- Booleans are encoded as 0x01(3GPP it is 0xff).
- IMEISV shall be sent if available else IMEI should be sent.
- Record Sequence Number is Mandatory.
- APN OI and NI part is length encoded.
- Cause for Record closure should be "RAT Change" instead of "intra-SGSNinter-system".

standard

Default: Enabled

This dictionary conforms to TS 32.215 v 4.6.0 for R4 (and also R5 - extended QoS format).

Usage Guidelines

Use this command to designate specific dictionary used by GTPP for specific context.

Important Note that the following warning message will be displayed whenever an existing GTPP dictionary is being changed or a new GTPP dictionary is configured irrespective of whether or not the calls are active on the system.

Warning: It is not recommended to change the dictionary when the system has active calls.

Are you sure? [Yes|No]: n

Important This change will require user's input on the CLI console for GTPP dictionary configuration / change.

Example

The following command configures the system to use *custom3* dictionary to encode IP address in Binary format in G-CDRs:

gtpp dictionary custom3

gtpp duplicate-hold-time

Configures the number of minutes to hold on to CDRs that are possibly duplicates while waiting for the primary Charging Gateway Function (CGF) to come back up.

Product

GGSN

SGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

gtpp duplicate-hold-time *minutes*
default gtpp duplicate-hold-time

default

Configures this command with the default setting.

Default: 60 minutes

minutes

Specifies the number of minutes to hold on to CDRs that may be duplicates whenever the primary CGF is down, *minutes* must be an integer from 1 through 10080.

Usage Guidelines

Use this command to configure how long to hold on to CDRs that are possibly duplicates while waiting for the primary CGF to come back up. If the GGSN/P-GW (SAEGW) determines that the primary CGF is down, CDRs that were sent to the primary CGF but not acknowledged are sent by the GSN to the secondary CGF as "possibly duplicates". When the primary CGF comes back up, the GSN uses GTPP to determine whether the possibly duplicate CDRs were received by the primary CGF. Then the secondary CGF is told whether to release or cancel those CDRs. This command configures how long the system should wait for the primary CGF to come back up. As soon as the configured time expires, the secondary CGF is told to release all of the possibly duplicate CDRs.

Example

Use the following command to set the amount of time to hold on to CDRs to 2 hours (120 minutes);

```
gtpp duplicate-hold-time 120
```

gtpp echo-interval

Configures the frequency at which the system sends GTPP echo packets to configured CGFs.

Product

GGSN

SGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > **context** *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

gtpp echo-interval *time*
{ default | no } gtpp echo-interval

default

Configures the default setting for this command,

Default: 60 seconds

no

Disables the use of the echo protocol except for the scenarios described in the *Usage* section for this command.

time

Specifies the time interval (in seconds) for sending GTPP echo packets as an integer from 60 through 2147483647. Default: 60

Usage Guidelines

The GTPP echo protocol is used by the system to ensure that it can communicate with configured CGFs. The system initiates this protocol for each of the following scenarios:

- Upon system boot
- Upon the configuration of a new CGF server on the system using the **gtpp server** command as described in this chapter

- Upon the execution of the **gtpp test accounting** command as described in the *Exec Mode Commands* chapter of this reference
- Upon the execution of the **gtpp sequence-numbers private-extensions** command as described in this chapter

The echo-interval command is used in conjunction with the gtpp max-retries and gtpp timeout commands as described in this chapter.

In addition to receiving an echo response for this echo protocol, if we receive a GTPP Node Alive Request message or a GTPP Echo Request message from a presumed dead CGF server, we will immediately assume the server is active again.

The alive/dead status of the CGFs is used by the AAA Managers to affect the sending of CDRs to the CGFs. If all CGFs are dead, the AAA Managers will still send CDRs, (refer to the **gtpp deadtime** command), albeit at a slower rate than if a CGF were alive. Also, AAA Managers independently determine if CGFs are alive/dead.

Example

The following command configures an echo interval of *120* seconds:

```
gtpp echo-interval 120
```

gtpp egcdr

Configures the eG-CDR and P-CDR (P-GW CDR) parameters and triggers.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

gtpp egcdr { closure-reason admin-disconnect [management-intervention | normal-release] | final-record [[include-content-ids { all | only-with-traffic }] [closing-cause { same-in-all-partials | unique }]] | losdv-max-containers *max_losdv_containers* **| lotdv-max-containers** *max_lotdv_containers* **| dynamic-path** *ddl-path* **| rulebase-max-length** *rulebase_name_max_length* **| service-data-flow threshold { interval** *interval* **| volume { downlink** *bytes* **[uplink** *bytes* **] | total** *bytes* **| uplink** *bytes* **[downlink** *bytes* **] } } | service-idle-timeout { 0 |** *service_idle_timeout* **} }**
default gtpp egcdr { closure-reason admin-disconnect | dynamic-path | final-record include-content-ids only-with-traffic closing-cause same-in-all-partials | losdv-max-containers | lotdv-max-containers |

```
service-idle-timeout 0 }
no gtpp egcdr { dynamic-path | rulebase-max-length | service-data-flow
threshold { interval | volume { downlink [ uplink ] | total | uplink [
downlink ] } } }
```

closure-reason admin-disconnect [management-intervention | normal-release]

Controls the configuration of "causeForRecordClosing" in PGW-CDR when a call is cleared from the chassis.

Releases prior to 14.1, when a call is cleared from the chassis the field "causeForRecordClosing" in a PGW-CDR shows "Normal Release". In 15.0 and later releases, the behavior has changed to comply with the 3GPP specifications. That is, the default "causeForRecordClosing" in PGW-CDR will be "Management Intervention".

Important This behavioral change is limited to PGW-CDR Release 8 dictionaries only.

closing-reason: Configures the record closing reason for PGW-CDR.

- **management-intervention**: Specifies to send Management-Intervention as causeForRecordClosing in PGW-CDRs. By default, Management-Intervention will be sent as the record closure reason for PGW-CDRs.
- **normal-release**: Specifies to send Normal Release as causeForRecordClosing in PGW-CDRs.

final-record [[include-content-ids { all | only-with-traffic }] [closing-cause { same-in-all-partials | unique }]]

Enables configuration of the final eG-CDR/P-CDR.

Default: Restores the GTPP eG-CDR/P-CDR final record to the default setting to include content IDs with some data to report are included. Also, sets the closing cause to the default of using the same closing cause for multiple final eG-CDR/P-CDRs.

- **include-content-ids**: Controls which content IDs are being included in the final eG-CDR/P-CDR.
  - **all**: Specifies that all content IDs be included in the final eG-CDR/P-CDR.
  - **only-with-traffic**: Specifies that only content-IDs with traffic be included in the final eG-CDR/P-CDRs.
- **closing-cause**: Configures closing cause for the final eG-CDR/P-CDR.
  - **same-in-all-partials**: Specifies that the same closing cause is to be included for multiple final eG-CDR/P-CDRs
  - **unique**: Specifies that the closing cause for final eG-CDR/P-CDRs is to be unique.

losdv-max-containers *max_losdv_containers*

The maximum number of List of Service Data Volume (LoSDV) containers in one eG-CDR/P-CDR.

max_losdv_containers must be an integer from 1 through 255.

Default: 10

lotdv-max-containers *max_lotdv_containers*

The maximum number of List of Traffic Data Volume (LoTDV) containers in one eG-CDR/P-CDR.

max_lotdv_containers must be an integer from 1 through 8.

Default: 8

dynamic-path *ddl-path*

This keyword activates a new and extensible framework to enable field defined (customer created) eGCDR/PGW-CDR generation. This option enables the user to load the customized or modified dictionary. The dictionary configured through this CLI command takes precedence over existing the **gtpp dictionary** CLI command.

This new framework is implemented to define a GTPP dictionary in a structured format using a "Dictionary Definition Language (DDL)". Using this language, customers can clearly define fields, triggers and behaviors applicable for a particular GTPP dictionary.

DDL file will be parsed at compilation time and metadata will be populated to generate eGCDR and PGW-CDR. This metadata makes the new framework more modular and maintainable. This will help in faster turnaround time in supporting any new enhancements.

When customer wants to add/modify/remove a field, this information has to be updated in DDL. The DDL file is processed dynamically and the field reflects in CDR. This framework works only for eGCDR and PGW-CDR.

ddl-path: Specifies the path of dictionary DDL. The path must be a string of size 0 through 127. This is to support field-loadable ddls. The DDL file will be parsed to populate metadata required to generate eGCDR/PGW-CDR.

Important It is not recommended to enable **gtpp egcdr dynamic-path** when there are active calls.

In this release, both current and new framework are functional to enable field defined (customer created) eGCDR/PGW-CDR generation. By default, the new framework is disabled.

rulebase-max-length *rulebase_name_max_length*

Specifies the maximum character length of charging rulebase name in LOSDVs of eG- CDR/P-CDR.

rulebase_name_max_length must be an integer from 0 through 63. Zero (0) means the rulebase name is added as-is.

Default: None. That is, full (un-truncated) charging rulebase name will go in LOSDVs of eG-CDR/P-CDR.

service-data-flow threshold { interval *interval* | volume { downlink *bytes* [uplink *bytes*] | total *bytes* | uplink *bytes* [downlink *bytes*] } }

Configures the thresholds for closing a service data flow container within an eG-CDR/P-CDR.

- **interval** *interval*: Specifies the time interval, in seconds, to close the eG-CDR/P-CDR if the minimum time duration thresholds for service data flow containers satisfied in flow-based charging.

  interval must be an integer from 60 through 40000000.

  Default: Disabled

- **volume { downlink** *bytes* **[uplink** *bytes* **] | total** *bytes* **| uplink** *bytes* **[downlink** *bytes* **] }**: Specifies the volume octet counts for the generation of the interim G-CDR/P-CDRs to service data flow container in FBC.
  - **downlink** *bytes*: specifies the limit for the number of downlink octets after which the eG-CDR/P-CDR is closed.
  - **total** *bytes*: Specifies the limit for the total number of octets (uplink+downlink) after which the eG-CDR/P-CDR is closed.
  - **uplink** *bytes*: specifies the limit for the number of uplink octets after which the eG-CDR/P-CDR is closed.
  - *bytes* must be an integer from 10000 through 400000000.

A service data flow container has statistics for an individual content ID. When the threshold is reached, the service data flow container is closed.

service-idle-timeout { 0 | *service_idle_timeout* }

Specifies a time period where if no data is reported for a service flow, the service container is closed and added to eG-CDR/P-CDR (as part of LOSDV container list) with service condition change as ServiceIdleOut.

service_idle_timeout must be an integer from 10 through 86400.

0: Specifies no service-idle-timeout trigger.

Default: 0

Usage Guidelines

Use this command to configure individual triggers for eG-CDR/P-CDR generation.

Use the **service-data-flow threshold** option to configure the thresholds for closing a service data flow container within an eG-CDR (eG-CDRs for GGSN and P-CDRs for PGW) during flow-based charging (FBC). A service data flow container has statistics regarding an individual content ID.

Thresholds can be specified for time interval and for data volume, by entering the command twice (once with interval and once with volume). When either configured threshold is reached, the service data flow container will be closed. The volume trigger can be specified for uplink or downlink or the combined total (uplink + downlink) byte thresholds.

When the PDP context is terminated, all service data flow containers will be closed regardless of whether the thresholds have been reached.

An eG-CDR/P-CDR will have at most ten service data flow containers. Multiple eG-CDR/P-CDRs will be created when there are more than ten.

Example

Use the following command to set the maximum number of LoSDV containers to *7*:

```
gtpp egcdr losdv-max-containers 7
```

The following command sets an eG-CDR threshold interval of *6000* seconds:

```
gtpp egcdr service-data-flow threshold interval 6000
```

gtpp error-response

Configures the response when the system receives an error response after transmitting a DRT (data record transfer) request.

Product

GGSN

SGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
gtpp error-response { discard-cdr | retry-request }
default gtpp error-response
```

default

Configures this command with the default setting.

Default: **retry-request**

discard-cdr

Instructs the system to purge the request upon receipt of an error response and not to retry.

retry-request

Instructs the system to retry sending a DRT after receiving an error response. This is the default behavior.

Usage Guidelines

This command configures the system's response to receiving an error message after sending a DRT request.

Example

```
gtpp error-response discard-cdr
```

gtpp group

Configures GTPP server group in a context for the Charging Gateway Function (CGF) accounting server(s) that the system is to communicate with.

Product

ePDG

GGSN

SGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] gtpp group *group_name* **[-noconfirm]**

group_name

Specifies the name of GTPP server group that is used for charging and/or accounting in a specific context. *group_name* must be an alphanumeric string of 1 through 63 character.

A maximum of eight GTPP server groups (excluding system created default GTPP server group "default") can be configured with this command in a context.

no

Removes the previously configured GTPP group within a context.

When a GTPP group is removed accounting information is not generated for all calls using that group and all calls associated with that group are dropped. A warning message displays indicating the number of calls that will be dropped.

-noconfirm

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

Usage Guidelines

This feature provides the charging gateway function (CGF) accounting server configurable for a group of servers. Instead of having a single list of CGF accounting servers per context, this feature configures multiple GTPP accounting server groups in a context and each server group is consist of list of CGF accounting servers.

In case no GTPP server group is configured in a context, a server group named "default" is available and all the CGF servers configured in a specific context for CGF accounting functionality will be part of this "default" server group.

Example

The following command configures a GTPP server group named *star1* for CGF accounting functionality. This server group is available for all subscribers within that context.

```
gtpp group star1
```

gtpp max-cdrs

Configures the maximum number of charging data records (CDRs) included per packet.

Product

GGSN

P-GW

SAEGW

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

gtpp max-cdrs *max_cdrs* **[wait-time** *wait_time* **]**
default gtpp max-cdrs

default

Configures this command with the default setting.

Default: One CDR per packet; disables **wait-time**

max_cdrs

Specifies the maximum number of CDRs to be inserted in a single packet as an integer from 1 through 255. Default: 1

wait-time ***wait_time***

Specifies the number of seconds the system waits for CDRs to be inserted into the packet before sending it. *wait_time* must be an integer from 1 through 300. Default: Disabled

Important

If the **wait-time** expires, the packet is sent as this keyword over-rides *max_cdrs*.

Usage Guidelines

CDRs are placed into a GTPP packet as the CDRs close. The system stops placing CDRs into a packet when either the maximum *max_cdrs* is met, or the **wait-time** expires, or the value for the **gtpp max-pdu-size** command is met.

Example

The following command configures the system to place a maximum of *10* CDRs in a single GTPP packet before transmitting the packet:

```
gtpp max-cdrs 10
```

sgtpp max-pdu-size

Configures the maximum payload size of a single GTPP packet that could be sent by the system.

Product

GGSN

P-GW

SAEGW

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

gtpp max-pdu-size *pdu_size*
default gtpp max-pdu-size

default

Configures this command with the default setting.

Default:65400 bytes

pdu_size

Specifies the maximum payload size (in octets) of the GTPP packet as an integer from 1024 to65400. The payload includes the CDR and the GTPP header.

Caution

This command is effective only when GTPP single-source is configured, otherwise this command has no effect.

Usage Guidelines

The GTPP packet contains headers (layer 2, IP, UDP, and GTPP) followed by the CDR. Each CDR contains one or more volume containers. If a packet containing one CDR exceeds the configured maximum payload size, the system creates and send the packet containing the one CDR regardless.

The larger the packet data unit (PDU) size allowed, the more volume containers that can be fit into the CDR.

The system performs standard IP fragmentation for packets that exceed the system's maximum transmission unit (MTU).

Important The maximum size of an IPv4 PDU (including the IPv4 and subsequent headers) is 65,535. However, a slightly smaller limit is imposed by this command because the system's max-pdu-size doesn't include the IPv4 and UDP headers, and because the system may need to encapsulate GTPP packets in a different/larger IP packet (for sending to a backup device).

Example

The following command configures a maximum PDU size of *2048* octets:

```
gtpp max-pdu-size 2048
```

gtpp max-retries

Configures the maximum number of times the system attempts to communicate with an unresponsive Charging Gateway Function (CGF).

Product

GGSN

P-GW

SAEGW

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > **context** *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

gtpp max-retries *max_attempts*
default gtpp max-retries

default

Configures this command with the default setting.

Default: 4

max_attempts

Specifies the number of times the system attempts to communicate with a CGF that is not responding. *max_attempts* is an integer from 1 through 15.

Usage Guidelines

This command works in conjunction with the **gtpp detect-dead-server** and **gtpp timeout** parameters to set a limit to the number of communication failures that can occur with a configured CGF.

When the value specified by this parameter is met, a failure is logged. The gtpp detect-dead-server parameter specifies the number of consecutive failures that could occur before the server is marked as down.

In addition, the gtpp timeout command controls the amount of time between re-tries.

If the value for the max-retries is met, the system begins storing CDRs in Random Access Memory (RAM). The system allocates memory as a buffer, enough to store one million CDRs for a fully loaded chassis (a maximum of one outstanding CDR per PDP context). Archived CDRs are re-transmitted to the CGF until they are acknowledged or the system's memory buffer is exceeded.

Refer to the **gtpp detect-dead-server** and **gtpp timeout** commands for additional information.

Example

The following command configures the maximum number of re-tries to be *8*:

```
gtpp max-retries 8
```

gtpp node-id

Configures the GTPP Node ID for all CDRs.

Product

ePDG

GGSN

P-GW

SAEGW

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

gtpp node-id *node_id*
no gtpp node-id

no

Removes the previous gtpp node ID configuration.

node_id

Specifies the node ID for all CDRs as an alphameric string of 1 through 16 characters.

Usage Guidelines

Use this command to configure the GTPP Node ID for all CDRs.

Example

The following command configures the GTPP Node ID as *test123*:

```
gtpp node-id test123
```

gtpp redirection-allowed

Configures the system to allow or disallow the redirection of CDRs when the primary Charging Gateway Function (CGF) is unavailable.

Product

GGSN

P-GW

SAEGW

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
gtpp redirection-allowed
{ default | no } gtpp redirection-allowed
```

default

Configures this command with the default setting. Default: Enabled

no

Deletes the command from the configuration.

Usage Guidelines

This command allows operators to better handle erratic network links, without having to remove the configuration of the backup server(s) via the **no gtpp server** command.

This functionality is enabled by default.

If the no gtpp redirection-allowed command is executed, the system only sends CDRs to the primary CGF. If that CGF goes down, we will buffer the CDRs in memory until the CGF comes back or until the system runs out of buffer memory. In addition, if the primary CGF announces its intent to go down (with a GTPP Redirection Request message), the system responds to that request with an error response.

gtpp redirection-disallowed

This command has been obsoleted and is replaced by the **gtpp redirection-allowed** command.

gtpp server

Configures the Charging Gateway Function (CGF) accounting server(s) with which the system will communicate.

Product

ePDG

GGSN

P-GW

SAEGW

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
gtpp server ip_address [ max max_messages ] [ priority priority ] [ port port ]
[ node-alive { enable | disable } ] [ -noconfirm ]
no gtpp server ip_address
```

no

Deletes a previously configured CGF.

ip_address

Specifies the IP address of the CGF in IPv4 dotted-decimal or IPV6 colon-separated-hexadecimal notation.

max *max_messages*

Default: 256

Specifies the maximum number of outstanding or unacknowledged GTPP packets (from any one AAA Manager task) allowed for this CGF before the system begins buffering the packets.

max_messages can be configured as an integer from 1 through 256.

Important In release 16.0, a warning message is displayed if the user tries to configure a value greater than 100 and the max-outstanding is configured as 100. This is because there is an internal limit of up to 100 max outstanding requests that can be configured.

priority *priority*

Default:1000

Specifies the relative priority of this CGF. When multiple CGFs are configured, the priority is used to determine which CGF server to send accounting data to.

priority can be configured as an integer from 1 through 1000. When configuring two or more servers with the same priority you will be asked to confirm that you want to do this. If you use the **-noconfirm** option, you are not asked for confirmation and multiple servers could be assigned the same priority.

port *port*

Default: 3386

Specifies the port the CGF is using. *port* can be configured as an integer from 1 through 65535. Default value for port is 3286.

Important The **port** keyword option has been modified from **udp-port** to make it a generic command. The **udp-port** keyword can still be used, however, it will be in concealed mode and will not be shown in auto-complete or help for the command.

node-alive { enable | disable }

Default: Disable.

This optional keyword allows operator to enable/disable GSN to send Node Alive Request to GTPP Server (i.e. CGF). This configuration can be done per GTPP Server basis.

-noconfirm

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

Usage Guidelines

Use this command to configure the CGF(s) that the system sends CDR accounting data to.

Multiple CGFs can be configured using multiple instances of this command. Up to 12 CGF scan be configured per system context. Each configured CGF can be assigned a priority. The priority is used to determine which server to use for any given subscriber based on the routing algorithm that has been implemented. A CGF with a priority of "1" has the highest priority.

Important The configuration of multiple CGFs with the same IP address but different port numbers is not supported.

Each CGF can also be configured with the maximum allowable number of unacknowledged GTPP packets. Since multiple AAA Manager tasks could be communicating with the same CGF, the maximum is based on

any one AAA Manager instance. If the maximum is reached, the system buffers the packets Random Access Memory (RAM). The system allocates memory as a buffer, enough to store one million CDRs for a fully loaded chassis (a maximum of one outstanding CDR per PDP context).

Example

The following command configures a CGF with an IP address of *192.168.2.2* and a priority of *5*.

```
gtpp server 192.168.2.2 priority 5
```

The following command deletes a previously configured CGF with an IP address of *100.10.35.7*:

```
no gtpp server 100.10.35.7
```

gtpp source-port-validation

Toggles port checking for node alive/echo/redirection requests from the CGF.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
[ default | no ] gtpp source-port-validation
```

default

Configures this command with the default setting.

Default: Enabled

no

Disables CGF port checking.Only the IP address will be used to verify CGF requests.

Usage Guidelines

This command is for enabling or disabling port checking on node alive/echo/redirection requests from the CGF. If the CGF sends messages on a non-standard port, it may be necessary to disable port checking in order to receive CGF requests. On the default setting, both IP and port are checked.

Example

The following command disables port checking for CGF requests:

```
no gtpp source-port-validation
```

gtpp storage-server

Configures information for the GTPP back-up storage server.

Product

ePDG

GGSN

P-GW

SAEGW

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ no ] gtpp storage-server` *ip-address* **`port`** *port-num*

no

Removes a previously configured back-up storage server.

ip-address

Specifies the IP address of the back-up storage server expressed in IPv4 dotted-decimal notation.

port *port-num*

Specifies the UDP port number over which the GSN communicates with the back-up storage server. Default: 3386

Usage Guidelines

This command configures the information for the server to which GTPP packets are to be backed up to if all the CGFs are unreachable.

One backup storage server can be configured per system context.

Important

This command only takes affect if **gtpp single-source** in the Global Configuration Mode is also configured. Additionally, this command is customer specific. Please contact your local sales representative for additional information.

Example

The following command configures a back-up server with an IP address of *192.168.1.2*:

```
gtpp storage-server 192.168.1.2
```

gtpp storage-server local file

Configures the parameters for GTPP files stored locally on the GTPP storage server. This command is available for both ASR 5000 and 5500 platforms.

Product

GGSN

P-GW

SAEGW

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > **context** *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
gtpp storage-server local file { compression { gzip | none } | format {
custom1 | custom2 | custom3 | custom4 | custom5 | custom6 | custom7 |
custom8 } | name { format string [ max-file-seq-num seq_number ] | prefix
prefix } | purge-processed-files [ file-name-pattern file_pattern |
purge-interval purge_dur ] | push { encrypted-url url | url url } [
encrypted-secondary-url url | secondary-url url ] [ via-local-context ] |
rotation { cdr-count count | time-interval time [ force-file-rotation ] |
volume mb size } | start-file-seq-num seq_num [ recover-file-seq-num ]  }
default gtpp storage-server local file { compression | format | name {
format | prefix } | purge-processed-files | rotation { cdr-count |
time-interval | volume } | start-file-seq-num }
no gtpp storage-server local file { purge-processed-files | push | rotation
 { cdr-count | time-interval } }
```

default

Configures default setting for the specified parameter.

no

Removes a previously configured parameters for local storage of CDR files on HDD on SMC card.

compression { gzip | none }

Configures the type of compression to be used on the files stored locally.

- **gzip**: Enables Gzip file compression.
- **none**: Disables Gzip file compression -this is the default value.

Default: Disabled

format { *custom-n* }

Configures the file format to be used to format files to be stored locally.

custom1: File format custom1—this is the default value.

custom2: File format custom2.

custom3: File format custom3.

custom4: File format custom4.

custom5: File format custom5.

custom6: File format custom6 with a block size of 8K for CDR files.

custom7: File format custom7 is a customer specific CDR file format.

custom8: File format custom8 is a customer specific CDR file format. It uses *node-id-suffix_date_time_fixed-length-seq-num* format for file naming.

Default: **custom1**

name { format | prefix *prefix* }

Allows the format of the CDR filenames to be configured independently from the file format so that the name format contains the file name with conversion specifications.

prefix — Enter an alphanumeric string of 1 through 127 characters. The string ***must begin*** with the % (percent sign).

- **%y**: = year as a decimal number without century (range 00 to 99).
- **%Y**: year as a decimal number with century.
- **%m**: month as a decimal number (range 01 to 12).
- **%d**: day of the month as a decimal number (range 01 to 31).
- **%H**: hour as a decimal number 24-hour format (range 00 to 23).
- **%h**: hour as a decimal number 12-hour format (range 01 to 12).
- **%M**: minute as a decimal number (range 00 to 59).
- **%S**: second as a decimal number (range 00 to 60). (The range is up to 60 to allow occasional leap seconds.)
- **%Q**: File sequence number. Field width may be specified between the % and the Q. If the natural size of the field is smaller than this width, then the result string is padded (on the left) to the specified width with 0s

- **%N**: No of CDRs in the file. Field width may be specified between the % and the N. If the natural size of the field is smaller than this width, then the result string is padded (on the left) to the specified width with 0s
- **max-file-seq-no**: This can be configured optionally. It indicates the maximum value of sequence number in file name (starts from 1). Once the configured max-file-seq-no limit is reached, the sequence number will restart from 1. If no max-file-seq-no is specified then file sequence number ranges from 1 – 4294967295.

By default the above keyword is not configured (default gtpp storage-server local filename format). In which case the CDR filenames are generated based on the file format as before (maintains backward compatibility).

purge-processed-files [file-name-pattern *file_pattern* | purge-interval *purge_dur*]

Enables the GSN to periodically (every 4 minutes) delete locally processed (*.p) CDR files from the HDD on the SMC card. Default: Disabled

This keyword also deletes the processed push files (tx.*,under $CDR_PATH/TX/tx.*) a well when purging is enabled instead of "*.p:*.P".

Important This option is available only when GTPP server storage mode is configured for local storage of CDRs with the **gtpp storage-server mode local** command.

Optional keyword **file-name-pattern** *file_pattern* provides an option for user to control the pattern of files. *file_pattern* must be mentioned in "*.p:*.P:tx.*" format in a string of size 1 through 127, which is also the default format. Wildcards * and: (synonymous to |) are allowed.

Optional keyword **purge-interval** *purge_dur* provides an option for user to control the purge interval duration (in minutes). *purge_dur* must be an integer from 1 through 259200. Default value 60.

push { encrypted-url *encrypted_url* | url *url* } [encrypted-secondary-url *encrypted_url* | secondary-url *url*] [via-local-context]

Enables push method to transfer local CDR files to remote system.

encrypted-url: Defines use of an encrypted url.

encrypted_url must be an alphanumeric string of 1 through 8192 characters in SFTP format.

url: Location where the CDR files are to be transferred.

url must be an alphanumeric string of 1 through 1024 characters in the format:

scheme://user:password@host

encrypted-secondary-url: Defines use of an encrypted secondary url.

encrypted_url must be an alphanumeric string of 1 through 8192 characters in SFTP format.

secondary-url: Secondary location where the CDR files are to be transferred, in case primary is unreachable.

url must be an alphanumeric string of 1 through 1024 characters in the format:

scheme://user:password@host

Important When a file transfer to primary fails four times, the transfer of files will automatically be failed over to the secondary server. The transfer will switch back to the original primary after 30 minutes, or if there are four transfer failures to the secondary server.

via-local-context: Pushes the CDR files via SPIO in the local context.

Default: Pushes via the group's context.

Important If the push is done through gtpp context, then the push rate is lesser compared to via local context as the HDD is attached to the local context.

rotation { cdr-countcount | time-interval *time* | volume mb *size* }

Specifies rotation related configuration for GTPP files stored locally.

cdr-count *count*: Configures the CDR count for the file rotation as an integer from 1000 through 65000. Default value 10000.

time-interval *time*: Configures the time interval (in seconds) for file rotation as an integer from 30 through 86400. Default value 3600 (1 hour).

volume mb *size*: Configure the file volume (in MB) for file rotation. Enter an integer from 2 to 40. This trigger cannot be disabled. Default value is 4MB.

start-file-seq-num *seq_num* [recover-file-seq-num]

Specifies the start sequence number. The sequence number goes on incrementing until ULONG_MAX (or max-seq-num configured in file name format) and then it would rollover. If **recover-file-seq-num** is configured, every time the system is rebooted (or aaaproxy recovery/ planned/ unplanned packet service card migration), the file sequence number continues from the last sequence number and during rollover it starts from first-sequence number.

seq_num: Configures the sequence number. Enter an integer from 1 through 4294967295.

recover-file-seq-num: Configures the recovery of file sequence number. This is an optional field and if configured, every time the machine rebooted, the file sequence number continues from the last sequence number.

Usage Guidelines

This command configures the parameters for storage of GTPP packets as files on the local server—meaning the hard disk.

Example

The following command configures rotation for every 1.5 hours (5400 seconds) for locally stored files.

```
gtpp storage-server local file rotation time-interval 5400
start-file-seq-num 20 recover-file-seq-num
```

gtpp storage-server max-retries

Configures the maximum number of times the system attempts to communicate with an unresponsive GTPP back-up storage server.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

gtpp storage-server max-retries *max_attempts*
default gtpp storage-server max-retries

default

Configures this command with the default setting.

Default: 2

max_attempts

Specifies the number of times the system attempts to communicate with a GTPP back-up storage server that is not responding. *max_attempts* enter an integer from 1 through 15.

Usage Guidelines

This command works in conjunction with the **gtpp storage-server timeout** parameters to set a limit to the number of communication failures that can occur with a configured GTPP back-up storage server.

The **gtpp storage-server timeout** command controls the amount of time between re-tries.

Example

The following command configures the maximum number of re-tries to be *8*:

gtpp storage-server max-retries 8

gtpp storage-server mode

Configures storage mode, local or remote, for CDRs. Local storage mode is available with ASR 5000 platforms only.

Product

GGSN

P-GW

SAEGW

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

gtpp storage-server mode { local | remote | streaming }
default gtpp storage-server mode

default

Configures this command with the default setting.

Default: **remote**

local

Default: Disabled

Specifies the use of the hard disk on the SMC for storing CDRs

remote

Specifies the use of an external server for storing CDRs. This is the default value.

streaming

Default: Disabled

Allows the operator to configure "streaming" mode of operation for GTPP group. When this keyword is supplied the CDRs will be stored in following fashion:

- When GTPP link is active with CGF, CDRs are sent to a CGF via GTPP and local hard disk is NOT used as long as every record is acknowledged in time.
- If the GTPP connection is considered to be down, all streaming CDRs will be saved temporarily on the local hard disk and once the connection is restored, unacknowledged records will be retrieved from the hard disk and sent to the CGF.

Usage Guidelines

This command configures whether the CDRs should be stored on the hard disk of the SMC or remotely, on an external server.

Example

The following command configures use of a hard disk for storing CDRs:

gtpp storage-server mode local

gtpp storage-server timeout

Configures the amount of time that must pass with no response before the system re-attempts to communicate with the GTPP back-up storage server.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

gtpp storage-server timeout *duration*
default gtpp storage-server timeout

default

Configures this command with the default setting.

Default: 30 seconds

duration

Specifies the maximum amount of time (in seconds) the system waits for a response from the GTPP back-up storage server before assuming the packet is lost. *duration* is an integer from 30 through 120.

Usage Guidelines

This command works in conjunction with the **gtpp storage-server max-retries** command to establish a limit on the number of times that communication with a GTPP back-up storage server is attempted before a failure is logged. This parameter specifies the time between retries.

Example

The following command configures a retry timeout of *60* seconds:

```
gtpp storage-server timeout 60
```

gtpp suppress-cdrs zero-volume

This command suppresses the CDRs with zero byte data count. The CDRs can be classified as Final-cdrs, Internal-trigger-cdrs, and External-trigger-cdrs. This command allows the selection of CDRs to be suppressed and it is disabled by default.

Important Use of the Zero Volume CDR Suppression feature requires that a valid ECS license key be installed. Contact your Cisco account representative for information on how to obtain a license.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
gtpp suppress-cdrs zero-volume { external-trigger-cdr | final-cdr |
internal-trigger-cdr }
default gtpp suppress-cdrs zero-volume
no gtpp suppress-cdrs zero-volume
```

default

Configures this command with the default setting.

no

Disables suppression of the CDRs with zero byte data count.

Usage Guidelines

This command suppresses the CDRs with zero byte data count. This command provides an option to select the CDRs to be suppressed.

Example

To suppress only final zero volume CDRs use:

```
gtpp suppress-cdrs zero-volume final-cdr
```

To suppress final zero Volume CDRs and interim zero volume CDRs due to internal triggers use:

```
gtpp suppress-cdrs zero-volume final-cdr internal-trigger-cdr
```

To suppress final zero volume CDRs and interim zero volume CDRs due to internal and external triggers use:

```
gtpp suppress-cdrs zero-volume final-cdr internal-trigger-cdr
external-trigger-cdr
```

To suppress interim zero volume CDRs due to internal and external triggers use:

```
gtpp suppress-cdrs zero-volume internal-trigger-cdr external-trigger-cdr
```

To suppress interim zero volume CDRs due to external triggers use:

```
gtpp suppress-cdrs zero-volume external-trigger-cdr
```

gtpp suppress-cdrs zero-volume-and-duration

Suppresses the CDRs created by sessions having zero duration and/or zero volume. By default this mode is disabled.

Product

GGSN

P-GW

SAEGW

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

gtpp suppress-cdrs zero-volume-and-duration { gcdrs [egcdrs] | egcdrs [gcdrs] }
default gtpp suppress-cdrs zero-volume-and-duration

default

Configures this command with the default setting.

Default: Disabled.

gcdrs [egcdrs]

Suppresses G-CDRs before eG-CDRs.

egcdrs [gcdrs]

Suppresses eG-CDRs before G-CDRs.

Usage Guidelines

Use this command to suppress the CDRs (G-CDRs and eG-CDRs) which were created when zero-duration sessions and zero-volume sessions are encountered due to any reason. By default this command is disabled and system will not suppress any CDR.

Example

The following command configures the system to suppress the eG-CDRs created for a zero duration session or zero volume session:

gtpp suppress-cdrs zero-volume-and-duration egcdrs gcdrs

gtpp timeout

Configures the amount of time that must pass with no response before the system re-attempts to communicate with the Charging Gateway Function (CGF).

Product

GGSN

SGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

gtpp timeout *time*
default gtpp timeout

default

Configures this command with the default setting. Default: 20 seconds

time

Specifies the maximum amount of time (in seconds) the system waits for a response from the CGF before assuming the packet is lost. *time* is an integer from 1 through 60.

Usage Guidelines

This command works in conjunction with the **gtpp max-retries** command to establish a limit on the number of times that communication with a CGF is attempted before a failure is logged.

This parameter specifies the time between retries.

Example

The following command configures a retry timeout of *30* seconds:

```
gtpp timeout 30
```

gtpp trigger

This command is left in place for backward compatibility. To disable and enable GTPP triggers you should use the **gtpp trigger** command in GTPP Server Group Configuration Mode.

gtpp transport-layer

Selects the transport layer protocol for the Ga interface for communication between the access gateways (GSNs) and GTPP servers.

Product

GGSN

P-GW

SAEGW

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
gtpp transport-layer { tcp | udp }
default gtpp transport-layer
```

default

Configures this command with the default setting.

Default: **udp**

tcp

Default: Disabled

Enables the system to implement TCP as transport layer protocol for communication with GTPP server.

udp

Default: Enabled

Enables the system to implement UDP as transport layer protocol for communication with GTPP server.

Usage Guidelines

Use this command to select the TCP or UDP as the transport layer protocol for Ga interface communication between GTPP servers and AGWs (GSNs).

Example

The following command enables TCP as the transport layer protocol for the GSN's Ga interface.

```
gtpp transport-layer tcp
```

gtpu-service

Creates a GTP-U service or specifies an existing GTP-U service and enters the GTP-U Service Configuration Mode for the current context.

Product

GGSN

P-GW

SAEGW

S-GW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

gtpu-service *service_name* **[-noconfirm]**
no gtpu-service *service_name*

gtpu-service *service_name*

Specifies the name of the GTP-U service. If *service_name* does not refer to an existing service, a new service is created if resources allow. *service_name* is an alphanumeric string of 1 through 63 characters.

Important Service names must be unique across all contexts within a chassis.

-noconfirm

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

no gtpu-service *service_name*

Removes the specified GTP-U service from the context.

Usage Guidelines

Enter the GTP-U Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.

A maximum of 256 services (regardless of type) can be configured per system.

Caution Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following prompt:

```
[context_name]hostname(config-gtpu-service)#
```

GTP-U Service Configuration Mode commands are defined in the *GTP-U Service Configuration Mode Commands* chapter.

Example

The following command enters the existing GTP-U Service Configuration Mode (or creates it if it does not already exist) for the service named *gtpu-service1*:

gtpu-service gtpu-service1

The following command will remove *gtpu-service1* from the system:

no gtpu-service gtpu-service1

gtpu peer statistics threshold

Specifies the maximum number of GTP-U peers for which statistics will be maintained.

Product

P-GW

SAEGW

S-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Stats-Profile

configure > stats-profile >*stats_profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-stats-profile)#
```

Syntax Description

gtpu peer statistics threshold *value*

gtpu peer statistics threshold *value*

Specifies the number of GTP-U peers for which the node will maintain statistics.

Valid entries are from 16000 to 128000.

The default setting is 16000.

The threshold cannot be configured to a lower value than the current value. For example if the threshold value is set to 18000, it can no longer be set to any value below 18000.

Usage Guidelines

Use this command to specify the number of GTP-U peers for which the node will maintain statistics.

Example

The following command specifies that the node will maintain GTP-U peer statistics for 50000 GTP-U peers:

gtpu peer statistics threshold *50000*

ha-service

Creates/deletes a home agent service or specifies an existing HA service for which to enter the Home Agent Service Configuration Mode for the current context.

Product

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax Description

ha-service *name* **[-noconfirm]**
no ha-service *name*

no

Indicates the home agent service specified is to be removed.

name

Specifies the name of the HA service to configure. If *name* does not refer to an existing service, the new service is created if resources allow. *name* is an alphanumeric string of 1 through 63 characters.

Important Service names must be unique across all contexts within a chassis.

-noconfirm

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

Usage Guidelines

Enter the HA Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.

A maximum of 256 services (regardless of type) can be configured per system.

Caution Large numbers of services greatly increase the complexity of management and may impact overall system performance (i.e. resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Example

The following command will enter, or create and enter, the HA service *sampleService*:

```
ha-service sampleService
```

The following command will remove *sampleService* as being a defined HA service:

```
no ha-service sampleService
```

hexdump-module

Enter the Hexdump Service Configuration Mode to configure hexdump records creation and other related parameters.

Product

ePDG

SaMOG

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

hexdump-module
no hexdump-module

no

Disables creation of hexdump records.

Usage Guidelines

Enter the Hexdump Service Configuration Mode to configure hexdump records creation and other related parameters.

hnbgw-service

Important In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

Creates or removes an Home Node B Gateway (HNB-GW) service or configures an existing HNB-GW service and enters the HNB-GW Service Configuration Mode for Femto UMTS access networks configuration in the current context.

Product

HNB-GW

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

hnbgw-service *hnbgw_svc_name* **[-noconfirm]**
no hnbgw-service *hnbgw_svc_name*

no

Removes the specified HNB-GW service from the context.

hnbgw_svc_name

Specifies the name of the HNB-GW service. If *service_name* does not refer to an existing service, the new service is created if resources allow. *hnbgw_svc_name* is an alphanumeric string of 1 through 63 characters.

Important Service names must be unique across all contexts within a chassis.

-noconfirm

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

Usage Guidelines

Use this command to enter the HNB-GW Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.

A maximum of one HNB-GW service which is further limited to a maximum of 256 services (regardless of type) can be configured per system.

Caution Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following prompt:

```
[context_name]hostname(config-hnbgw-service)#
```

The commands available in this mode are defined in the *HNB-GW Service Configuration Mode Commands* chapter of *Command Line Interface Reference*.

Caution This is a critical configuration. The HNB-GW service can not be configured without this configuration. Any change to this configuration would lead to restarting the HNB-GW service and removing or disabling this configuration will stop the HNB-GW service.

Example

The following command enters the existing HNB-GW Service Configuration Mode (or creates it if it does not already exist) for the service named *hnb-service1*:

hnbgw-service hnb-service1

The following command will remove *hnb-service1* from the system:

no hnbgw-service hnb-service1

hsgw-service

Creates an HSGW service or specifies an existing HSGW service and enters the HSGW Service Configuration Mode for the current context.

Product HSGW

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

hsgw-service *service_name* **[-noconfirm]**
no hsgw-service *service_name*

no

Removes the specified HSGW service from the context.

service_name

Specifies the name of the HSGW service. If *service_name* does not refer to an existing service, the new service is created if resources allow. *service_name* is an alphanumeric string of 1 through 63 characters.

Important Service names must be unique across all contexts within a chassis.

-noconfirm

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

Usage Guidelines

Enter the HSGW Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.

A maximum of 256 services (regardless of type) can be configured per system.

Caution Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following prompt:

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

HSGW Service Configuration Mode commands are defined in the *HSGW Service Configuration Mode Commands* chapter.

Use this command when configuring the following eHRPD components: HSGW.

Example

The following command enters the existing HSGW Service Configuration Mode (or creates it if it does not already exist) for the service named *hsgw-service1*:

```
hsgw-service hsgw-service1
```

The following command will remove *hsgw-service1* from the system:

```
no hsgw-service hsgw-service1
```

hss-peer-service

Creates a Home Subscriber Service (HSS) peer service or configures an existing HSS peer service and enters the HSS Peer Service configuration mode.

Product

MME

SGSN

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

hss-peer-service *service_name* **[-noconfirm]**
no hss-peer-service *service_name*

no

Removes the specified HSS peer service from the context.

service_name

Specifies the name of the HSS peer service. If *service_name* does not refer to an existing service, a new service is created if resources allow. *service_name* is an alphanumeric string of 1 through 63 characters.

Important Service names must be unique across all contexts within a chassis.

-noconfirm

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

Usage Guidelines

Enter the HSS Peer Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.

The maximum number of HSS Peer Services that can be created and configured for the SGSN is 16.

The maximum number of HSS Peer Services that can be created and configured for the MME is 64.

Caution On a PSC2 setup, all diamproxy tasks might go in to a warning state if the number of hss-peer-services configured are more than 64 since the memory usage may exceed the allocated value.

Important In some cases, two diameter endpoints (S6a and S13) can be configured for a single HSS Peer Service. To ensure peak system performance, we recommend that the total of all Diameter endpoints should be taken into consideration and limited to 64 endpoints.

Caution A maximum of 256 services (regardless of type) can be configured per system. Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following prompt:

```
[context_name]hostname(config-hss-peer-service)#
```

HSS Peer Service Configuration Mode commands are defined in the *HSS Peer Service Configuration Mode Commands* chapter.

Example

The following command enters the existing HSS Peer Service Configuration Mode (or creates it if it does not already exist) for the service named *hss-peer1*:

hss-peer-service hss-peer1

The following command will remove *hss-peer1* from the system:

no hss-peer-service hss-peer1