VPC Commands

This chapter details commands that were introduced or changed on the VPC since StarOS Release 19.1.

access-type

This command is used to configure the NB-IoT RAT per TAI database.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration > LTE TAI Management Database Configuration

configure > lte-policy > tai-mgmt-db *db_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(tai-mgmt-db)#`

Syntax Description

```
[ no ] access-type nb-iot
```

no

Removes the configured access type for the TAI database.

nb-iot

Configures the access type as NB-IoT for a TAI database.

Usage Guidelines

The LTE TAI Management Database Configuration Mode is used to create and manage the LTE Tracking Area Identifier (TAI) management database on the system. Enter the TAI Management Database Configuration Mode for an existing or newly defined database. This command is also used to remove an existing database. Use this command to configure the access type of a TAC or group of TACs as NB-IoT RAT. As per 3GPP standards, the same TAC cannot belong to both EUTRAN and NB-IoT RATs. This command is not enabled by default. The default RAT is WB-EUTRAN.

Example

The following command is used to configure the access type as NB-IoT:

```
access-type nb-iot
```

access-type

This command is used to configure the NB-IoT RAT per TAI object.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration > LTE TAI Management Database Configuration > LTE TAI Management Object Configuration

configure > lte-policy > tai-mgmt-db *db_name* **> tai-mgmt-obj** *obj_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(tai-mgmt-obj)#`

Syntax Description

```
[ no ] access-type nb-iot
```

no

Removes the configured access type for the TAI object.

nb-iot

Configures the access type as NB-IoT for a TAI object.

Usage Guidelines

The LTE TAI Management Object Configuration Mode is used to create and manage the LTE Tracking Area Identifiers for the TAI database. This mode is used to create, remove or modify the existing LTE Tracking Area Identifier (TAI) object configurations. Use this command to configure the access type of a TAC or group of TACs as NB-IoT RAT. As per 3GPP standards, the same TAC cannot belong to both EUTRAN and NB-IoT RATs. This command is not enabled by default. The default RAT is WB-EUTRAN.

Example

The following command is used to configure the access type as NB-IoT:

```
access-type nb-iot
```

bfd

Configures Bidirectional Forwarding Detection (BFD) interface parameters.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration

configure > context *context_name* **> interface** *interface_name* **broadcast**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-eth)#
```

Syntax Description

```
[no] bfd { echo [echo-interval interval_num] | interval interval_num }
    min_rx milliseconds multiplier value
```

no

Disables the specified option on this interface.

echo

Enables BFD echo mode.

BFD echo mode works with asynchronous BFD. Echo packets are sent by the forwarding engine and forwarded back along the same path in order to perform detection—the BFD session at the other end does not participate in the actual forwarding of the echo packets. The echo function and the forwarding engine are responsible for the detection process, therefore the number of BFD control packets that are sent out between two BFD neighbors is reduced.

Since the forwarding engine is testing the forwarding path on the remote (neighbor) system without involving the remote system, there is an opportunity to improve the interpacket delay variance, thereby achieving quicker failure detection times than when using BFD Version 0 with BFD control packets for the BFD session.

echo-interval *interval_num*

Specifies the transmit interval between BFD echo packets. The default interval is 150 ms. The range is from 0 to 999 ms. (VPC only)

interval *interval_num*

Specifies the transmit interval (in milliseconds) between BFD packets.

- *For releases prior to 17.0*, *interval_num* is an integer from 50 through 999. (Default 50)
- *For release 17.0 onwards*, *interval_num* is an integer from 50 through 10000. (Default 50)

min_rx *milliseconds*

Specifies the receive interval in milliseconds for control packets.

- *For releases prior to 17.0*, *milliseconds* is an integer from 50 through 999. (Default 50)
- *For release 17.0 onwards*, *milliseconds* is an integer from 50 through 10000. (Default 50)

multiplier *value*

Specifies the value used to compute the hold-down time as a number from 3 to 50.

Usage Guidelines

Specify BFD parameters including echo mode and the transmit interval between BFD packets.

Example

To apply enable echo mode on this interface, use the following command:

```
bfd echo
```

The following command sets BFD interval parameters:

bfd interval 3000 min_rx 300 multiplier 3

ciot-optimisation

This command is used to configure Control Plane (CP) CIoT optimization for an UE.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]`*host_name*`(config-call-control-profile-`*profile_name*`)#`

Syntax Description

```
ciot-optimisation { cp-optimisation { access-type { all | nb-iot |
wb-eutran } |  ciot-capable-ue } | eps-attach-wo-pdn access-type { all |
 nb- iot | wb-eutran } }
remove ciot-optimisation cp-optimisation  ciot-capable-ue
remove ciot-optimisation eps-attach-wo-pdn access-type { all | nb-iot |
wb-eutran }
```

remove

The keyword remove deletes the existing configuration.

cp-optimisation

Use this keyword to enable Control Plane optimization for an UE.

access-type

Use this keyword to specify the access type extension on which control plane optimization should be enabled. Control plane optimization and EPS attach without PDN can be enabled on both NB-IoT and WB-EUTRAN RATs or on either of them.

ciot-capable-ue

Uses only the ue-nw-capability to determine whether CP optimization or not.

all

Use this keyword to enable control plane optimization on both RAT types WB-EUTRAN and NB-IOT. This keyword is provided to the operator for the ease of configuring. Both NB-IoT and WB-EUTRAN will be considered as two independent access types for all functions.

nb-iot

Use this keyword to enable control plane optimization on the RAT type NB-IoT.

wb-eutran

Use this keyword to enable control plane optimization on the RAT type WB-EUTRAN.

eps-attach-wo-pdn

Use this keyword to enable EPS attach without PDN support for an UE.

Usage Guidelines

Use this command to configure the control plane optimization on the RAT type and to configure EPS attach without PDN support for UE. This command is not enabled by default. The call-control-profile can be associated with the operator-policy or with IME-TAC group, therefore it is possible to either enable or disable CIoT optimization on a per subscriber (IMSI) basis or on a group of subscribers or on per group of IMEI basis. CIoT optimization can be enabled on both NB-IoT and WB-EUTRAN RATs or on either of them. Enabling one RAT type does not disable the other RAT type.

Example

Use the following command to configure control plane optimization by specifying the access type as NB-IoT:

```
ciot-optimisation cp-optimisation access-type nb-iot
```

Use the following command to configure EPS attach without PDN support for UE, specify the access type as WB-EUTRAN:

```
ciot-optimisation eps-attach-wo-pdn access-type wb-eutran
```

debug bfd

Enables or disables the debug options for Bidirectional Forwarding Detection BFD) debugging. If logging is enabled, results are sent to the logging system.

Product

All

Privilege

Security Administrator, Administrator, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

```
[ no ] debug bfd [all | events ipc-error | ipc-events | nsm | packet |
session]
    [level-1 | level-2 | level-3]
```

no

Indicates the IP debugging is to be disabled for the IP interfaces/function specified.

bfd *name*

Specifies which IP interfaces/function to debug.

all: enables debug for all BFD items.

events: enables debug for BFD events.

ipc-error: enables debug for BFD Inter-process communication (IPC) errors.

ipc-events: enables debug for BFD Inter-process communication (IPC) events.

nsm: enables debug for BFD Network Service Manager messages.

packet: enables debug for BFD packets.

session: enables debug for BFD sessions.

level-1 | level-2 | level-3

Optionally specifies the amount of information provided by the debug command:

- Level-1 debugging shows errors, warnings, and some critical one time events. Level-1 is the default.
- Level-2 debugging shows errors, warnings, and all events.
- Level-3 debugging shows errors, warnings, all events and is much more verbose.

Usage Guidelines

The **debug** command is valuable when troubleshooting network problems with BFD-enabled BGP routers. The debugging is stopped by using the **no** keyword.

Caution Issuing this command could negatively impact system performance depending on system configuration and/or loading.

Example

The following commands enable/disable debugging for BFD.

```
debug bfd
no debug bfd
```

delay-tolerant-pdn

Configures Delay Tolerant behavior for PDN connection to support UE in Power Saving Mode.

Product

P-GW

S-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > APN Configuration

configure > context *context_name* **> apn** *apn_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
delay-tolerant-pdn max-control-signal-buffer  1-4
no delay-tolerant-pdn
```

no

Removes and restores the configuration to its default value.

max-control-signal-buffer *1-4*

Configures maximum number of P-GW initiated control signaling messages to be buffered (range 1 to 4) when the UE is in Power Saving Mode (PSM).

Usage Guidelines

When the CLI is configured, it indicates that the PDN supports delay tolerant behavior. Also, the number of control signals that can be buffered is indicated by **max-control-signal-buffer**. When a new Rule is sent to update/create bearer, the number of transactions that will be buffered gets restricted to 4.

By default, the command is disabled and eDRX support is not applicable.

This CLI command takes effect during new call set-up or during handoff procedure to S5/S8 interface.

Example

The following command configures *3* P-GW initiated control signaling messages to be buffered when UE is in Power Saving mode.

```
delay-tolerant-pdn max-control-signal-buffer  3
```

diameter

This command configures the diameter interface for an SCEF service.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > SCEF Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax

```
diameter { dictionary standard | endpoint endpoint_name }
[ no ] diameter endpoint
[ default ] diameter dictionary
```

no

The prefix no disables the configuration.

default

The prefix default assigns or restores the default vale for the selected parameters.

endpoint *endpoint_value*

This command configures the diameter endpoint.

endpoint_name must be for the Diameter server expressed as an alphanumeric string of 1 through 63 characters.

dictionary standard

This command configures the dictionary to be used for the interface. The above configuration can be used to configure the transfer of Non-IP data over SCEF at the T6a diameter interface

Usage Guidelines

Use this command to configure the diameter interface. The above mentioned commands can be used to configure the transfer of Non-IP data over SCEF at the T6a diameter interface.

A diameter endpoint name must be specified. It is not recommended to remove the diameter endpoint when there are active calls on the system. Hence, please adhere to the 'Method of Procedure' to remove the endpoint. Otherwise, the system behavior would be undefined.

Example

The following command configures the diameter with an endpoint t6a-endpoint:

```
diameter endpoint t6a-endpoint
```

Example

The following command configures the diameter standard dictionary:

```
diameter dictionary standard
```

edrx

This command enables Extended Discontinuous Reception (eDRX) and configures its respective parameters, on the MME.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax

```
edrx { ptw ptw_value edrx-cycle cycle_length_value | ue-requested } [
dl-buf-duration [ packet-count packet_count_value ] ]
remove edrx
```

remove

The keyword **remove**disables the eDRX configuration on the MME.

ptw *ptw_value*

This keyword is used to configure the PTW value.

In releases prior to 21.2: The *ptw_value* is an integer ranging from "0" up to "20".

In 21.2 and later releases: The *ptw_value* is an integer ranging from "0" up to "15".

ue-requested

The keyword **ue-requested**specifies the UE requested values of the Paging Time Window (PTW) and the eDRX cycle length received from the UE in the Attach Request/TAU Request message be accepted.

edrx-cycle *cycle_length_value*

The keyword **edrx-cycle**is used to configure the eDRX cycle length. The *cycle_length_value* is an integer value from " 512" up to "262144". It is a multiple of 2 starting from 512 up to 262144 (for example: 512, 1024, 2048, and so on).

dl-buf-duration

The keyword **dl-buf-duration** is used to send downlink buffer duration in DDN ACK when unable to page UE.

packet-count*packet_count_value*

The keyword **packet-count** is used to send 'DL Buffering Suggested Packet Count' in DDN ACK when unable to page UE. The *packet_count_value* is an integer value from "0" up to "65535". If the *packet_count_value* is not configured locally, the subscription provided value for the *packet_count_value* is used. The subscription value can be "0" in which case packet count IE will not be sent for that subscriber even if it is configured locally.

Usage Guidelines

Use this command to enable eDRX on the MME. This command is configured as part of the eDRX feature for MME - it allows UEs to connect to the network on a need basis. With eDRX, a device can remain inactive or in sleep mode for minutes, hours or even days based on the H-SFN synchronization time (UTC Time). The H-SFN synchronization time for eDRX is configured at an MME-Service level. See *MME Service Configuration*

Mode Commands chapter for configuration information on H-SFN synchronization. This command is not enabled by default.

Example

The following command is used to configure the PTW and eDRX cycle length. The command is also used to send the downlink buffer duration in the DDN ACK along with a suggested packet count:

edrx ptw 10 edrx-cycle 512 dl-buf-duration packet-count 10

gtpc

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

Product

ePDG

MME

P-GW

S-GW

SAEGW

SaMOG

SGSN

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > eGTP Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

gtpc { allow-on-congestion { apn-name *apn_name* **| arp** *priority_level* **} | bind { ipv4-address** *ipv4_address* **[ipv6-address** *ipv6_address* **] | ipv6-address** *ipv6_address* **[ipv4-address** *ipv4_address* **] } | command-messages { dual-ip-stack-support } | disable cause-source | echo-interval** *seconds* **[dynamic [smooth-factor** *multiplier* **]] echo-max-retransmissoins** *number* **| echo-retransmission-timeout** *seconds* **| error-response-handling | peer-salvation | ip qos-dscp {** *forwarding_type* **| max-remote-restart-counter-change** *integer* **} | max-retransmissions** *num* **| node-feature { cellular-iot network-triggered-service-restoration | pgw-restart-notification } | path-failure detection-policy { echo | control-restart-counter-change | echo-restart-counter-change } | private-extension overcharge-protection | reject s2b-ho-no-context | retransmission-timeout** *seconds* **| retransmission-timeout-ms** *milliseconds* **}**
no gtpc { allow-on-congestion { apn-name *apn_name* **| arp** *priority_level* **} | bind { ipv4-address** *ipv4_address* [ipv6-address *ipv6_address* **] | ipv6-address** *ipv6_address* **[ipv4-address** *ipv4_address***] } | command-messages { dual-ip-stack-support } | disable cause-source | echo-interval |**

```
error-response-handling | node-feature {
cellular-iotnetwork-triggered-service-restoration |
pgw-restart-notification } | path-failure detection-policy |
private-extension overcharge-protection | reject s2b-ho-no-context }
default gtpc  disable cause-source |{ echo-interval |
echo-max-retransmissons | echo-retransmission-timeout disable cause-source|
 ip qos-dscp | max-retransmissions | node-feature { cellular-iot
network-triggered-service-restoration | pgw-restart-notification } |
path-failure detection-policy | retransmission-timeout |
retransmission-timeout-ms }
```

no

Disables or removes the configured GTP-C setting.

default

Resets the specified parameter to its default value.

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

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

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

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

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

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

Important There is no APN-to-ARP mapping.

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

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

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

ipv4_address must be entered using IPv4 dotted-decimal notation.

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

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

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

ipv4_address must be entered using IPv4 dotted-decimal notation.

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

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

cellular-iot

Enables the Cellular IoT features supported for eGTP Service.

command-messages dual-ip-stack-support

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

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

disable cause-source

disable: Disables functionality at eGTPC level.

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

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

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

Default: 60

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

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

Default: 2

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

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

Valid settings are from 1 to 255.

The recommended setting is 32.

The default setting is 255.

echo-max-retransmissions *number*

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

Default: 4

echo-retransmission-timeout *seconds*

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

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

Default: 3

error-response-handling

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

peer-salvation

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

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

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

Note

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

ip qos-dscp { ***forwarding_type*** **}**

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

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

The following forwarding types are supported:

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

  This is the default setting.

- **af12**: Designates the use of Assured Forwarding 12 PHB.
- **af13**: Designates the use of Assured Forwarding 13 PHB.
- **af21**: Designates the use of Assured Forwarding 21 PHB.
- **af22**: Designates the use of Assured Forwarding 22 PHB.
- **af23**: Designates the use of Assured Forwarding 23 PHB.
- **af31**: Designates the use of Assured Forwarding 31 PHB.
- **af32**: Designates the use of Assured Forwarding 32 PHB.
- **af33**: Designates the use of Assured Forwarding 33 PHB.
- **af41**: Designates the use of Assured Forwarding 41 PHB.
- **af42**: Designates the use of Assured Forwarding 42 PHB.
- **af43**: Designates the use of Assured Forwarding 43 PHB.
- **be**: Designates the use of Best Effort forwarding PHB.
- **cs1**: Designates the use of Class Selector code point "CS1".
- **cs2**: Designates the use of Class Selector code point "CS2".
- **cs3**: Designates the use of Class Selector code point "CS3".
- **cs4**: Designates the use of Class Selector code point "CS4".
- **cs5**: Designates the use of Class Selector code point "CS5".
- **cs6**: Designates the use of Class Selector code point "CS6".
- **cs7**: Designates the use of Class Selector code point "CS7".
- **ef**: Designates the use of Expedited Forwarding PHB typically dedicated to low-loss, low-latency traffic.

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

	Class 1	Class 2	Class 3	Class 4
Low Drop	AF11	AF21	AF31	AF41

	Class 1	Class 2	Class 3	Class 4
Medium Drop	AF12	AF22	AF32	AF42
High Drop	AF13	AF23	AF33	AF43

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

max-retransmissions *num*

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

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

Default: 4

node-feature pgw-restart-notification

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

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

Default: Disabled

node-feature network-triggered-service-restoration

This keyword applies to MME and S-GW only.

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

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

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

path-failure detection-policy echo

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

Default: Enabled

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

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

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

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

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

private-extension overcharge-protection

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

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

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

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

reject s2b-ho-no-context

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

retransmission-timeout *seconds*

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

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

Default: 5

retransmission-timeout-ms *milliseconds*

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

Default: 5000

Usage Guidelines

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

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

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

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

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

Example

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

gtpc bind ipv4-address 112.104.215.177

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 attribute

Enables the specification of some of the optional fields in the CDRs that the GSN (GGSN or SGSN) generates and/or how the information is to be presented. Many keywords are also applicable to S-GW and P-GW CDRs.

Product

GGSN

P-GW

SAEGW

SaMOG

SGSN

S-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > GTPP Server Group Configuration

configure > context *context_name* **> gtpp group** *group_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-gtpp-group)#`

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 | extended-bitrate | 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 packet-count | pco-nai | 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 | ue-tun-ip-port | uwanuli | 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 | uwanuli
 | 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 | extended-bitrate | 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* **packet-count | pco-nai | 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 | ue-tun-ip-port | uwanuli | uli | user-csg-information } +**

default

Resets the default attribute values for this GTPP group configuration.

no

Disables the specified optional field so that the information will not be present in generated 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.

extended-bitrate

Default: Disabled

This keyword controls the inclusion of extended bit-rate information in P-GW CDRs when the APN-AMBR, MBR, or GBR is greater than 4.2 Gbps.

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.

VPC Commands

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

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

last-uli

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 *nddd**STRING*** 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.

packet-count

Default: Disabled

Specifying this option includes the optional field "datapacketFBCUplink" and "datapacketFBCDownlink" in the CDR.

Important This keyword is applicable to custom24 GTPP dictionary.

pco-nai

Specifying this option includes optional field "PCO- Network Access Identifier" in the P-GW CDR.

Important This keyword is applicable to custom44 GTPP dictionary.

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.

ue-tun-ip-port

Default: Disabled

In 21.9.5 and later releases, this keyword is introduced for P-GW to include new parameter in CDR generated for S2b (VoWifi) call/subscriber.

Important This keyword is applicable to custom24 GTPP dictionary.

uwanuli

Default: Disabled

This keyword controls the inclusion of the optional field "UWAN 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

This command dictates some of the optional information fields that should be reported in CDRs generated by the GGSN. 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).

Example

The following command disables the inclusion of the field "SGSN Change" in the S-CDR:

```
no gtpp attribute sgsn-change
```

Example

The following command dictates that the time provided in the Duration field of the CDR is reported in milliseconds:

```
gtpp attribute duration-ms
```

gtpp trigger

Disables GTPP trigger conditions that cause either partial CDR record closure or opening of a new CDR record container. GTPP Triggers are specified in 3GPP TS 32.251 v6.6.0. All GTPP trigger changes take effect immediately, except **volume-limit**.

Product

ECS

GGSN

P-GW

SAEGW

SGSN

S-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > GTPP Server Group Configuration

configure > context *context_name* **> gtpp group** *group_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-gtpp-group)#`

Syntax Description

```
gtpp trigger { apn-ambr-change | [ default-bearer-only |
all-non-gbr-bearers | all-bearers ] | cell-update |  ciot-userplane-change|
 dcca | direct-tunnel | egcdr max-losdv | ggsn-preservation-mode-change
| inter-plmn-sgsn-change | ms-timezone-change | plmn-id-change | qos-change
 | rat-change [ generate { cdr | container } ] | routing-area-update |
service-idle-out | serving-node-change-limit | sgsn-change-limit |
tariff-time-change | time-limit | uli-change | volume-limit }
default gtpp trigger
no gtpp trigger { apn-ambr-change | [ default-bearer-only |
all-non-gbr-bearers | all-bearers ] | cell-update |  ciot-userplane-change|
 dcca | direct-tunnel | egcdr max-losdv | ggsn-preservation-mode-change
| inter-plmn-sgsn-change | ms-timezone-change | plmn-id-change | qos-change
 | rat-change [ generate { cdr | container } ] | routing-area-update |
service-idle-out | serving-node-change-limit | sgsn-change-limit |
tariff-time-change | time-limit | uli-change | volume-limit }
```

default

Sets the specified trigger condition back to the default setting. All trigger conditions are enabled by default.

no

Disables the specified trigger condition.

apn-ambr-change [default-bearer-only | all-non-gbr-bearers | all-bearers]

Default: Disabled

Enables APN AMBR trigger only for default-bearer or for all bearers for that PDN or selectively for apn-non-gbr bearers.

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.

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

- **default-bearer-only**: Adds container only to default bearer.
- **all-non-gbr-bearers**: Adds container to all non-gbr-bearers.
- **all-bearers**: Adds containers for all bearers.

Important This CLI command and the associated options are not available for products other than S-GW and P-GW.

The first container of each CDR includes apn-ambr fields along with QoS. In the following containers this field is present if previous change condition is "QoS change" or "APN AMBR Change".

cell-update

Enables the cell update trigger for S-CDRs, if the dictionary specified in the **gtpp dictionary** configuration includes support for cell update. This trigger is available only for 2G. Currently, custom18 dictionary supports the cell update trigger.

ciot-userplane-change

Enables User Plane change trigger for CDR.

dcca

This keyword enables or disables the addition of LOSDV in PGW-CDR for the following DCCA generated triggers.

- Time Threshold Reached
- Volume Threshold Reached
- Service Specific Unit Threshold Reached
- Time Exhausted
- Volume Exhausted
- Validity Timeout
- Reauthorization Request
- Continue Ongoing Session

- Retry And Terminate Ongoing Session
- Terminate Ongoing Session
- Service Specific Unit Exhausted
- Envelope Closure

direct-tunnel

Enables the direct tunnel trigger for CDRs.

egcdr max-losdv

Enables the trigger for an eG-CDR/P-CDR if the List of Service Data Volume (LoSDV) containers crosses the configured limit for LOSDV containers. Default: Disabled

ggsn-preservation-mode-change

This keyword is for GGSN only.

This trigger enables the preservation-mode-change trigger for G-CDR.

inter-plmn-sgsn-change

This keyword is for GGSN only.

Disabling this trigger ignores an Inter-PLMN SGSN change and doesn't release a G-CDR. Default: Enabled

ms-timezone-change

This keyword is specific to GGSN.

No partial record closure for a time zone change occurs when this trigger is disabled. MS time zone change should be applicable only for 3GPP R6 based GTPP dictionaries. Default: Enabled

plmn-id-change

This trigger keyword is specific to the 2G SGSN and is proprietary (non-standard).

Enables the PLMNID change trigger for S-CDRs if the dictionary specified in the **gtpp dictionary** configuration supports the PLMNID change. If enabled, the SGSN generates a partial S-CDR when the MS changes the PLMN while under the same SGSN (intra-system intra-SGSN PLMN-ID handover). Currently, custom18 dictionary supports this trigger. Default: Disabled

qos-change

Enables the QoS-change trigger for CDRs. Disabling this trigger ignores a QoS-change and does not open a new CDR for it. Default: Enabled

When QoS changes are observed, the system generates only containers. However when the max-container condition is reached, an interim CDR is generated.

rat-change [generate { cdr | container }]

Enables or disables the partial record closure for a RAT change. If disabled, no partial record closure for a RAT change occurs. RAT change should be applicable only for 3GPP R6 based GTPP dictionaries. Default: Enabled

In SGSN, RAT change trigger (2G<->3G) means inter-service handoff (SGSN service <-> GPRS service). If this trigger is enabled, after the RAT change interim CDR is generated. After this RAT change CDR, CDR thresholds such as volume/time etc. and GTPP Group are applicable from new service. If RAT change trigger is disabled, the CDR thresholds and GTPP group etc. will not change and will continue to use from old service.

After the RAT change, the System Type field in CDR changes to indicate the new system type. If this trigger is disabled, then the next CDR generated will indicate System Type, but the data count in the CDR does not necessarily belong to the system type indicated in CDR; instead, it may belong to both 2G and 3G as CDR is not closing when handover takes place.

Important The System Type field in CDR-related change is not applicable to customized CDR formats, which does not use the System Type field.

generate { cdr | container }: Sets generation of CDR or just a Container on a RAT change.

cdr: Generates a CDR on a RAT-change.

container: Generates a container only on a RAT-change.

routing-area-update

Enables the routing-area-update trigger for CDRs.

service-idle-out

This keyword enables or disables the addition of LOSDV in PGW-CDR when a service idles out.

Note that the CDR module receives service idle out trigger from DCCA module when the quota hold timer expires, or from ACS manager when rulebase has a service idle out configuration.

serving-node-change-limit [also-intra-sgsn-multiple-address-group-change]

This keyword is enabled for P-GW, S-GW, and GGSN. However, the **also-intra-sgsn-multiple-address-group-change** is enabled only for GGSN. Default: Enabled

Disabling this trigger ignores an SGSN change and does not add the SGSN IP address into the SGSN address list of the CDR. This helps to reduce the release of CDRs due to SGSN changes crossing the configured limit.

also-intra-sgsn-multiple-address-group-change: This keyword includes Intra-SGSN group changes as an SGSN change.

sgsn-change-limit [also-intra-sgsn-multiple-address-group-change]

This keyword is obsolete and is available to maintain the backward compatibility for existing customers. The new keyword for **sgsn-change-limit** is **serving-node-change-limit**. Default: Enabled

Disabling this trigger ignores an SGSN change and does not add the SGSN IP address into the SGSN address list of the CDR. This helps to reduce the release of CDRs due to SGSN changes crossing the configured limit.

also-intra-sgsn-multiple-address-group-change: This keyword includes Intra-SGSN group changes as an SGSN change.

tariff-time-change

When this trigger is disabled, container closure does not happen for a tariff-time change. Default: Enabled

This trigger is applicable for G-MB-CDRs for MBMS session too.

time-limit

When this trigger is disabled, no partial record closure occurs when the configured time limit is reached. Default: Enabled

This trigger is applicable for G-MB-CDRs for MBMS session too.

uli-change

Enables the user location update trigger for eG-CDRs/PGW-CDRs/SGW-CDRs, if the dictionary specified in the GTPP dictionary configuration includes support for user location update trigger. Default: Enabled

volume-limit

When this trigger is disabled no partial record closure occurs when volume limit is reached. Default: Enabled

This trigger is applicable for G-MB-CDRs for MBMS session too.

Usage Guidelines

Use this command to disable or enable GTTP triggers that can cause partial CDR record closure or cause a new CDR to be created.

Example

The following command disables partial record closure when a configured time limit is reached:

```
gtpp trigger time-limit
```

The following command re-enables partial record closure when a configured time limit is reached:

```
no gtpp trigger time-limit
```

gtpu-error-ind

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

Product

S-GW

SAEGW

Privilege

Administrator

Command Modes

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

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

default

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

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

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

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

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

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

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

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

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

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

Usage Guidelines

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

Example

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

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

ie-override

This command is used to override the RAT type AVP value with the configured value for messages sent from MME to HSS.

Important

This command ensures backward compatibility with previous releases as the HSS does not support the new NB-IoT RAT type.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

```
[ remove ] ie-override s6a rat-type wb-eutran
```

remove

The keyword remove deletes the existing configuration.

ie-override

This keyword allows the operator to configure IE override in messages sent from MME to HSS.

s6a

This keyword is used to specify the interface as s6a. The s6a interface used by the MME to communicate with the Home Subscriber Server (HSS).

rat-type

Use this keyword to configure the supported RAT type AVP IE.

wb-eutran

Use this keyword to specify the WB-EUTRAN AVP Value.

Usage Guidelines

Use this command to override the RAT type AVP value with the configured value for messages sent from MME to HSS over the s6a interface. If the configured RAT type is NB-IoT, it is changed to wb-eutran for messages sent from the MME to HSS. This command is not enabled by default.

Example

The following command is used to enable override of the RAT type AVP value with the configured value of WB-EUTRAN:

ie-override s6a rat-type wb-eutran

iftask mcdmatxbatch

Configures multi-channel direct memory access (MCDMA) transmit batching. The MCDMA is the path from the IFTASK to the SESSMGR. This command applies only to StarOS on virtualized platforms.

Product

All

Privilege

Operator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

[no] iftask mcdmatxbatch { burstsize *number_of_packets* **| latency** *milliseconds* **}**

no

Deletes the setting for iftask mcdmatxbatch.

burstsize *number_of_packets*

Maximum packets per burst from 1 through 1024.

latency *milliseconds*

Not currently supported.

Usage Guidelines

The following example sets the maximum number of packets per burst for MCDMA to 512:

iftask mcdmatxbatch burstsize 512

iftask txbatch

Configures transmit batching. This command applies only to StarOS on virtualized platforms.

Product

All

Privilege

Operator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

`[local]host_name(config)#`

Syntax Description

[no] iftask txbatch { burstsize *number_of_packets* **| flush_latency | latency** *milliseconds* **}**

no

Deletes the setting for iftask txbatch.

burstsize *number_of_packets*

Specifies the maximum number of packets from 1 through 1024 to accumulate in a vector before sending to the ethernet interface.

latency *milliseconds*

Not currently supported.

Usage Guidelines

Use this command to configure the transmit batching parameters for system-wide IFTASK operation.

The following example sets the maximum number of packets per burst for MCDMA to *512*:

iftask txbatch burstsize 512

The following example sets the maximum wait time to *1000* milliseconds to flush the bytes on the control port:

iftask txbatch flush_latency 1000

ip name-servers

Modifies the list of domain name servers the current context may use for logical host name resolution.

Product

All

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

ip name-servers *ip_address secondary_ip_address* [*third_ip_address*]
no ip name-servers *ip_address*

no

Indicates the name server specified is to be removed from the list of name servers for the current context.

ip_address

Specifies the IP address of a domain name server using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

secondary_ip_address

Specifies the IP address of a secondary domain name server using either IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

third_ip_address

Specifies the IP address of a third domain name server using either IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation. (VPC only)

Usage Guidelines

Manage the list of name servers the current context may use in resolving logical host names.

The DNS can be specified at the Context level in Context configuration as well as at the APN level in APN Configuration Mode with **dns** and **ipv6 dns** commands, or it can be received from AAA server.

When DNS is requested in PCO configuration, the following preference will be followed for DNS value:

1. DNS Values received from LNS have the first preference.
2. DNS values received from RADIUS Server has the second preference.
3. DNS values locally configured with APN with **dns** and **ipv6 dns** commands has the third preference.
4. DNS values configured at context level has the last preference.

Important The same preference would be applicable for the NBNS servers to be negotiated via ICPC with the LNS.

Example

```
ip name-servers 10.2.3.4
```

ip qos-dscp

Defines the IP parameters for this APN profile.

Product

MME

SGSN

S-GW

SAEGW

Privilege

Administrator

Command Modes

Exec > Global Configuration > APN Profile Configuration

configure > apn-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(apn-profile-profile_name)#`

Syntax Description

```
ip { qos-dscp {  { { downlink | uplink } { backgroundforwarding |
conversational forwarding | interactive traffic-handling-priority priority
forwarding | streaming forwarding } + } s11u-mme  value }  | source-violation
 { deactivate [ all-pdp | exclude-from accounting | linked-pdp |
tolerance-limit } | discard [ exclude-from-accounting ] | ignore }
default ip { qos-dscp [ downlink | uplink | s11u-mme ] | source-violation
 }
no ip qos-dscp { downlink | uplink } { background | conversational |
interactive | streaming } +
```

Important

All parameters not specifically configured will be included in the configuration with default values.

default

Resets the configuration to the default values.

no

Disables the specified IP QoS-DSCP mapping.

qos-dscp

Configures the Differentiated Services Code Point (DCSP) marking to be used for sending packets of a particular 3GPP QoS class.

downlink | uplink

Configures the packets for either downlink (network to subscriber) or uplink (subscriber to network) direction. **downlink** and **uplink** configuration must include one or more of the following:

- **background** - Configures the DSCP marking to be used for packets of sessions subscribed to 3GPP background class. Must be followed by a DSCP marking
- **conversational** - Configures the DSCP marking to be used for packets of sessions subscribed to 3GPP conversational class. Must be followed by a DSCP marking
- **interactive** - Configures the DSCP marking to be used for packets of sessions subscribed to different traffic priorities in the 3GPP interactive class. Must be followed by a traffic handling priority (THP): 1, 2, or 3.
- **streaming** - Configures the DSCP marking to be used for packets of sessions subscribed to 3GPP streaming class. Must be followed by a DSCP marking

DSCP marking options

Downlink and uplink must include a DSCP forwarding marking; supported options include:

- af11 - Designates use of Assured Forwarding 11 PHB
- af12 - Designates use of Assured Forwarding 12 PHB
- af13 - Designates use of Assured Forwarding 13 PHB
- af21 - Designates use of Assured Forwarding 21 PHB
- af22 - Designates use of Assured Forwarding 22 PHB
- af23 - Designates use of Assured Forwarding 23 PHB
- af31 - Designates use of Assured Forwarding 31 PHB
- af32 - Designates use of Assured Forwarding 32 PHB
- af33 - Designates use of Assured Forwarding 33 PHB
- af41 - Designates use of Assured Forwarding 41 PHB
- af42 - Designates use of Assured Forwarding 42 PHB
- af43 - Designates use of Assured Forwarding 43 PHB
- be - Designates use of Best Effort forwarding PHB
- ef - Designates use of Expedited Forwarding PHB

Forwarding defaults for both uplink and downlink are:

- conversational - ef;
- streaming - af11;
- interactive 1 - ef;
- interactive 2 - af21;
- interactive 3 - af21;
- background - be

s11u-mme *value*

This keyword is used to configure the S11-U interface parameters. The DSCP values can be specified using this keyword. The DSCP value for S11-U interface can be separately specified for each APN. This keyword is enabled by default. The default value is “be”. Listed below are DSCP values which can be configured for the S11U interface:

- af11 - Designates use of Assured Forwarding 11 PHB
- af12 - Designates use of Assured Forwarding 12 PHB
- af13 - Designates use of Assured Forwarding 13 PHB
- af21 - Designates use of Assured Forwarding 21 PHB
- af22 - Designates use of Assured Forwarding 22 PHB
- af23 - Designates use of Assured Forwarding 23 PHB
- af31 - Designates use of Assured Forwarding 31 PHB
- af32 - Designates use of Assured Forwarding 32 PHB
- af33 - Designates use of Assured Forwarding 33 PHB

- af41 - Designates use of Assured Forwarding 41 PHB
- af42 - Designates use of Assured Forwarding 42 PHB
- af43 - Designates use of Assured Forwarding 43 PHB
- be - Designates use of Best Effort forwarding PHB
- cs0 - Designates use of Class Selector 0 PHB
- cs1 - Designates use of Class Selector 1 PHB
- cs2 - Designates use of Class Selector 2 PHB
- cs3 - Designates use of Class Selector 3 PHB
- cs4 - Designates use of Class Selector 4 PHB
- cs5 - Designates use of Class Selector 5 PHB
- cs6 - Designates use of Class Selector 6 PHB
- cs7 - Designates use of Class Selector 7 PHB
- ef - Designates use of Expedited Forwarding PHB

source-violation

Configures settings related to IP source-violation detection with one of the following criteria:

- **deactivate** - deactivate the PDP context with one of the following conditions:
  - **all-pdp** - deactivates all PDP context of the MS/UE. Default is to deactivate errant PDP contexts.
  - **exclude-from-accounting** - excludes packets having an invalid source IP address from the statistics used in the accounting records.
  - **linked-pdp** - deactivate all associated pdp contexts (primary and secondary). Default is to deactivate errant pdp context.
  - **tolerance-limit** - Configures maximum number of allowed IP source violations before the session is deactivated.
- **discard** - discard errant packets, can include the following option:
  - **exclude-from-accounting** - excludes packets having an invalid source IP address from the statistics used in the accounting records.
- **ignore** - ignore checking of packets for MS/UE IP source violation.

Usage Guidelines

This command configures a range of IP functions to be associated with the APN profile; such as:

- SGSN/S-GW action in response to detected IP source violations,
- DSCP marking for downlink and uplink configuration per traffic class,
- QoS class diffserv code.

- Configures the S11U interface parameters.

Example

The following command configures the APN profile to instruct the SGSN or S-GW not to check incoming packets for IP source violation information:

ip source-violation ignore

The following command configures the S11-U interface parameters and specifies the DSCP marking value as “ef”:

ip qos-dscp s11u-mme ef

nb-iot

This command enables Extended Discontinuous Reception (eDRX) and configures the respective parameters for NB-IoT subscribers on the MME.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

[local]*host_name*(config-call-control-profile-*profile_name*)#

Syntax Description

nb-iot edrx { ptw *ptw_value* **edrx-cycle** *cycle_length_value* **| ue-requested } [dl-buf-duration [packet-count** *packet_count_value* **]]**
remove nb-iot edrx

remove

This keyword disables the eDRX configuration on the MME for NB-IoT subscribers.

edrx

This keyword configures extended discontinuous reception parameters.

ptw *ptw_value*

This keyword configures the Paging Time Window (PTW) value. *ptw_value* must be an integer value in seconds. The allowed values are 2.56, 5.12, 7.68, 10.24, 12.80, 15.36, 17.92, 20.48, 23.04, 25.60, 28.16, 30.72, 33.28, 35.84, 38.40 and 40.96 seconds.

ue-requested

This keyword specifies the UE requested values of the Paging Time Window (PTW) and the eDRX cycle length received from the UE in the Attach Request or TAU Request message be accepted.

edrx-cycle *cycle_length_value*

This keyword configures the eDRX cycle length. *cycle_length_value* is an integer value in seconds. The allowed values are 5.12, 7.68, 10.24, 12.80, 15.36, 17.92, 20.48, 40.96, 81.92, 163.84, 327.68, 655.36, 1310.72, 2621.44, 5242.88 and 10485.76 seconds.

dl-buf-duration

This optional keyword sends downlink buffer duration in DDN ACK when unable to page UE.

packet-count *packet_count_value*

This optional keyword sends "DL Buffering Suggested Packet Count" in DDN ACK when unable to page UE. The *packet_count_value* is an integer value from 0 to 65535. If the *packet_count_value* is not configured locally, the subscription provided value for the *packet_count_value* is used. The subscription value can be 0 in which case the packet count IE will not be sent for that subscriber even if it is configured locally.

Usage Guidelines

Use this command to enable eDRX on the MME for NB-IoT subscribers. The operator can use this command for:

- Accept eDRX parameters: Paging Time Window (PTW) and eDRX cycle length value, from the UE
- Configure PTW and eDRX cycle length value
- Configure downlink buffer duration in DDN ACK when unable to page UE
- Configure "DL Buffering Suggested Packet Count" in DDN ACK when unable to page UE

When the eDRX feature is enabled on the MME, it pages the NB-IoT subscribers only at valid paging occasions. The MME sends the NB-IoT eDRX paging parameters to the eNodeB during paging. The operator can either configure the option to accept the UE requested values or configure the values using this command. This command is not enabled by default.

A similar CLI command is implemented for WB-EUTRAN subscribers. Both WB-UTRAN eDRX and NB-IoT eDRX parameters can be configured on the system for WB-UTRAN and NB-IoT subscribers.

See the *eDRX Support on the MME* feature chapter in the *MME Administration Guide* for more information.

Example

The following command configures the PTW and eDRX cycle length. The command also sends the downlink buffer duration in the DDN ACK along with a suggested packet count:

```
nb-iot edrx ptw 256 edrx-cycle 512 dl-buf-duration packet-count 10
```

path-failure

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

Product

S-GW

SAEGW

Privilege

Administrator

Command Modes

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

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

default

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

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

Specifies the interface to which the action will be applied.

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

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

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

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

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

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

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

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

{ local-purge | signal-peer }

Specifies the action to apply to the selected interface.

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

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

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

Usage Guidelines

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

Example

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

path-failure s5 signal-peer

pco-options

In releases prior to 21.1.V0 (N5.1):

This command controls the sending of customized PCO (Protocol Configuration Options) options in the network to MS GTP messages and configures APN to include link MTU in PCO IE.

In release 21.1.V0 (N5.1) and later:

Configures APN to include protocol configuration options in PCO/APCO/EPCO IE as applicable.

Product

P-GW

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > APN Configuration

configure > context *context_name* **> apn** *apn_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

pco-options { custom1 [ue-requested] | link-mtu *bytes* **[non-ip** *bytes* **] }**epdg fqdn *domain_name*

{ default | no } pco-options [custom1 | link-mtu [non-ip]]

custom1

Enable sending of customized PCO options in the network to MS messages; send customized PCO options to all UEs regardless of support.

ue-requested

Enable sending of customized PCO options in the network to MS messages for "UE-Requested" mode; send PCO to only UEs that request customized PCO options.

link-mtu *bytes*

In releases prior to 21.1.V0 (N5.1):

Configures APN to include link MTU in PCO IE, if it is requested by UE.

In release 21.1.V0 (N5.1) and later:

Configures APN to include Link MTU in PCO/APCO/EPCO IE of IP and Non-IP PDN connection response, if it is requested by UE.

When UE sends IPv4 Link MTU Size PCO request during Initial attach/ Standalone PDN connection, then the S-GW/SGSN/HSGW sends the same transparently in Create Session Request, Create/Update PDP Context Request, or PBU to P-GW, GGSN, or PMIP-PGW. Create Session Response, Create/ Update PDP Context Response/ PBA will be sent with latest configured MTU size PCO value in APN. If UE is in outbound roaming, then default value (1500) will be provided in the MTU size PCO.

bytes must be an integer from 1280 to 2000.

Default: 1500

non-ip *bytes*

Link MTU for Non-IP PDN. *bytes* must be an integer from 128 to 2000. Default is 1358.

epdg

Enables operator specific epdg selection in the PCO. By default it is disabled.

fqdn

Specifies fully qualified domain name. Based on this, IP addresses would be queried from the DNS.

default

Disable sending of customized PCO options in the network to MS messagesand/ or sets the link MTU PCO to 1500 bytes.

no

Do not send customized PCO options to any UEs and/ or sets the link MTU PCO to 1500 bytes.

Usage Guidelines

Use this command to enable or disable sending of customized PCO options in the network to MS GTP messages and configure link MTU size PCO value.

Important Configure custom PCO values in **pco-custom1** command in *ACS Charging Action Configuration Mode*.

Example

The following command enables sending customized PCO options to all UEs regardless of support:

`pco-options custom1`

The following command disables sending of customized PCO options in the network to MS messagesand sets the link MTU PCO to 1500 bytes:

`default pco-options`

The following command configures epdg.com

```
pco-options epdg fqdn epdg.com
```

pdn-type

This command is used to configure the PDN type indicator in the APN profile.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > APN Profile Configuration

configure > apn-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(apn-profile-profile_name)#`

Syntax Description

```
pdn-type { ip | non-ip { sgi | t6a [ scef-id scef_id [ scef-realm realm_name
 ] ] } }
remove pdn-type
```

remove

The keyword remove deletes the existing configuration.

ip

Use this keyword to configure the Cellular IoT PDN type as IP PDN.

non-ip

Use this keyword to configure the Cellular IoT PDN type as Non-IP PDN.

sgi

Use this keyword to configure the Cellular IoT Non-IP PDN delivery path type as SGi.

t6a

Use this keyword to configure the Cellular IoT Non-IP PDN delivery path type as T6a.

scef-id *scef_id*

The user can optionally specify the SCEF ID using this keyword. The SCEF identifier is a string of length 1 up to 63 characters.

scef-realm *realm_name*

Use this keyword to optionally specify the SCEF diameter realm name. The *realm_name* is string of length 1 up to 127 characters.

Usage Guidelines

Use this command to specify the Cellular IoT PDN type. With this command the user has an option to override the HSS provided APN subscription PDN type. This command is applicable during Attach and additional PDN connectivity only and not during Handover scenarios. This command is not enabled by default.

Use the following command to configure the PDN type as Non-IP and the delivery path type as SGi:

pdn-type non-ip sgi

Use the following command to specify the PDN type as Non-IP and the delivery path as T6a along with the SCEF identifier and realm name:

pdn-type non-ip t6a scef-id *sc1* **scef-realm** *xyz.com*

pdp-type

Configures the type of PDP contexts that are supported by this APN.

Product

GGSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > APN Configuration

configure > context *context_name* **> apn** *apn_name*

Entering the above command sequence results in the following prompt:

[*context_name*]*host_name*(config-apn)#

Syntax Description

pdp-type { **ipv4** [**ipv6**] | **ipv6** [**ipv4**] | **ppp** | **non-ip** }
default pdp-type

default

Configures the default PDP type, IPv4, for the APN.

ipv4 [ipv6]

Enables support for IPv4 PDP contexts. Also enables support for IPv6 if the IPv6 optional keyword is entered in this command. Default: Enabled

Important

Entering both IPv4 and IPv6 in either order enables support for both.

ipv6 [ipv4]

Enables support for IPv6 PDP contexts. Also enables support for IPv4 if the IPv6 optional keyword is entered in this command. Default: Disabled

Important Entering both IPv4 and IPv6 in either order enables support for both.

ppp

Enables support for PPP PDP contexts. Default: Disabled

non-ip

Enables support for Non-IP PDP Type for the APN.

Usage Guidelines

IP PDP context types are those in which the MS is communicating with a PDN such as the Internet or an intranet using IP. PPP PDP contexts are those in which PPP or PPP Network Control Protocol (NCP) frames from the MS are either terminated at, or forwarded by the GGSN.

If a session specifies a PDP type that is not supported by the APN, the system rejects the session with a cause code of 220 (DCH, Unknown PDP address or PDP type).

Caution For the IPv6 calls to work, the destination context must have at least one IPv6 interface configured.

Example

The following command configures the APN to support PPP context types:

pdp-type ppp

psm

This command is used to configure UE Power Saving Mode parameters.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

[local]*host_name*(config-call-control-profile-*profile_name*)#

Syntax Description

[remove] psm {ue-requested [dl-buf-duration [packet-count *packet_value* **]]| t3324-timeout** *t3324_value* **t3412-extended-timeout** *t3412_ext_value* **[dl-buf-duration [packet-count** *packet_value* **]]}**

remove

The **remove** keyword deletes the existing power saving mode configuration.

ue-requested

Use this keyword when UE requested values for Active and Extended Periodic timers are to be accepted.

t3324-timeout *t3324_value*

Use this keyword to configure the T3324 active timer value.

t3324_value

The T3324 active timer is an integer value in the range 0 up to 11160 seconds.

t3412-extended-timeout *t3412_ext_value*

Use this keyword to configure the t3412 Extended timer value.

t3412_ext_value

The T3412 extended timer is an integer value in the range 0 up to 35712000 seconds.

dl-buf-duration

Use this keyword to Send Downlink Buffer Duration in DDN ACK when unable to page UE.

packet-count *packet_value*

Use this keyword to send 'DL Buffering Suggested Packet Count' in DDN ACK when unable to page UE.

packet_value

The *packet_value* is an integer value from 0 up to 65535.

Usage Guidelines

Use this CLI command to configure the T3324 active and T3412 extended timers. The CLI also provides an option to either accept UE requested values or HSS subscribed values or MME configured values for these timers. This command is used to configure either to send or not send the Downlink Buffer Duration in DDN Ack, the DDN Ack Optional IE "Downlink Suggested Packet Count". The CLI option **dl-buf-duration [packet-count** *packet_value* **]** is used to optionally configure either to send or not send the downlink buffer duration in DDN Ack, the DDN Ack Optional IE "Downlink Suggested Packet Count" can also be configured. If this option is not configured and not sent in subscription, MME does not send IE in DDN reject. If the **packet-count** value is not configured locally, the subscription value for **packet-count** is used. The subscription value can be "0", in this case the packet count IE will not be sent for that subscriber even if it is configured locally. If the T3324 active and T3412 extended timers are locally configured these values are always used. If the **psm** command is configured to use the UE requested values for Active and Extended Periodic timers the UE requested values are accepted, but in case if the UE does not request T3412 extended timer, then the value available in subscription data are used for Extended Periodic timer. If the values are not available in the subscription data then the values configured under the MME service are used .

As per latest version of 3GPP TS 24.008, the maximum value of T3412 extended timer can be "320*31" hours that is "35712000" seconds. Due to MME constraints on timer implementation the T3412 extended timer is restricted to 1050 hours that is "3780000" seconds. However, the nearest usable value of this timer as 3GPP TS 24.008 GPRS Timer 3 is 960 hours (320 * 3) that is 3456000 seconds.

Example

Use the following command to enable power saving mode and to accept UE requested values for T3324 and T3412 timers.

psm ue-requested

Use the following command enable UE power saving mode and provide operator desired values for T3324 and T3412 timers:

psm t3324-timeout *100* **t3412-extended-timout** *5000*

Use the following command to enable PSM and accept UE requested values for T3324 and T3412 timers. This command also specifies the 'DL Buffering Suggested Packet Count' in DDN ACK when unable to page UE.

psm ue-requested dl-buf-duration packet-count *100*

In the following example, PSM is enabled and values of T3324 and T3412 timers are specified along with configuring a packet count in DDN ACK:

psm t3324-timeout *1000* **t3412-extended-timeout** *5000* **dl-buf-duration packet-count** *100*

require session ipsecmgr-per-vcpu

Configures the number of IP Security Manager (ipsecmgr) processes per vCPU.

Product

ePDG (VPC-DI platform only)

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

`[local]host_name(config)#`

Syntax Description

[default] require session ipsecmgr-per-vcpu *count* **}**

default

Returns the number of ipsecmgrs per vCPU to the default of 1.

count

Sets the number from 1 through 2 of the ipsecmgr processes to be created for each vCPU. Default: 1.

Usage Guidelines

Enables multiple IP Security Manager (ipsecmgr) processes per vCPU.

Example

The following command configures the system to create 2 ipsecmgrs per vCPU:

require session ipsecmgr-per-vcpu 2

require session sessmgr-per-vcpu

Configures the number of Session Manager (sessmgr) processes per vCPU.

Product

All (VPC-DI platform only)

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

`[local]host_name(config)#`

Syntax Description

[default] require session sessmgr-per-vcpu *count* **}**

default

Returns the number of sessmgrs per vCPU to the default of 1.

count

Sets the number from 1 though 4 of the sessmgr processes to be created for each vCPU. Default: 1.

Usage Guidelines

For applications that are light on CPU usage but heavy on RAM usage, such as Internet of Things (IoT) Gateway, it is more efficient to have multiple session manager (sessmgr) processes per vCPU.

A maximum of 4 sessmgr processes per vCPU and 64 sessmgr processes per Service Function (SF) VM are supported. A maximum of 1152 sessmgr processes are supported for a single VPC-DI instance.

Example

The following command configures the system to create 2 sessmgrs per vCPU:

require session sessmgr-per-vcpu 2

scef-service

This command associates SCEF-service to the Call Control Profile.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax

[remove] associate scef-service *service_name*

remove

This command prefix removes the SCEF association from Call Control Profile.

associate

This command associates the SCEF service with Call Control Profile.

scef-service*service_name*

This command associates SCEF with the call-control-profile, which is identified by a service name. The service name is a string which ranges from 1 to 63.

Usage Guidelines

Use this command to associate an SCEF service to the Call Control Profile for Non-IP Data Delivery (NIDD).

scef-service

This command associates SCEF-service to the MME Service.

Product

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > MME Service

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

Entering the above command sequence results in the following prompt:

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

Syntax

[remove] associate scef-service *service_name*

remove

This command prefix removes the SCEF association from MME Service.

associate

This command associates the SCEF service with MME Service.

scef-service*service_name*

This command associates SCEF with the MME Service, which is identified by a service name. The service name is a string which ranges from 1 to 63.

Usage Guidelines

Use this command to associate an SCEF service to the MME Service for Non-IP Data Delivery (NIDD).

serving-plmn-rate-control

This command is used to configure the serving PLMN rate control for control plane CIoT optimization. The serving PLMN rate control limits the rate at which UE or PGW/SCEF can send data over the control plane when CP optimization is enabled.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

Syntax Description

```
serving-plmn-rate-control ul-rate ul_rate_value dl-rate dl_rate_value
remove serving-plmn-rate-control
```

remove

The keyword remove deletes the existing configuration.

ul-rate *ul_rate_value*

The maximum number of data NAS PDUs the UE can send in uplink path per deci-hour (6 minutes). The uplink rate is an integer from 10 up to 65535. A value of 65535 in this case implies no limit on the number of PDUs the UE can send in the uplink path per deci-hour.

dl-rate *dl_rate_value*

The maximum number of data NAS PDUs the PGW/SCEF can send in the downlink path to the UE per deci-hour (6 minutes). The downlink rate is an integer from 10 up to 65535. A value of 65535 in this case implies no limit on the number of PDUs the PGW/SCEF can send in the downlink path per deci-hour.

Usage Guidelines

This command configures serving PLMN rate for data over NAS. It limits the rate for data exchange between UE and the PGW/SCEF while using control plane CIoT optimization. This command is not enabled by default.

Example

Use the following command to configure the serving PLMN rate for data over NAS, with uplink rate as 35 and downlink rate as 45:

```
serving-plmn-rate-control ul-rate 35 dl-rate 45
```

show card

The output of the **show card table** and **show card information** commands were modified to reflect a new Slot Type.

Service Functions (SFs), Network Functions (NFs), and Application Functions (AFs) are now collectively represented as Function Cards and are grouped under a common Slot Type of "FC" in the output of these commands.

Previously, these cards were represented by the following slot types:

- Service Function: SFC
- Network Function: NFC
- Application Function: AFC

Note Thie Slot Type designator for the Control Function (CF) virtual card type ,which are always in slots 1 and 2, remains unchanged as "CFC".

The following are examples of the new **show card table** and **show card information** command output:

show card table Example

show card table

```
1: CFC      Control Function Virtual Card      Standby        -
2: CFC      Control Function Virtual Card      Active         No

3: FC  2-Port Service Function Virtual Card    Standby        -
8: FC  1-Port Network Function Virtual Card    Active         No
9: FC  1-Port Application Func. Virtual Card   Active         No
10:FC  1-Port Service Function Virtual Card    Standby        -
```

show card information Example

show card information 3

```
Card 3:
  Slot Type                : FC
  Card Type                : 2-Port Service Function Virtual Card
  Operational State        : Standby
  Desired Mode             : Standby
```

show cloud configuration

Displays the contents of the configuration file.

Product All

Privilege Security Administrator, Administrator, Inspector, Operator

Mode

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax

show cloud configuration

Usage

This command dumps the contents of the configuration file to the screen. It displays the configuration file on the config disk or the local flash. Usually the user does not have direct access to these files. The local param file on the flash is defined during the VPC installation and the config disk is usually created by the orchestrator and then attached to the card.

Example

This command displays the hardware configuration associated with card number 1:

show cloud configuration

show cloud hardware

Displays the hardware configuration for each card or a specific card.

Product All

Privilege Security Administrator, Administrator, Inspector, Operator

Mode

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax

show cloud hardware *card_number*

card_number

Specifies the number of the card for which to display information.

Usage

Displays the configuration of the underlying VM hardware for a specific card or all cards in the VPC. It provides information regarding the configured vCPU, memory size, huge page size, crypto hardware and the NIC.

Example

This command displays the hardware configuration associated with card number 1:

show cloud hardware 1

show cloud hardware optimum

Displays the optimum hardware configuration of the hardware parameters listed to achieve highest throughput.

Product

All

Privilege

Security Administrator, Administrator, Inspector, Operator

Mode

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax

show cloud hardware optimum

Usage

Displays the optimum configuration of the underlying VM hardware according to the available parameters. It provides information regarding the configured vCPU, memory size, huge page size, crypto hardware and the NIC.

Example

This command displays the optimum hardware configuration for the associated VM hardware:

show cloud hardware optimum

show cloud hardware test

Compares the current hardware configuration for each card or a specific card against the optimum settings.

Product

All

Privilege

Security Administrator, Administrator, Inspector, Operator

Mode

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax

`show cloud hardware test` *`card_number`*

card_number

Specifies the number of the card for which to display information.

Usage

Compares the configuration of the underlying VM hardware of a specific card or all cards in the VPC to the optimum configuration. It provides information regarding the configured vCPU, memory size, huge page size, crypto hardware and the NIC and indicates the optimum values for each parameter.

Example

This command displays the hardware configuration associated with card number 1:

`show cloud hardware test 1`

show cloud monitor

Displays VPC-DI network latency and packet loss statistics for all cards or a specific card in the VPC.

Product

All

Privilege

Security Administrator, Administrator, Inspector, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

`show cloud monitor di-network` `{`**`detail`** `|` **`summary`**`}` *`card_number`*

detail

Displays detailed information about the VPC-DI network.

summary

Displays summary information about the VPC-DI network.

card_number

Specifies the number of the card for which to display information.

Usage Guidelines

Displays the configuration of the underlying VM hardware for a specific card or all cards in the VPC. It provides information regarding the configured vCPU, memory size, huge page size, crypto hardware and the NIC.

Example

This command displays summary monitored statistics for VPC-DI network communications from and to the third card in the VPC. The display shows the test packet loss rate for the past five minutes and past 60 minutes. If the rate is larger than 1%, the health status is marked as "Bad".

show cloud monitor di-network summary 3

```
Card 3 Test Results:

ToCard   Health   5MinLoss   60MinLoss
   1      Good       0.0%      0.0%
   2      Good       0.0%      0.0%
   4       Bad       6.32%     5.36%
   5      Good       0.0%      0.0%
   6      Good       0.0%      0.0%
```

show scef-service statistics

Displays SCEF Service configuration and status information.

Product

MME

Privilege

Security Administrator, Administrator, Operator, Inspector

Command Modes

Exec

The following prompt is displayed in the Exec mode:

[local]*host_name*#

Syntax Description

show scef-service statistics { all | name *service_name* **| summary }**

all

Displays all available configuration and status information for all SCEF Services.

name *service_name*

Displays all status information for a specified SCEF service name.

summary

Displays the summary of the available SCEF service statistics.

Usage Guidelines

Use this command to display SCEF service information and its statistics.

Example

The following command displays all SCEF service statistics:

show scef-service statistics all

The following command displays information for an SCEF service configuration with the service name *Test*:

show scef-service statistics name *Test*

Important

Output descriptions for commands are available in the *Statistics and Counters Reference*.

show system ssh key status

Displays the fingerprint of the current internal SSH key in use, the source of where the key was found, and the SSH status of all online VMs.

Product

VPC-DI

Privilege

Security Administrator, Administrator, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]`*`host_name`*`#`

Syntax Description

show system ssh key status [| { grep *grep_options* **| more }]**

| { grep *grep_options* | more }

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

Usage Guidelines

This command displays information about the SSH keys used for internal communication between all component VMs in a VPC-DI system, such as for remote command execution and file transfers.

system packet-dump

Initiates a packet dump on an SF or CF card in a VPC-DI system.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

system packet-dump { di-net card *slot_num* **| port** *service_port* **} [bond { a | b } | direction { both-rxtx | rx | rxtx | tx } | duration** *seconds* **| packet-type { ipv4 | ipv6 } | pcapfile-size** *size* **| pcapfile-split-val** *value* **| protocol { icmpv4 | icmpv6 | tcp | udp } | to file** *filename* **]**

di-net card *slot_num*

Specifies the card from 1 through *n*.

port *card_port/port_num*

Specifies the ethernet interface based on the card number from 1 through *n* and port number from 1 through 50, for example 3/1.

bond { a | b }

Specifies a slave for bonded interfaces.

direction { both-rxtx | rx | rxtx | tx }

Specifies a filter for the direction of the packets to capture, either receive (**rx**), transmit (**tx**), or both (**rxtx**). Use the **both-rxtx** option to capture both receive and transmit, but output each to separate files.

duration *seconds*

Specifies the number of seconds from 1 through 600 for the packet dump. Default: 5 seconds

packet-type { ipv4 | ipv6 }

Specifies a filter for the type of the packets to capture, either **ipv4** or **ipv6**.

pcapfile-size *size*

Specifies the maximum size for each packet capture (pcap) file from 10 to 800 megabytes. Default: 10 megabytes.

pcapfile-split-val *value*

Specifies the number of pcap files to generate for a given capture from 0 to 10. Default: 0 (do not split files).

protocol { icmpv4 | icmpv6 | tcp | udp }

Specifies a filter for the protocol of the packets to capture, either **icmpv4**, **icmpv6**, **tcp**, or **udp**.

to file { /flash | /hd-raid | /cdrom1 | /sftp } [/directory]/ *filename*

Specifies the output location and filename.

Usage Guidelines

Use this command to perform packet captures to troubleshoot issues within a VPC-DI deployment.

Example

The following command initiates a packet dump on card in slot 7, port 1, and output the dump to a file stored locally at /flash/example7-1.pcap

system packet-dump port 7/1 to file /flash/example7-1.pcap

system ping

Initiates a ping test on the internal network between two VMs within the VPC-DI system.

Product

VPC-DI

Privilege

Security Administrator, Administrator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

system ping from card *slot_num* **to card** *slot_num* **[count** *number_of_packets* **| size** *bytes* **]**

from card *slot_num*

Specifies the card slot number from 1 through *n* from which the ping test originates.

to card *slot_num*

Specifies the destination card slot number from 1 through *n*.

count *number_of_packets*

Sets the number of ping packets from 1 through 10000 to be sent. Default: 5 packets

size *bytes*

Sets the size of the ICMP Datagram in bytes from 40 to 18432. Default: 56

Usage Guidelines

Use this command to perform ping tests to troubleshoot connectivity issues within a VPC-DI deployment.

Example

The following command initiates a ping test of 1000 packets from the card in slot 1 to the card in slot 9:

system ping from card 1 to card 9 count 1000

system ssh

Manages the persistent ssh user keys used for the internal ssh sessions between cards (VMs) in a VPC-DI system.

Product

VPC-DI

Privilege

Security Administrator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

```
system ssh key { copy boot1 to card slot_num | create boot1 }
 no system ssh key boot1 { all | card slot_num }
```

no system ssh key boot1 { all | card *slot_num* }

Deletes the persistent ssh keys on a specific card or all cards in the VPC-DI system. Deletion of keys may be used to purge a VM of the persistent keys or prepare the system for using a different distribution method (ESC, OpenStack, attached ISO).

- **all** : Deletes the ssh keys on all cards in the VPC-DI system.
- **card** *slot_num* : Deletes the ssh keys on the card specified by *slot_num* .

Note This command does not affect the VM until it is rebooted. It will continue to use the active key found during its boot.

copy boot1 to card *slot_num*

Transfers the persistent ssh keys (both public and private) in /boot1 on the active CF to another VM. That VM must be in a state to accept it by a user with console access placing it in receiver mode during its failed boot.

create boot1

Creates new persistent ssh keys (both public and private) and stores it in /boot1 on the active CF.

Note This command does not affect the VM until it is rebooted. It will continue to use the active key found during its boot.

Usage Guidelines

Use this command to manage the internal ssh keypairs in a VPC-DI deployment. While StarOS provides sshd services for user CLI and SFTP sessions on the management VMs (CF), another set of sshd services run for the exlusive use of internal communication between all component VMs, such as for remote command execution and file transfers. This internal sshd is only used on the internal DI-network interface.

This command enables you to store and manage ssh keys on the VM's virtual hard disk drive (HDD). This provides an alternate option for storing ssh keypairs besides the other methods such as Cisco Elastic Services Controller (ESC), OpenStack, or a directly attached ISO. The /boot1 partition is only accessible by a security administrator.

Use the **show system ssh key status** command to display the fingerprint of the current public key in use, the origin of where the key was found, and the status of all online VMs.

Example

The following command copies the ssh keypairs from the active CF to the card in slot 12

`system ssh key copy boot1 to card 12`

tunnel udpip

Configures UDP-IPv4 or UDP-IPv6 tunneling parameters between the P-GW and an external application server for the APN.

Product

P-GW

S-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > APN Configuration

configure > context *context_name* **> apn** *apn_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
tunnel udpip peer-address peer_address peer-port peer_udp_port [ local-port local_udp_port ]
no tunnel udpip
```

no

Disables UDP-IPv4 or UDP-IPv6 tunneling for the APN.

peer-address *peer_address*

Specifies the Peer address for the tunnel.

peer_address must be expressed in dotted-decimal notation.

peer-port *peer_udp_port*

Specifies the port number of the peer for the tunnel.

peer_udp_port must be expressed in dotted-decimal notation.

local-port ***local_udp_port***

Specifies the local UDP port number.

Default: 49152

Usage Guidelines

For local and peer UDP port number, it is recommended to use unregistered port number with IANA.

This CLI command takes effect during new subscriber call creation on S5/S8 interface to the APN.

Example

The following command configures the system to encapsulate subscriber traffic using UDP-IPv4 and tunnel it from a locally assigned IP address with port number *49152* to an external application server with an IP address of *192.168.1.100* on peer UDP port *11220*:

```
tunnel udpip peer-address 192.168.1.100 peer-port 11220 local-port 49152
```