

APN Configuration Mode Commands

Command Modes

The Access Point Name (APN) Configuration Mode is used to create and configure APN profiles within the current system context of an UMTS/LTE service.

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)#
```

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

- aaa, on page 4
- access-link, on page 6
- accounting-mode, on page 7
- active-charging bandwidth-policy, on page 10
- active-charging fallback-to-apn-rulebase, on page 11
- active-charging link-monitor tcp, on page 12
- active-charging radio-congestion, on page 13
- active-charging rulebase, on page 14
- active-charging rulebase-list, on page 15
- apn-ambr, on page 16
- associate accounting-policy, on page 18
- associate qci-qos-mapping, on page 19
- authentication, on page 20
- authorize-with-hss, on page 25
- bearer-control-mode, on page 26
- backoff timer-value, on page 28
- bearer-duration-stats, on page 29
- cc-home, on page 30
- cc-profile, on page 31
- cc-roaming, on page 33
- cc-sgsn, on page 34

- cc-visiting, on page 37
- content-filtering category, on page 38
- credit-control-client, on page 39
- credit-control-group, on page 40
- daf-pdp-type, on page 42
- data-tunnel mtu, on page 43
- data-tunneling ignore df-bit, on page 44
- dcca origin endpoint, on page 45
- dcca peer-select, on page 45
- delay-tolerant-pdn, on page 46
- description, on page 47
- dhcp context-name, on page 48
- dhcp lease-expiration-policy, on page 48
- dhcp service-name, on page 49
- dhcpv6 context-name, on page 50
- dhcpv6 service-name, on page 51
- dns, on page 52
- egtp, on page 53
- egtpc-qci-stats, on page 54
- ehrpd-access, on page 56
- emergency-apn, on page 57
- end, on page 58
- exit, on page 58
- firewall policy, on page 58
- fw-and-nat policy, on page 59
- gsm-qos negotiate, on page 60
- gtpp group, on page 62
- gtpp secondary-group, on page 64
- idle-timeout-activity, on page 65
- ignore-alt-config, on page 66
- ikev2 tsr, on page 67
- ims-auth-service, on page 68
- iot-rate-control, on page 69
- ip access-group, on page 70
- ip address alloc-method, on page 72
- ip address pool, on page 76
- ip address pool-exhaust-action, on page 77
- ip context-name, on page 78
- ip header-compression, on page 78
- ip hide-service-address, on page 79
- ip local-address, on page 80
- ip multicast discard, on page 81
- ip-pool-mgmt-policy, on page 82
- ip qos-dscp, on page 82
- ip source-violation, on page 85
- ip user-datagram-tos copy, on page 87

- ipv6 access-group, on page 88
- ipv6 address alloc-method, on page 89
- ipv6 address delegate-prefix-pool, on page 90
- ipv6 address prefix-delegation-len, on page 91
- ipv6 address pool-exhaust-action, on page 91
- ipv6 dns, on page 92
- ipv6 egress-address-filtering, on page 93
- ipv6 initial-router-advt, on page 94
- l3-to-l2-tunnel address-policy, on page 95
- loadbalance-tunnel-peers, on page 96
- long-duration-action detection, on page 97
- long-duration-action disconnection, on page 98
- lte-s2bgtp-first-uplink, on page 99
- mbms bmsc-profile, on page 100
- mbms bearer timeout, on page 101
- mbms ue timeout, on page 102
- mbr, on page 103
- mediation-device, on page 104
- mobile-ip home-agent, on page 106
- mobile-ip min-reg-lifetime-override, on page 107
- mobile-ip mn-aaa-removal-indication, on page 108
- mobile-ip mn-ha-hash-algorithm, on page 109
- mobile-ip mn-ha-shared-key, on page 109
- mobile-ip mn-ha-spi, on page 110
- mobile-ip required, on page 111
- mobile-ip reverse-tunnel, on page 112
- nai-construction, on page 112
- nbns, on page 114
- netloc-s2b-ue-ip-udp-port-always, on page 115
- network-behind-mobile, on page 115
- nexthop-forwarding-address, on page 116
- npu qos, on page 117
- outbound, on page 118
- paging-policy-differentiation, on page 119
- p-cscf, on page 121
- pco-options, on page 122
- pdn-behavior, on page 127
- pdn validate-post-switchover, on page 129
- pdp-type, on page 129
- permission, on page 130
- pgw fqdn, on page 131
- pilot-packet, on page 132
- policy, on page 135
- ppp, on page 137
- proxy-mip, on page 139
- qci, on page 140

- qos negotiate-limit, on page 141
- qos rate-limit, on page 144
- qos-renegotiate, on page 146
- qos traffic-police, on page 147
- radius, on page 147
- radius group, on page 147
- radius returned-framed-ip-address, on page 147
- radius returned-username, on page 148
- radius rulebase-format, on page 149
- reporting-action, on page 150
- restriction-value, on page 151
- secondary ip pool, on page 153
- selection-mode, on page 154
- stats-profile, on page 155
- timeout, on page 156
- timeout bearer-inactivity, on page 157
- timeout emergency-inactivity, on page 160
- timeout idle, on page 161
- timeout idle micro-checkpoint-deemed-idle, on page 162
- timeout idle micro-checkpoint-periodicity, on page 163
- timeout long-duration, on page 165
- tpo policy, on page 166
- tunnel address-policy, on page 166
- tunnel gre, on page 167
- tunnel ipip, on page 168
- tunnel ipsec, on page 169
- tunnel l2tp, on page 170
- tunnel udpip, on page 173
- user-plane-group, on page 174
- virtual-apn gdcr, on page 174
- virtual-apn preference, on page 176

aaa

This command configures Authentication, Authorization, and Accounting (AAA) functionality at the Access Point Name (APN) level.

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

```
aaa { group aaa_group_name | secondary-group aaa_group_name }
default aaa { group | secondary-group aaa_group_name }
no aaa { group aaa_group_name  | secondary-group }
```

no aaa

Disables the specified AAA group for the specific APN.

no aaa { group | secondary-group }

- **group**: Uses the default AAA group.
- **secondary-group**: Removes the secondary AAA group from the APN's configuration.

default aaa { group | secondary-group }

Configures the default setting for the specified parameter.

- **group**: Uses the default AAA group—the one specified at the context level or in the APN template.
- **secondary-group**: Removes the secondary AAA group from the APN configuration.

aaa_group_name

Specifies the AAA server group for the APN.

aaa_group_name must be an alphanumeric string of 1 through 63 characters.

secondary-group *aaa_group_name*

Specifies the secondary AAA server group for the APN.

aaa_group_name must be an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to configure AAA functionality at the APN level.

Instead of having a single list of servers per context, this feature configures multiple server groups within a context and applies individual server group for APNs in that context. Each server group consists of a list of AAA servers for each AAA function (accounting, authentication, charging, etc.).

The AAA secondary server group supports the RADIUS Fire-and-Forget feature in conjunction with GGSN for secondary accounting (with different RADIUS accounting group configuration) to the RADIUS servers without expecting acknowledgment from the server, in addition to standard RADIUS accounting. This secondary accounting will be an exact copy of all the standard RADIUS accounting message (RADIUS Start / Interim / Stop) sent to the standard AAA RADIUS server.

If the same AAA group is configured with both the **aaa group** *aaa_group_name* and the **aaa secondary-group** *aaa_group_name* commands, then this configuration will have no effect and secondary accounting will not happen.

The AAA secondary server group configuration takes effect only when used with APN accounting-mode set to radius-diameter (or) with mediation-acct enabled. The RADIUS accounting triggers for both standard

RADIUS accounting and secondary accounting will be taken from the AAA group configured with the **aaa group** *aaa_group_name* command. On the fly change of this configuration is not supported. Any change to the configuration will have effect only for new calls.

Example

The following command applies the AAA server group *star1* to an APN within the specific context:

```
aaa group star1
```

access-link

Configures IP fragmentation processing over the Access-link (PPP, GTP etc.).

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

```
[ no ]access-link ip-fragmentation { df-fragment-and-icmp-notify |
df-ignore | normal }
default access-link ip-fragmentation
```

df-fragment-and-icmp-notify

Default: Disabled

Partially ignores the DF bit; fragments and forwards the packet, but also returns an ICMP error message to the source of the packet. The number of ICMP errors sent like this is rate-limited to one ICMP error packet per second per session.

no

Disables the access-link IP fragmentation at APN level to the mobile node if the link MTU is smaller than the packet length.

df-ignore

Default: Enabled

Ignores the DF (Don't Fragment) bit setting; fragments and forwards the packet over the access link. This is the default behavior.

normal

Default: Disabled

Drops the packet and sends an ICMP unreachable message to the source of packet.

Usage Guidelines

If the IP packet to be forwarded is larger than the access-link MTU and if the DF (Don't Fragment) bit is set for the packet, then the fragmentation behavior configured by this command is applied. Use this command to fragment packets even if they are larger than the access-link MTU.

Fragmentation may also occur for other reasons, regardless of whether or not fragmentation is performed because of one of the above reasons.

Payloads are encapsulated within IP/UDP/GTP before being sent to the SGSN. If that encapsulation causes the packet to exceed 1500 bytes, the inner IP payload is fragmented (even if it's not considered too-large by the above tests) into two payloads (if the DF bit is not set). If the DF bit is set (and access-link ip-fragmentation normal is configured), the system performs IP fragmentation of the entire packet (i.e., IP fragmentation in the outer IP header) rather than fragmenting the inner IP payload. Either way, the result is two packets, but in one case the MS would have to perform IP reassembly while in the other case the SGSN would have to perform reassembly.

Example

Set fragmentation so that the DF bit is ignored and the packet is forwarded anyway by entering the following command:

```
access-link ip-fragmentation df-ignore
```

accounting-mode

Configures the protocol to be used for PDP context accounting by this APN.

Product

eWAG

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

In 16.0 and earlier releases:

```
accounting-mode { gtpp | none | radius-diameter [ no-early-pdus ] [
no-interims ] }
default accounting-mode
```

In 17.0 and later releases:

```
accounting-mode { gtpp | none | radius [ no-early-pdus ] [ no-interims ]
 }
default accounting-mode
```

default

Restores the command to its default setting.

gtpp

Configures the APN to use GPRS Tunneling Protocol Prime for accounting purposes. If used, accounting will begin as soon as the PDP context is established. This is the default setting. Default: Enabled



Important The system's GTPP parameters must be configured prior to using this protocol for accounting. Refer to the **gtpp** commands in the *Context Configuration Mode Commands* chapter.

In 16.0 and earlier releases, the default value of "**accounting-mode gtpp**" was not displayed in the "**show configuration**" command. The value was only displayed in the output of "**show configuration verbose**" command.

In 17.0 and later releases, even for a default configuration of **accounting-mode** under APN, this will be indicated in "**show configuration**" both in verbose and non-verbose modes.

none

Disables accounting for PDP contexts using this APN.

When accounting mode is set to none, it indicates to the GTP stack at session manager to not generate the regular GTPP accounting triggers. Default: Disabled.

radius-diameter

Configures the APN to use RADIUS protocol for accounting purposes. Default: Disabled



Important The system's RADIUS accounting parameters must be configured prior to using either of the protocols for accounting. Refer to the **radius** commands in the *Context Configuration Mode Commands* and the *AAA Server Group Configuration Mode Commands* chapters.



Important The **accounting-mode** CLI command is used only for RADIUS and GTPP accounting. Hence, in 17.0 and later releases, the keyword option "**radius-diameter**" has been replaced with **radius** option, and is concealed to support backward compatibility.

no-early-pdus

Configures the GGSN to discard user traffic once the buffer is full until the RADIUS server has returned a response to the GGSN's accounting START request per 3GPP standards.

Configures the GGSN to delay PDUs from/to MS until the RADIUS server returns a response to the GGSN's accounting START request as per 3GPP standards. The GGSN buffers up to two PDUs per call. Additional PDUs disable the queuing. On receiving the Accounting response message, the GGSN forwards all the subsequent PDUs for that call.

Important For StarOS 10.0 and earlier releases, the system buffers up to four PDUs and queues or discards the remaining PDUs.

Important For StarOS 11.0 and later releases, the system is configured so that none of the PDUs are discarded.

no-interims

Disables the generation of RADIUS interims per APN.

When configured, RADIUS interim updates for this APN will not be sent, regardless of what is configured in the context that is used for RADIUS accounting.

Important Different CLI commands are used to disable RADIUS interims for RADIUS accounting and mediation accounting. To disable RADIUS interims for RADIUS accounting, use the following command: **accounting-mode radius no-interims**. To disable RADIUS interims for mediation accounting, use the following command: **mediation-device context-name** *context_name* **no-interims**.

Usage Guidelines

This command specifies which protocol, if any, will be used to provide accounting for PDP contexts accessing the APN profile.

When the GTPP protocol is used, accounting messages are sent to the charging gateways (CGs) over the Ga interface. The Ga interface and GTPP functionality are typically configured within the system's source context. As specified by the standards, a CDR is not generated when a session starts - CDRs are generated according to the interim triggers (configured using the **cc** command in the GGSN service configuration mode) and a CDR is generated when the session ends. For interim accounting, STOP/START pairs are sent based on configured triggers.

GTPP version 2 is always used. However, if version 2 is not supported by the CGF, the system reverts to using GTPP version 1. All subsequent CDRs are always fully-qualified partial CDRs. All CDR fields are R4.

If the **radius** option is used, RADIUS protocol is used as configured in the Context Configuration mode or the AAA Server Group Configuration mode.

If the RADIUS protocol is used, accounting messages can be sent over a AAA interface or the Gi to the RADIUS server. The AAA or Gi interface(s) and RADIUS functionality are typically configured with the system's destination context along with the APN. RADIUS accounting begins immediately after an IP address is allocated for the MS. Interim accounting can be configured using the **radius accounting interim interval**. The **radius accounting interim interval** command sends INTERIM-UPDATE messages at specific intervals.

Keywords to this command can be used in combination to each other, depending on configuration requirements.



Important If the accounting type in the APN is set to 'none' then G-CDRs will not be generated. If accounting type is left as default "GTPP" and "billing-records" are configured in the ACS Rulebase Configuration Mode, then both G-CDRs and eG-CDRs would be generated.

Example

The following command configures the APN to use the RADIUSr protocol for accounting:

```
accounting-mode radius
accounting-mode radius no-interims no-early-pdus
accounting-mode radius no-early-pdus no-interims
```

active-charging bandwidth-policy

Configures the bandwidth policy to be used for subscribers who use this APN.

Product

ACS

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

active-charging bandwidth-policy *bandwidth_policy_name*
{ default | no } active-charging bandwidth-policy [fallback-enabled]

default

Configures the default setting.

Default: The default bandwidth policy configured in the rulebase is used for subscribers who use this APN.

no

Disables bandwidth control for the APN.

bandwidth-policy *bandwidth_policy_name*

Specifies the bandwidth policy name. *bandwidth_policy_name* must be an alphanumeric string from 1 through 63 characters.

fallback-enabled

Determines whether policy under rulebase can be applied as a fallback value. Fallback is disabled by default.

Usage Guidelines

Use this command to configure bandwidth policy to be used for subscribers who use this APN.

Example

The following command configures a bandwidth policy named *standard* for the APN:

```
active-charging bandwidth-policy standard [ fallback-enabled ]
```

active-charging fallback-to-apn-rulebase

Configures the session to fallback to the default rulebase configured under the APN.

Product

4G CUPS

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

```
[no] active-charging fallback-to-apn-rulebase
```

fallback-to-apn-rulebase

Enables fallback to APN rulebase when PCRF only removes the rulebase and does not send rulebase to install.

By default, this CLI is disabled.



Note This CLI configuration will be applicable for the new incoming calls only. The existing calls will not have any impact on the ongoing calls.

no

Removes the configuration of fallback to default rule configured under the APN.

Usage Guidelines

Use this command to configure the session to fallback to the default rulebase configured under the APN when the session moves back from 5G to 4G.

Example

```
[ingress]qvpc-si(config-apn)# no active-charging fallback-to-apn-rulebase
```

active-charging link-monitor tcp

Enables the TCP link monitoring feature on the Mobile Video Gateway. This command can be configured in either APN Configuration Mode or Subscriber Configuration Mode.



Important In release 20.0, MVG is not supported. This command must not be used in release 20.0. For more information, contact your Cisco account representative.

Product

MVG

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

[default | no] active-charging link-monitor tcp [log [rtt [histogram | time-series] [bitrate [histogram | time-series]] | bitrate [histogram | time-series] [rtt [histogram | time-series]]]] [-noconfirm]

default

Sets TCP link monitoring to its default value, which is the same as **no**.

no

Deletes the TCP link monitoring settings and disables TCP link monitoring if previously configured.

link-monitor tcp

Enables the TCP link monitoring feature on the Mobile Video Gateway. Note that TCP link monitoring is not enabled by default. Also note that when this command is configured without the **log** option, TCP link monitoring is enabled without logging, and the output from TCP link monitoring is only used by the dynamic translating feature.

log [rtt [histogram | time-series] [bitrate [histogram | time-series]] | bitrate [histogram | time-series] [rtt [histogram | time-series]]]

This option enables statistical logging for TCP link monitoring.

The **rtt** option can be used to enable either **histogram** or **time-series** logging for RTT.

Similarly, the **bitrate** option can be used to enable either **histogram** or **time-series** logging for bit rate.

When **rtt** and **bitrate** options are used without additional options, histogram and time-series logging are enabled for RTT and/or bit rate respectively.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage Guidelines

Use this command to enable TCP link monitoring on the Mobile Video Gateway.

Examples

The following command enables TCP link monitoring with statistical logging, with histogram and time-series logging enabled for both RTT and bit rate:

```
active-charging link-monitor tcp log
```

The following command enables TCP link monitoring with statistical logging, with histogram and time-series logging enabled for RTT:

```
active-charging link-monitor tcp log rtt
```

The following command enables TCP link monitoring with statistical logging, with histogram logging enabled for RTT:

```
active-charging link-monitor tcp log rtt histogram
```

The following command enables TCP link monitoring with statistical logging, with histogram logging enabled for RTT and time-series logging enabled for bit rate:

```
active-charging link-monitor tcp log rtt histogram bitrate time-series
```

active-charging radio-congestion

Enables the Congestion Management feature on the Mobile Video Gateway. This command can be configured in either APN Configuration Mode or Subscriber Configuration Mode.



Important In release 20.0, MVG is not supported. This command must not be used in release 20.0. For more information, contact your Cisco account representative.

Product

MVG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context *context_name* **> subscriber { default | name** *subscriber_name* **}**

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
active-charging radio-congestion policy policy_name
[ default | no ] active-charging radio-congestion policy
```

default

Sets congestion management to its default value, which is the same as **[no]**.

Default: Disabled

no

Deletes the settings and disables congestion management if previously configured.

active-charging radio-congestion policy *policy_name*

Enables the Congestion Management feature on the Mobile Video Gateway.

policy_name must be an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to enable or disable congestion management on the Mobile Video Gateway at either APN or subscriber. As congestion management makes use of the Link Monitoring feature, this must also be enabled along with the congestion monitoring feature.

Example

The following command enables radio congestion for a policy named *test123* for the subscriber:

```
active-charging radio-congestion policy test123
```

active-charging rulebase

Specifies the name of the Active Charging Service (ACS) rulebase to be used for subscribers who use this APN.



Important In release 20.0, MVG is not supported. This command must not be used in release 20.0. For more information, contact your Cisco account representative.

Product

ACS

eWAG

GGSN

MVG

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

active-charging rulebase *rulebase_name*
no active-charging rulebase

no

Removes the rulebase previously configured for this APN.

rulebase_name

Specifies the name of the ACS rulebase as an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to specify the ACS rulebase to be used for subscribers who use the APN.

Example

The following command specifies the ACS rulebase named *rule1* for the APN:

active-charging rulebase rule1

active-charging rulebase-list

Specifies the name of the ACS rulebase list to be used for subscribers who use this APN.

Important In release 20.0, MVG is not supported. This command must not be used in release 20.0. For more information, contact your Cisco account representative.

Product

ACS

GGSN

MVG

P-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

active-charging rulebase-list *rulebase_list_name*
no active-charging rulebase-list

no

If previously configured, removes the rulebase list configured in the APN.

rulebase_list_name

Specifies the name of the ACS rulebase list.

rulebase_list_name must be an alphanumeric string of 1 through 63 characters.

Usage Guidelines

Use this command to specify the ACS rulebase list to be used for subscribers who use the APN. The rulebase list is created and configured in the ACS Configuration Mode. For more information, see the **rulebase-list** command in the *ACS Configuration Mode Commands* chapter.

Example

The following command specifies the ACS rulebase list named *rblist* for the APN:

```
active-charging rulebase-list rblist
```

The following command removes the rulebase list named *rblist* from the APN:

```
no active-charging rulebase-list rblist
```

apn-ambr

Configures the Aggregated Maximum Bit Rate (AMBR) for all PDNs of a subscriber using this APN.

Product

GGSN

P-GW

SAEGW

Privilege

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

```
apn-ambr rate-limit direction { downlink | uplink } [ burst-size {
auto-readjust duration   milliseconds msecs | seconds 1:30bytes } |
violate-action { drop | lower-ip-precedence | shape [
transmit-when-buffer-full ] | transmit } ][ token-replenishment-interval
 msecs ]
[ default | no ] apn-ambr rate-limit direction { downlink | uplink }
```

default

Returns the selected command to it's default setting of no APN-AMBR.

no

Disables the selected command.

rate-limit direction { downlink | uplink }

Specifies that the rate limit is to be applied to either the downlink (network to subscriber) traffic or the uplink (subscriber to network) traffic.

downlink: Applies the AMBR parameters to the downlink direction.

uplink: Applies the AMBR parameters to the uplink direction.

burst-size { auto-readjust duration milliseconds *msecs| seconds 1:30* | *bytes*}

This parameter is used by policing and shaping algorithms to permit short bursts of traffic in order to not exceed the allowed data rates. It is the maximum size of the token bucket.

auto-readjust duration *seconds*: The duration (in seconds) used in this burst size calculation: burst size = peak data rate/8 * auto-readjust duration

seconds must be an integer value from 1 to 30. Default is 1 second.

milliseconds must be an integer value from 100 to 900, in increments of 100 milliseconds. For example, 100, 200, or 300, and so on.

bytes: Specifies the burst size in bytes allowed by this APN for the associated PDNs. It must be an integer from 1 to 4294967295 (1 byte to 4 GB).



Important In 17.3 and later releases, the *bytes* option has been deprecated.

violate-action { drop | lower-ip-precedence | shape [transmit-when-buffer-full] | transmit }

The action that the P-GW will take when the data rate of the bearer context exceeds the AMBR.

drop: Drops violating packets.

lower-ip-precedence: Sets the DSCP value to zero ("best effort") for violating packets.

shape [transmit-when-buffer-full]: Places all violating packets into a buffer and, optionally, transmits the packets when the buffer is full.



Important The **shape** keyword and optional **transmit-when-buffer-full**option are available only in StarOS v12.0 and earlier releases, and StarOS v19.2 and later releases.



Important Traffic Shaping is a license-controlled feature. Contact your Cisco account or support representative for detailed licensing information.

transmit: Transmits violating packets. This is the default setting.

token-replenishment-interval

The token replenishment interval is used for both APN AMBR traffic policing and shaping. Operators have the option of using the default interval (100ms) or configuring a lower token replenishment interval of 10ms. Reducing the interval to 10ms helps reduce the queuing time required for the 100ms interval for a given packet size.

Valid entries are 10ms or 100ms.

The default is 100ms.



Important Traffic Shaping is a license-controlled feature. Contact your Cisco account or support representative for detailed licensing information.

Usage Guidelines Use this command to enforce the AMBR for the APN on bearers that do not have a Guaranteed Bit Rate (GBR).

Example

The following command sets the downlink burst rate to use an auto-readjust duration of 2 seconds and lowers the IP precedence of violating packets:

```
apn-ambr rate-limit direction downlink burst-size auto-readjust duration
 2 violate-action lower-ip-precedence
```

associate accounting-policy

Associates the APN with specific pre-configured policies configured in the same context.

Product P-GW

SAEGW

Privilege 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 **`[ no ] associate accounting-policy`** *`name`*

no

Removes the selected association from this APN.

name

Associates the P-GW APN with an accounting policy configured in the same context. *name* must be an existing accounting policy expressed as a string of 1 through 63 characters.

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

Usage Guidelines Use this command to associate the P-GW APN with an accounting policy configured in this context.

Example

The following command associates this P-GW APN with an accounting policy called *acct1*:

```
associate accounting-policy acct1
```

associate qci-qos-mapping

Associates a pre-configured QCI-QoS-Mapping table with this APN to support per APN DSCP marking.

Product P-GW

SAEGW

Privilege 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

```
associate qci-qos-mapping qci_qos_map_table_name rat-type { eutran | geran |
utran }
[ no ] associate qci-qos-mapping rat-type { eutran | geran | utran }
```

no

Removes the selected association of QCI-QoS-Mapping table from this APN.

qci_qos_map_table_name

Specifies a pre-configured QCI-QoS-Mapping table from global configuration mode to this APN. *qci_qos_map_table_name* must be an existing QCI-QoS-mapping table expressed as a string of 1 through 63 characters.

QCI-QoS-Mapping tables are configured in QCI-QoS_Mapping Configuration mode.

rat-type { eutran | geran | utran }

This command selects the Radio Access Technology (RAT) type to implement DSCP marking on user traffic. Only one mapping table can be configured per RAT-type.

eutran: DSCP marking on RAT-Type for EUTRAN.

geran: DSCP marking on RAT-Type for GERAN.

utran: DSCP marking on RAT-Type for UTRAN.

Usage Guidelines

Use this command to associate a pre-configured QCI-QoS-Mapping table with an APN to provide per APN basis DSCP marking.

The GGSN/PGW supports configurable DSCP marking of the outer header of a GTP-U tunnel packet based on a QCI/THP table for the Gn/Gp and S5/S8 interfaces. This feature allows configuring DSCP marking table on a per APN basis.

From Release 21.6 onwards, RAT-Type based DSCP Marking is supported. The supported RAT-Types are: EUTRAN, GERAN and UTRAN.

Important

In order to be backward compatible with old configuration, if a DSCP marking table is associated with GGSN service and not with the APN, then the one in GGSN service will be used. If table is associated in both GGSN service and APN, then the one on APN will take precedence.

Backward compatibility is maintained for existing DSCP marking and IPToS functionalities, with RAT-Type based DSCP marking.

Example

The following command associates a pre-configured QCI-QoS-Mapping table *dscp_mark_table1* with this APN.

```
associate qci-qos-mapping dscp_mark_table1
```

The following command configures DSCP marking for the RAT-Type EUTRAN

```
associate qci-qos-mapping dscp_mark_table rat-type eutran
```

authentication

Configures the APN's authentication parameters.

Product

GGSN

P-GW

PDG/TTG

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

authentication [[**msid-auth** | **imsi-auth** [**password-use-pco** | **username-strip-apn** | **prefer-chap-pco**] | **msisdn-auth** [**password-use-pco** | **username-strip-apn** | **username-append-apn** | **prefer-chap-pco**] | **eap initial-access-request** [**authenticate-authorize** | **authenticate-only**] | [**allow-noauth** [**pco-usernmae** { **chap | pap** }]] [**chap** *preference* [**convert-to-mschap**]] [**mschap** *preference*] [**pap** *preference*]]
default authentication

default

Sets the default authentication type for this APN. By default **allow-noauth** is the type for authentication for an APN.

msid-auth

Obsolete. Use **imsi-auth**.

imsi-auth

Default: Disabled.

Configures the APN to attempt to authenticate the subscriber based on their International Mobile Subscriber Identification (IMSI) number.

msisdn-auth

Default: Disabled.

Configures the APN to attempt to authenticate the subscriber based on their Mobile Station International Integrated Services Digital Network (MSISDN) number as described in the *Usage* section of this command.

username-strip-apn

Default: Disabled.

This keyword if enabled, either with **msisdn-auth** or **imsi-auth** strips the APN name from the user name *msisdn@apn* or *imsi@apn* received from AAA and makes the user name as *msisdn* or *imsi* respectively.

username-append-apn

Default: Disabled.

This keyword if enabled, works only with pap and chap options. If username-append-apn option enabled in authentication CLI, then apn name will be appended to the pco received username and same username will be used across all interfaces.

password-use-pco

Default: Disabled.

This keyword, if enabled, uses the password received through Protocol Configuration Options (PCO) from AAA for authentication.

prefer-chap-pco

Default: Disabled.

If this keyword along with msisdn-auth/imsi-auth is enabled, GGSN performs Challenge Handshake Authentication Protocol (CHAP) authentication, if CHAP parameters are received in Protocol Configuration Options (PCO). However, chap username would be constructed as *msisdn@apn* / *imsi@apn* and chap challenge, chap response parameters should be used as it is from CHAP parameters received in the PCO IE. If CHAP parameters are not received in the PCO IE of the CPC Request, GGSN does normal Password Authentication Protocol (PAP) authentication with PAP username as *msisdn@apn* / *imsi@apn* (ignoring any PAP username if received).

eap initial-access-request

Default: Enabled

Configures the type of initial access request to be used in Diameter EAP (Extensible Authentication Protocol) request. This feature is applicable to only Diameter-based AAA interface and not applicable to RADIUS or any other type of AAA interface.

authenticate-authorize

Default: Enabled

Configures the "authenticate and authorize" type of initial access request to be used in a Diameter EAP request.

authenticate-only

Default: Disabled

Configures the "authenticate only" type of initial access request to be used in a Diameter EAP request.

allow-noauth

Default: Enabled

Configures the APN to not perform authentication for PDP contexts as described in the *Usage* section.

pco-username

Default: Disabled

This option is used in conjunction with allow-noauth. It allows session to get established when PCO contains both pap and chap in authentication disabled case.

chap *preference*

Default: Disabled

Configures the APN to attempt to use CHAP to authenticate the subscriber as described in the *Usage* section of this command.

A *preference* must be specified in conjunction with this option. Priorities specify which authentication protocol should be attempted first, second, third and so on. It must be an integer from 1 through 1000. The lower the integer, the higher the preference.

convert-to-mschap

Default: Disabled

If enabled, the CHAP parameters received with the length of 49 bytes, the AAAmgr converts it to MSCHAP.

mschap *preference*

Default: Disabled

Configures the APN to attempt to use the Microsoft Challenge Handshake Authentication Protocol (MSCHAP) to authenticate the subscriber as described in the *Usage* section of this command.

A *preference* can be specified in conjunction with this option. Priorities specify which authentication protocol should be attempted first, second, third and so on. It must be an integer from 1 through 1000. The lower the integer, the higher the preference.

pap *preference*

Default: Disabled

Configures the APN to attempt to use PAP to authenticate the subscriber as described in the *Usage* section of this command.

A *preference* must be specified in conjunction with this option. Priorities specify which authentication protocol should be attempted first, second, third and so on. It must be an integer from 1 through 1000. The lower the integer, the higher the preference.

Usage Guidelines

Use this command to specify how the APN profile should handle PDP context authentication and what protocols to use (if any). The ability to configure this option is provided to accommodate the fact that not every MS will implement the same authentication protocols.

The authentication process varies depending on whether the PDP context is of type IP or PPP. Table given in this section describes these differences.

For IP PDP contexts, the authentication protocol and values will be passed from the SGSN as Protocol Configuration Options (PCOs) within the create PDP context PDU to the GGSN. The GGSN requires that the authentication protocol is specified by this command (with no regard to priority) and will use this information to authenticate the subscriber.

Table 1: Authentication Process Variances Between PDP Context Type

Authentication Mechanism	IP PDP Context Behavior	PPP PDP Context Behavior
allow-noauth	Allows the session even if the PCOs do not match any of the configured algorithms. If the there was no match and the **aaa constructed-nai authentication** parameter is enabled in the authentication context, the system attempts to determine a subscriber profile (via PAP with no password) using the subscriber's MSISDN as the username.	Allows the session with no authentication algorithm selected. If the **aaa constructed-nai authentication** parameter is enabled in the authentication context, the system attempts to determine a subscriber profile (via PAP with no password) using the subscriber's MSISDN as the username.

Authentication Mechanism	IP PDP Context Behavior	PPP PDP Context Behavior
chap	If also specified in the PCOs, this protocol will be used to authenticate the subscriber.	Attempts this protocol according to its configured priority. If accepted by the remote end of the PPP connection, this protocol will be used to provide authentication.
mschap	If also specified in the PCOs, this protocol will be used to authenticate the subscriber.	Attempts this protocol according to its configured priority. If accepted by the remote end of the PPP connection, this protocol will be used to provide authentication.
pap	If also specified in the PCOs, this protocol will be used to authenticate the subscriber. If this protocol is used is specified and the **allow-noauth** parameter is disabled, the system will attempt to use the APN's default username/password specified by the **outbound** command for authentication via PAP.	Attempts this protocol according to its configured priority. If accepted by the remote end of the PPP connection, this protocol will be used to provide authentication.
msid-auth	Obsolete. Use **imsi-auth**.	Obsolete. Use **imsi-auth**.
imsi-auth	Values in the PCOs are ignored. The subscriber's IMSI is used as the username for PAP authentication. No password is used.	The subscriber's IMSI is used as the username for PAP authentication. No password is used.
msisdn-auth	Values in the PCOs are ignored. The subscriber's MSISDN is used as the username for PAP authentication. No password is used.	Option not available.

Example

The following command would configure the system to attempt subscriber authentication first using MSCHAP, then CHAP, and finally PAP. Since the **allow-noauth** command was also issued, if all attempts to authenticate the subscriber using these protocols fail, then the subscriber would be still be allowed access.

```
authentication mschap 1 chap 2 pap 3 allow-noauth
```

To enable **imsi-auth** or **msisdn-auth**, the following command instances must be issued:

```
authentication imsi-auth
authentication msisdn-auth
```

authorize-with-hss

This command enables or disables subscriber session authorization per APN via a Home Subscriber Server (HSS) over an S6b Diameter interface. This feature is required to support the interworking of GGSN with P-GW and HA.

Product

P-GW

SAEGW

Privilege

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

authorize-with-hss [egtp[gn-gp-enabled] [s2b [gn-gp-enabled]][s2a [gn-gp-enabled] [report-ipv6-addr]][s5-s8 [gn-gp-enabled | gn-gp-enabled]] [report-ipv6-addr]| lma [s6b-aaa-group *aaa-group-name* **| report-ipv6-addr] | report-ipv6-addr]**
[default | no] authorize-with-hss

default | no

Disables the default authorization of subscriber over S6b interface. Resets the command to the default setting of "authorize locally" from an internal APN authorization configuration.

egtp

Enables S6b authorization for eGTP only.

gn-gp-disabled

Disables s6b authorization for 3G initial attach and GNGP handover.

gn-gp-enabled

Enables s6b authorization for 3G initial attach and GNGP handover.

s2b

Enables S6b authorization for eGTP S2b.

s2a

Enables S6b authorization for eGTP S2a.

s5-s8

Enables S6b authorization for eGTP S5S8.

lma [s6b-aaa-group *aaa-group-name*]

Enables S6b authorization for LMA only.

The keyword **s6b-aaa-group** *aaa-group-name* is used to enable the configuration of AAA group used for S6b authorization in PMIP P-GW.

Two AAA groups are defined within APN configuration, one for RADIUS and another one for Diameter. All the parameters required for RADIUS authentication and accounting will go under *radius_group*. Similarly, Diameter authentication parameters will go under *s6b_group*.



Important If the S6b AAA group is configured under both APN and P-GW service, the APN level configuration takes higher precedence.

report-ipv6-addr

Enables the IPv6 address reporting through Authorization-Authentication-Request (AAR) towards the S6b interface.

Usage Guidelines Use this command to enable/disable the authorization support per APN for subscriber over S6b interface, which is used between P-GW and the 3GPP AAA to exchange the information related to charging, GGSN discovery, etc.

bearer-control-mode

Enables or disables the bearer control mode for network controlled QoS (NCQoS) through this APN. It also controls the sending of an IE in GTP messages.

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

```
bearer-control-mode [ mixed | ms-only | none |
use-gx-avp-online-response-required[ prefer-local-value ] ]
default bearer-control-mode
```

default

Sets the bearer control mode to default mode of "none".

mixed

Default: Disabled.

This keyword indicates that the bearer will be controlled by User Equipment (UE) and network side (from GGSN) as well.

To enable network controlled QoS this option must be enabled.

ms-only

Default: Disabled.

This keyword indicates that the bearer will be controlled by the UE side.

none

Default: Enabled.

This keyword indicates that the system will not send any BCM mode information, BCM IE and BCM information in the protocol configuration option (PCO) IE within GTPC messages sent by the GGSN. This option is useful in networks where AGWs or firewalls do not support unknown optional IEs in GTP messages.

use-gx-avp-online-response-required

This keyword allows P-GW to function according to the behavior requested in Gx AVP OnlineResponseRequired or override-OnlineResponseRequired.

prefer-local-value

Default: Disabled.

This keyword indicates that the APN configured with "none" option for bearer control mode will not be overridden by any other interface (e.g. Gx interface towards PCRF). As a result it is ensured that BCM IE is never sent in GTP message.



Important When bearer control mode is set to "none" with the keyword set "prefer-local-value", even PCRF provided values will not override APN config and therefore sending of BCM mode IE and BCM in PCO IE in CPC Response is supressed.

Usage Guidelines

Use this command to enable the QoS through bearer control. This can be done either through the MS side or from both the GGSN and MS. To enable network requested QoS user need to enable "Mixed" mode for bearer control.

With this keyword the operator can control sending of BCM information in GTPC messages from the GGSN.

With MS-Only or Mixed options in this mode, the system sends the BCM information element in every Create PDP Context Response and Unknown PDP Context Request and Response message.

In some networks AGWs/Firewall drop/reject GTPC messages if there is an Unknown optional IE. To resolve this, the operator can use the "none" option to control sending of BCM IE and BCM information in the PCO IE within GTPC messages from the GGSN.

Example

The following command enables the bearer control from network and MS side for NCQoS.

```
bearer-control-mode mixed
```

backoff timer-value

Specifies a fixed value and a jitter to introduce randomness in the Backoff Timer value that is returned to the MME for different sessions. This helps prevent a session storm after the Backoff Timer expiry.

Important The APN Backoff Timer feature requires that the M2M license be enabled on the P-GW/SAEGW. Contact your Cisco account or support representative for licensing details.

Product

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

`[ no ] backoff timer-value` *`seconds`* **`[ jitter`** *`seconds`* **`]`**

no

Disables the backoff timer values.

backoff timer-value *seconds*

Specifies the backoff timer value, in seconds.

Valid entries are from 0 to 576000 seconds.

There is no default setting.

jitter *seconds*

Specifies the jitter value, in seconds.

Valid entries are from 0 to 1000 seconds.

There is no default setting.

Usage Guidelines

This command must be used with the **pdn-behavior lapi** command in *APN Configuration Mode*.

Example

The following command specifies a timer-value and jitter setting of 20 seconds:

backoff timer-value *20* **jitter** *20*

bearer-duration-stats

Enables or disables per QCI call duration statistics for dedicated bearers.

Product

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

[no] bearer-duration-stats qci { all |1|2|3|4|5|6|7|8|9 } +

no

Disables per QCI call duration statistics.

all

Configures QCI-based duration statistics for all QCI.

1|2|3|4|5|6|7|8|9|80|82|83

Configures bearer duration statistics for QCI .

+

More than one of the previous keywords can be entered within a single command.

Usage Guidelines

Use this command to enable or disable per QCI call duration statistics for dedicated bearers.

Example

The following command enables QCI-based duration statistics for all QCI:

bearer-duration-stats qci all

cc-home

Configures the home subscriber charging characteristics (CC) used by the GGSN when those from the SGSN will not be accepted.

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

```
cc-home { behavior bits | profile index }
default cc-home
```

default

Restores the cc-home parameter to its default setting of the following:

- **behavior bits:** 0x00
- **profile index:** 8

behavior *bits*

Specifies the behavior bit for the home subscriber charging characteristic. *bits* can be configured to any unique bit from 001H to FFFH (0001 to 1111 1111 1111 bin) where the least-significant bit corresponds to B1 and the most-significant bit corresponds to B12.

profile *index*

Specifies the profile index for the home subscriber charging characteristic. *index* can be configured to any integer value between 0 and 15. Default: 8



Important 3GPP standards suggest that profile index values of 1, 2, 4, and 8 be used for hot billing, flat rate billing, prepaid billing and normal billing, respectively. A single charging characteristics profile can contain multiple behavior settings.

Usage Guidelines

When the GGSN is configured to reject the charging characteristics sent by the SGSN for "home" subscribers, it uses the profile index specified by this command to determine the appropriate CCs to use.

Multiple behavior bits can be configured for a single profile index by ORing the bit strings together and converting the result to hexadecimal.

The properties of the actual CC profile index are configured as part of the GGSN service using the **cc profile** command. Refer to the *GGSN Service Configuration Mode* chapter of this reference for additional information on this command.

Example

The following command configures a behavior bit of 2 (0000 0000 0010) and a profile index of *10* for home subscribers charging characteristics:

```
cc-home behavior 2 profile 10
```

The following command configures the behavior bits *3* (0000 0000 0100) and 5 (0000 0001 0000 bin) and a profile index of *14* for home subscriber charging characteristics:

```
cc-home behavior 14 profile 14
```

cc-profile

This command selectively enables or disables the Gy sessions based on the Charging Characteristics (CC) profile of the subscriber.

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

```
cc-profile { cc_profile_index | any } { prepaid-prohibited |
credit-control-group cc_group_name }
no cc-profile cc_profile_index
```

no

This command allows you to specify a CC profile index value. Whatever the CC profile value that was set with **no** command will fall back to "**any**" CC profile behavior.

Note that this command will not have "any" option. The verbose configuration will display other valid CC profiles and an entry for "any".

cc_profile_index

Specifies the CC profile index.

cc_profile_index must be an integer from 0 through 15.

Note that one charging characteristic value can be mapped to only one credit-control-group/prepaid-prohibited configuration within one APN.

any

This keyword is applicable for any non-overridden cc-profile index. This keyword has the least priority over specific configuration for a CC profile value. So, configuring "any" CLI command will not override other specific configurations under APN.

prepaid-prohibited

Disables prepaid Gy session for the configured profile index.

cc_group_name

Specifies name of the credit control group as an alphanumeric string of 1 through 63 characters.

Creating different credit control groups enables applying different credit control configurations (DCCA dictionary, failure-handling, session-failover, Diameter endpoint selection, etc.) to different subscribers on the same system.

Usage Guidelines

Use this command to selectively enable or disable the Gy sessions towards OCS based on the Charging Characteristics (CC) profile of the subscriber. When the prepaid prohibited CLI command is configured, the Gy messages are not triggered for postpaid subscribers. This feature is enabled by default. If APN does not have a specific cc-profile configured, it will fall back to "any" CC profile behavior.



Important The existing **credit-control-group** command within APN configuration is obsolete in 17 and later releases. This functionality is available as part of the **cc-profile** command. Also, note that the backward compatibility support exists for the **credit-control-group** CLI command.

The Session controller stores/updates the APN configuration in the AAA manager. During the session setup, the session manager fills the CC value received in session authenticate request, and sends it to AAA manager. The AAA manager matches this against the locally stored APN configuration, and selects the desired credit-control-group/prepaid-prohibited configuration for the session. Then the session manager passes this credit-control-group/prepaid-prohibited information received from the AAA manager to ACS manager.

When the local authentication (session setup request) is done, the credit-control group with the matching charging-characteristic is selected and used. If there is no matching charging-characteristic configuration found for the credit-control group selection, then the default credit-control group for the APN is selected.

The CC based Gy Session Controlling feature is applicable only for the CC value received via GTP-Auth-Request, and during the session establishment. The CC value updated via AAA/PCRF after the session setup will not cause any change in already selected credit-control group. Once the credit-control group is selected after session setup, this feature is not applicable.

Example

The following command configures the CC value 2 as prepaid to disable Gy session:

```
cc-profile 2 prepaid-prohibited
```

cc-roaming

Configures the roaming subscriber charging characteristics (CC) used by the GGSN when those from the SGSN will not be accepted.

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

cc-roaming { **behavior** *bits* | **profile** *index* }
default cc-roaming

default

Restores the cc-roaming parameter to its default setting of the following:

- **behavior bits:** 0x00
- **profile index:** 8

behavior *bits*

Specifies the behavior bit for the roaming subscriber charging characteristic. *bits* can be configured to any unique bit from 001H to FFFH (0001 to 1111 1111 1111 bin) where the least-significant bit corresponds to B1 and the most-significant bit corresponds to B12.

profile *index*

Specifies the profile index for the roaming subscriber charging characteristic. *index* can be configured to any integer value between 0 and 15. Default: 8



Important 3GPP standards suggest that profile index values of 1, 2, 4, and 8 be used for hot billing, flat rate billing, prepaid billing and normal billing, respectively. A single charging characteristics profile can contain multiple behavior settings.

Usage Guidelines

When the GGSN is configured to reject the charging characteristics sent by the SGSN for "roaming" subscribers, it uses the profile index specified by this command to determine the appropriate CCs to use.

Multiple behavior bits can be configured for a single profile index by ORing the bit strings together and convert the result to hexadecimal.

The properties of the actual CC profile index are configured as part of the GGSN service using the cc profile command. Refer to the GGSN Service Configuration Mode chapter of this reference for additional information on this command.

Example

The following command configures a behavior bit 10 (0010 0000 0000) and a profile index of *10* for roaming subscriber charging characteristics:

```
cc-roaming behavior 200 profile 10
```

The following command configures the behavior bits 9 (0001 0000 0000) and 6 (0000 0010 0000) and a profile index of *14* for roaming subscriber charging characteristics:

```
cc-roaming behavior 120 profile 14
```

cc-sgsn

Specifies the source for charging characteristics (CC) - those configured locally or those received from the SGSN.

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

```
cc-sgsn { gx-returned | home-subscriber-use-GGSN | radius-returned |
roaming-subscriber-use-GGSN | visiting-subscriber-use-GGSN } +
cc-sgsn { use-GGSN behavior bits profile index[ 0...15 ] [ radius-returned {
accept-invalid | replace-invalid } ] | [ gx-returned { accept-invalid |
replace-invalid } ] }
default cc-sgsn
no cc-sgsn { { radius-returned | home-subscriber-use-GGSN |
roaming-subscriber-use-GGSN | visiting-subscriber-use-GGSN } + | [ use-GGSN
 ] [ radius-returned { accept-invalid | replace-invalid } ] | [ gx-returned
{ accept-invalid | replace-invalid } ] }
```

default cc-sgsn

Restores the cc-sgsn parameter to its default setting of the following:

- **home-subscriber-use-GGSN**: Disabled

- **roaming-subscriber-use-GGSN**: Disabled
- **visiting-subscriber-use-GGSN**: Disabled

no cc-sgsn

Causes the GGSN/P-GW to accept CCs from the SGSN(s) when the **no cc-sgsn** command is entered with all applicable keywords. Otherwise, **no cc-sgsn** can be used to turn off one or more of the GGSN/P-GW sources of CC.

- **roaming-subscriber-use-GGSN**
- **home-subscriber-use-GGSN**
- **roaming-subscriber-use-GGSN**
- **visiting-subscriber-use-GGSN**

Before entering **no cc-sgsn**, it is helpful to determine which CC sources have been configured. This can be done with either **show configuration** or **show apn name** in Exec Mode.

home-subscriber-use-GGSN

Configures the GGSN/P-GW to use the locally defined charging characteristics for home subscribers, as configured with the APN Configuration Mode **cc-home** command.

radius-returned

Configures the GGSN/P-GW to accept Gx returned charging characteristics for all subscribers for the APN.

gx-returned

Configures the GGSN/P-GW to accept charging characteristics returned from the RADIUS server for all subscribers for the APN.

accept-invalid

Configures the GGSN/P-GW to accept charging characteristics returned from PCRF for all subscribers for the APN. It always accepts CC with profile index zero.

replace-invalid

Configures GGSN/P-GW to accept charging characteristics returned from PCRF for all subscribers for the APN, except If CC profile index is zero, it will be replaced with default profile index. Default profile index is 8. This is the default behavior for gx-returned CC.

roaming-subscriber-use-GGSN

Configures the GGSN/P-GW to use the locally defined charging characteristics for roaming subscribers, as configured with the APN Configuration Mode **cc-roaming** command.

use-GGSN [behavior *bits*] profile *index[0...15]*

Configures the GGSN/P-GW to accept charging characteristics for all subscribers in the APN.

bits specifies the behavior bit for the charging characteristic. This variable can be configured to any unique bit from 001H to FFFH (0001 to 1111 1111 1111 bin) where the least-significant bit corresponds to B1 and the most-significant bit corresponds to B12.

index indicates which profile defined with **cc profile** in GGSN Service Configuration mode, the GGSN will use as a source for CCs. The index can be configured to an integer from 0 to 15.

The **use-GGSN** keyword can be entered alone or in conjunction with the **radius-returned** keyword. When entered, this keyword overrides the previous configuration using any of the home, roaming, and/or visiting keywords.

visiting-subscriber-use-GGSN

Configures the GGSN/P-GW to use the locally defined charging characteristics for visiting subscribers, as configured with the APN Configuration Mode **cc-visiting** command.

+

More than one of the above keywords can be entered within a single command.

Usage Guidelines

This command specifies whether or not CCs received from the SGSN will be accepted. If they are not accepted, the GGSN/P-GW will use those that have been configured locally.

The GGSN/P-GW's behavior can be configured for the following subscriber types:

- **Home:** Subscribers belonging to the same Public Land Mobile Network (PLMN) as the one on which the GGSN/P-GW is located.
- **Roaming:** Subscribers that are serviced by a an SGSN belonging to a different PLMN than the one on which the GGSN/P-GW is located.
- **Visiting:** Subscribers belonging to a different PLMN than the one on which the GGSN/P-GW is located.
- Any subscriber in the APN.

Example

The following command instructs the GGSN/P-GW to accept CCs for any subscriber in the APN based on local profile configurations of CCs.

```
cc-sgsn use-GGSN profile x
```

Assuming the CC source as defined with the previous command, the following command instructs the GGSN/P-GW to accept CCs supplied by the SGSN(s) and disables the acceptance of CCs supplied by the GGSN/P-GW for any subscriber within the APN:

```
no cc-sgsn use-GGSN
```

The following command instructs the GGSN/P-GW to accept CCs for any subscriber in the APN based on CC information returned from the RADIUS server. This command can be issued after the previous command to expand the possible sources.

```
cc-sgsn radius-returned
```

The following command disables the acceptance of CCs supplied by the GGSN/P-GW for visiting and roaming subscribers:

```
no cc-sgsn roaming-subscriber-use-GGSN visiting-subscriber-use-GGSN
```

cc-visiting

Configures the visiting subscriber charging characteristics (CC) used by the GGSN when those from the SGSN will not be accepted.

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

cc-visiting behavior *bits* **profile** *index*
default cc-visiting

default

Restores the cc-visiting parameter to its default setting of the following:

- **behavior bits:** 0x00
- **profile index:** 8

behavior *bits*

Specifies the behavior bit for the visiting subscriber charging characteristic. *bits* can be configured to any unique bit from 001H to FFFH (0001 to 1111 1111 1111 bin) where the least-significant bit corresponds to B1 and the most-significant bit corresponds to B12.

profile *index*

Specifies the profile index for the visiting subscriber charging characteristic. *index* can be configured to any integer value between 0 and 15. Default: 8

Important 3GPP standards suggest that profile index values of 1, 2, 4, and 8 be used for hot billing, flat rate billing, prepaid billing and normal billing, respectively. A single charging characteristics profile can contain multiple behavior settings.

Usage Guidelines

When the GGSN is configured to reject the charging characteristics sent by the SGSN for "visiting" subscribers, it uses the profile index specified by this command to determine the appropriate CCs to use.

Multiple behavior bits can be configured for a single profile index by ORing the bit strings together and convert the result to hexadecimal.

The properties of the actual CC profile index are configured as part of the GGSN service using the cc profile command. Refer to the GGSN Service Configuration Mode chapter of this reference for additional information on this command.

Example

The following command configures a behavior bit 7 (0000 0100 0000) and a profile index of 10 for visiting subscriber charging characteristics:

```
cc-visiting behavior 40 profile 10
```

The following command configures the behavior bits 1 (0000 0000 0001) and 12 (1000 0000 0000) and a profile index of 14 for visiting subscriber charging characteristics:

```
cc-visiting behavior 801 profile 14
```

content-filtering category

Enables or disables the specified pre-configured Category Policy Identifier for Category-based Content Filtering support.

Product

CF

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

content-filtering category policy-id*cf_policy_id*
no content-filtering category policy-id

no

Disables the previously configured category policy identifier for Content Filtering support to the APN. This is the default setting.

policy-id *cf_policy_id*

Applies the specified content filtering category policy ID, configured in the ACS Configuration Mode, to this APN.

cf_policy_id must be a category policy ID entered as an integer from 1 through 4294967295.

If the specified category policy ID is not configured in the ACS Configuration Mode, all packets will be passed regardless of the categories determined for such packets.

Important Category Policy ID configured through this mode overrides the Category Policy ID configured through **content-filtering category policy-id** command in the ACS Rulebase Configuration Mode.

Usage Guidelines Use this command to enter the Content Filtering Policy Configuration Mode and to enable or disable the Content Filtering Category Policy ID for an APN.

Important If Content Filtering Category Policy ID is not specified here the similar command in the ACS Rulebase Configuration Mode determines the policy.

Up to 64 different policy IDs can be defined.

Example

The following command enters the Content Filtering Policy Configuration Mode and enables the Category Policy ID *101* for Content Filtering support:

```
content-filtering category policy-id 101
```

credit-control-client

Configures the credit-control client parameters for subscribers who use this APN.

Product

GGSN

HA

IPSG

PDSN

P-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

```
credit-control-client { event-based-charging | override session-mode {
per-sub-session | per-subscriber } }
no credit-control-client { event-based-charging | override session-mode
}
default credit-control-client event-based-charging
```

no

Disables the configured setting.

default

Resets the command to its default setting of disabled.

event-based-charging

Enables event-based charging.

override session-mode { per-sub-session | per-subscriber }

Overrides the session-mode configured through the CLI command "**require ecs credit-control session-mode per-subscriber**" in Global Configuration mode so that different APN can operate in different modes. For example, one APN can be configured to work in per-subscriber mode, while another in per-sub-session mode.

This keyword is used to switch between subscriber level Gy and sub-session level Gy.



Important This CLI can be changed on the fly. The modified values will be reflected only in the new subscriber session.

The **no** command removes the override CLI and makes the APN fall back to the configuration specified through the CLI command "**require ecs credit-control session-mode per-subscriber**".

Usage Guidelines

Use this command to configure the credit-control client parameters for this APN.

This configuration should be enabled to report UE's PLMN, time zone and ULI changes through Event-based-Gy session. In the event that both Gy Online charging and Gy event reporting are enabled, the P-GW shall send only CCR-Update requests to the OCS and shall not send CCR-Event requests.

With the inclusion of this keyword **override session-mode ...** in 14.1 release, it is possible to seamlessly change the configuration from bearer level to APN level and vice-versa without requiring a system reboot.

Example

The following command enables event-based Gy support for the current APN:

```
credit-control-client event-based-charging
```

credit-control-group

Configures the credit control group to be used for subscribers who use this APN.



Important This command is obsolete in 17 and later releases. The functionality of this command is available as part of the **cc-profile** command in the APN Configuration mode. Refer to the **cc-profile** command in this chapter.

Product

GGSN

ACS

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

credit-control-group *cc_group_name* **[cc-profile** *cc_profile_index* **]**
no credit-control-group [*cc_group_name* **cc-profile** *cc_profile_index* **]**

no

Removes the previously configured credit control group from the APN configuration.

cc_group_name

Specifies name of the credit control group as an alphanumeric string of 1 through 63 characters.

Important Release 16 onwards, a maximum of up to four credit-control-group - charging-profile configurations are possible within one APN.

cc-profile *cc_profile_index*

Specifies the charging-characteristic preference for the credit-control-group.

For example, 1 for Hot Billing, 2 (Flat Rate), and 8 (Post-Paid)

cc_profile_index must be an integer from 0 through 15.

Note that one charging-characteristic value can be mapped to only one credit-control-group inside one APN.

Important The CLI command "**cc-sgsn**" within APN configuration mode, should be used cautiously as this will cause the charging-chars to be altered/modified.

Usage Guidelines

Use this command to configure the credit control group for this APN.

Creating different credit control groups enables applying different credit control configurations (DCCA dictionary, failure-handling, session-failover, Diameter endpoint selection, etc.) to different subscribers on the same system.

Without credit control groups, only one credit control configuration is possible on a system. All the subscribers in the system will have to use the same configuration.

In releases prior to 16, only one credit-control-group can be specified inside an APN. In 16 and later releases, the APN configuration is extended to include the Charging-Characteristic (CC) preference for the credit-control-group. This APN configuration is also extended to allow configuring additional credit-control-groups for each of the CC values. With this enhancement, the OCS selection can be done based on the CC value received via GTP request.

When the local authentication (session-setup-request) is done, the credit-control-group with the matching charging-characteristic will be selected, and used. If there is no matching charging-characteristic configuration found for the credit-control-group selection, then the default credit-control-group for the APN will be selected.

The CC based OCS selection feature is applicable only for the Charging-Chars value received via GTP-Auth-Request, and during the session-establishment. The Charging-Chars value updated via AAA/PCRF after the session setup will not cause any change in already selected "credit-control-group". Once the credit-control-group is selected (after session setup), this feature is not applicable.

APN configuration information is stored in AAA manager. Credit control group information from the APN configuration is filled during the session-authentication time, by AAA manager. So, AAA manager should be informed of the Charging-Characteristic value received at the time of Session-Authentication, so that the desired credit-control-group can be selected.

Thus, the operator has the added flexibility to choose different OCS charging servers based on their business logic. This could help multi-national operators to choose correct OCS servers based on countries for roaming subscribers.

Example

The following command configures a credit control group named *testgroup12* for the current APN:

```
credit-control-group testgroup12
```

daf-pdp-type

By configuring this command P-GW/GGSN can set different behavior of assigning PDN Type and return cause code when request for ipv4v6 PDN with DAF bit False is received.

Product

GGSN

P-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

```
daf-pdp-type { ipv4 | ipv6 } cause-code { network-preference |
single-address-bearer-only }
```

daf-pdp-type

Configures PDP type for requested IPv4v6 PDN with Dual Address Flag zero. Default PDP type is IPv6.

ipv4

Configures PDP type for this APN to be IPv4.

ipv6

Configures PDP type for this APN to be IPv6

ipv6

Configures PDP type for this APN to be IPv6.

cause-code

Configures GTP cause code for requested IPv4v6 PDN with Dual Address Flag zero. Default GTP cause code is single-address-bearer-only.

network-preference

New PDP type due to network preference.

single-address-bearer-only

New PDP type due to single address bearer only.

Usage Guidelines

By configuring this command P-GW/GGSN can set different behavior of assigning PDN Type and return cause code when request for ipv4v6 PDN with DAF bit False is received. If this command is not configured P-GW/GGSN it uses the default option of assigning ipv6 pdn type with return cause of 'New PDN Type due to single address bearer only'.

Example

The following command configures PDP type and GTP cause code for requested IPv4v6 PDN due to network preference.

```
daf-pdp-type ipv4 cause-code network-preference
```

data-tunnel mtu

Configures the Maximum Transmission Unit (MTU) for data sent on the IPv6 tunnel between the P-GW and the mobile node.

Product

P-GW

SAEGW

Privilege

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

data-tunnel mtu*bytes*
default data-tunnel mtu

default

Returns the command to the default value of 1500.

bytes

Specifies the MTU for the IPv6 tunnel between the P-GW and the mobile node. *bytes* must be an integer between 1280 and 2000. Default: 1500

Usage Guidelines

Use this command to set the MTU for data traffic on the IPv6 tunnel between the P-GW and the mobile node.

Example

The following command sets the MTU for IPv6 data traffic to *1400* bytes:

```
data-tunnel mtu 1400
```

data-tunneling ignore df-bit

Controls the handling of the DF (Don't Fragment) bit present in the user IPv4/IPv6 packet for tunneling used for the Mobile IP data path.

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

[default | no] data-tunneling ignore df-bit

default

Restores the data-tunneling parameter to its default setting of disabled.

no

Disables this option. The DF bit in the tunneled IP packet header is not ignored during tunneling. This is the default setting.

ignore df-bit

Ignores the DF bit in the tunneled IP packet header during tunneling. This is the default setting.

Usage Guidelines

Use this command to configure a user so that during Mobile IP tunneling the DF bit is ignored and packets are fragmented.

If this feature is enabled, and fragmentation is required for the tunneled user IPv4/IPv6 packet, then the DF bit is ignored and the packet is fragmented. Also the DF bit is not copied to the outer header.

In the GGSN, this command also affects the other L3 tunneling options, IP-in-IP and GRE, but does not affect L2TP tunneling.

Example

To enable fragmentation of a subscribers packets over a MIP tunnel even when the DF bit is present, enter the following command:

```
data-tunneling ignore df-bit
```

dcca origin endpoint

This command is obsolete. To configure the Diameter Credit Control Origin Endpoint, in the Credit Control Configuration Mode, use the **diameter origin endpoint** command.

dcca peer-select

Specifies the Diameter credit control primary and secondary host for credit control.

Product

GGSN

ACS

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

dcca peer-select peer *host_name* [**realm** *realm_name*] [**secondary-peer** *host_name*]
no dcca peer-select

no

Removes the previously configured Diameter credit control peer selection.

host_name

Specifies a unique name for the peer as an alphanumeric string of 1 through 63 characters that allows punctuation marks.

realm *realm_name*

Specifies the ream as an alphanumeric string of from 1 through 127 characters that allows punctuation marks. The realm may typically be a company or service name.

secondary-peer *host_name*

Specifies a back-up host that is used for fail-over processing as an alphanumeric string of from 1 through 63 characters. When the route-table does not find an AVAILABLE route, the secondary host performs fail-over processing.

Usage Guidelines

Use this command to select a Diameter credit control peer and realm.

Important This configuration completely overrides all instances of **diameter peer-select** that have been configured within the Credit Control Configuration Mode for an Active Charging Service.

Example

The following command selects a Diameter credit control peer named test and a realm of *companyx*:

dcca peer-select test realm companyx

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*

description

Allows you to enter descriptive text for this configuration.

Product

All

Privilege

Security Administrator, Administrator

Syntax Description

description *text*
no description

no

Clears the description for this configuration.

text

Enter descriptive text as an alphanumeric string of 1 to 100 characters.

If you include spaces between words in the description, you must enclose the text within double quotation marks (" "), for example, "AAA BBBB".

Usage Guidelines The description should provide useful information about this configuration.

dhcp context-name

Configures the name of the context on the system in which Dynamic Host Control Protocol (DHCP) functionality is configured.

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

```
[ no ] dhcp context-name name
```

no

Removes a previously configured context name.

name

Specifies the name of a context configured on the system in which one or more DHCP services are configured. *name* is an alphanumeric string of 1 through 79 characters that is case sensitive.

Usage Guidelines

If the APN is to support dynamic address assignment via DHCP (either the proxy or relay mode), this parameter must be configured to point the APN to the name of a pre-configured context on the chassis in which one or more DHCP services are configured.

The command can be used to identify a single DHCP service instance within the specified context to use to facilitate the address assignment.

Example

The following command configures the APN to look for DHCP services in a context called *dhcp-ctx:*

```
dhcp context-name dhcp-ctx
```

dhcp lease-expiration-policy

Configures the system's handling of PDP contexts whose DHCP assigned IP lease has expired.

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

`dhcp lease-expiration-policy { auto-renew | disconnect }`
`default dhcp lease-expiration-policy`

default

Restores the dhcp lease-expiration-policy parameter to its default setting of auto-renew.

auto-renew

Configures the system to automatically renew an IP address' lease when it is about to expire for PDP contexts facilitated by the APN. Default: Enabled

disconnect

Configures the system to automatically release the PDP context when the lease for the IP address associated with that context expires. Default: Disabled

Usage Guidelines

Use this command to specify the action the system is to take when leases for IP addresses for PDP contexts that it are currently facilitated by the current APN are about to expire.

Example

The following command causes the system to release PDP contexts associated with the current APN when the lease for their DHCP-assigned IP address expires:

`dhcp lease-expiration-policy disconnect`

dhcp service-name

Configures the name of a specific DHCP service to use when dynamically assigning IP addresses to PDP contexts using the Dynamic Host Control Protocol.

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

[no] dhcp service-name *service_name*

no

Removes a previously configured DHCP service name.

service_name

Configures the name of the DHCP service instance that is to be used by the current APN for the dynamic assignment of IP addresses to PDP contexts. The name can be an alphanumeric string of 1 through 63 characters that is case sensitive.

Usage Guidelines

Use this command to specify a pre-configured DHCP service instance that is to be used by the APN for IP address assignment when the Dynamic Host Control Protocol is used.

The name of the context in which the desired DHCP service is configured must be specified by the **dhcp context-name** command.

Example

The following command instructs the APN to use a DHCP service called *dhcp1*:

```
dhcp service-name dhcp1
```

dhcpv6 context-name

Configures the name of the context on the system in which DHCPv6 functionality is configured. If a DHCPv6 service is configured in the APN, this DHCPv6 context name is used to get an address

Product

GGSN

P-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

dhcpv6 context-name *ctxt_name*
[no] dhcp context-name

no

Removes a previously configured context name.

ctxt_name

Specifies the name of a context configured on the system in which one or more DHCPv6 services are configured. *ctxt_name* is an alphanumeric string of 1 through 79 characters that is case sensitive.

Usage Guidelines

If the APN is to support dynamic address assignment via DHCPv6, this parameter must be configured to point the APN to the name of a pre-configured context on the chassis in which one or more DHCPv6 services are configured.

The command can be used to identify a single DHCPv6 service instance within the specified context to use to facilitate the address assignment.

Example

The following command configures the APN to look for DHCPv6 services in a context called *dhcpv6-ctx:*

```
dhcpv6 context-name dhcpv6-ctx
```

dhcpv6 service-name

Specifies which DHCPV6 service to use, if the alloc-type is configured as dhcpv6-client or dhcpv6-relay.

Product

GGSN

P-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

```
[ no ] dhcpv6 service-name service_name server-profile dhcpv6-server-prof
client-profile dhcpv6-client-prof
```

no

Removes a previously configured DHCPv6 service name.

service_name

Configures the name of the DHCPv6 service instance that is to be used by the current APN for the dynamic assignment of IPv6 addresses to PDP contexts. The name can be an alphanumeric string of 1 through 63 characters that is case sensitive.

server-profile *dhcpv6-server-prof*

Specify the profile name for DHCPv6 Server profile.

client-profile *dhcpv6-client-prof*

Specify the profile name for DHCPv6 Client profile.

Usage Guidelines

Use this command to specify a pre-configured DHCPv6 service instance that is to be used by the APN for IPv6 address assignment when the Dynamic Host Control Protocol is used.

The name of the context in which the desired DHCP service is configured must be specified by the **dhcpv6 context-name** command.



Important Only one DHCPv6 service can be configured for an APN

Example

The following command instructs the APN to use a DHCPv6 service called *dhcpv6_svc*:

```
dhcp service-name dhcpv6_svc
```

dns

Configures the Domain Name Service (DNS) servers that will be used by the APN for PPP.

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

```
dns { primary | secondary } { address }
no dns { primary | secondary } [ dns_address ]
```

no

Deletes a previously configured DNS server.

primary

Configures the primary DNS server for the APN.

secondary

Configures the secondary DNS server for the APN. Only one secondary DNS server can be configured.

address

Configures the IP address of the DNS server expressed in IPv4 dotted-decimal notation.

Default: primary = 0.0.0.0, secondary = 0.0.0.0

dns_address

Specifies the IP address of the DNS server to remove, expressed in IPv4 dotted-decimal notation.

Usage Guidelines

DNS servers are configured on a per-APN profile basis. This allows each APN profile to use specific servers in processing PDP contexts.

The configured DNS IP addresses are relayed to the subscriber within IPCP if the PDP type is PPP, or as PCOs (Protocol Configuration Options) if the PDP type is IP.

The DNS can be specified at the APN level in APN configuration as well as at the Context level in Context configuration mode with **ip name-servers** command, 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 has the third preference.
4. DNS values configured at context level with **ip name-servers** command has the last preference.



Important The same preference would be applicable for the NBNS (NetBIOS Name Service) servers to be negotiated via ICPC (Initial Connection Protocol Control) with the LNS (L2TP Network Server).

Example

The following commands configure a primary DNS server address of *192.168.100.3* and a secondary DNS server address of *192.168.100.4*:

```
dns primary 192.168.100.3
dns secondary 192.168.100.4
```

egtp

Enables/disables the Overcharging Protection feature on an APN service.

Product

P-GW

SAEGW

Privilege

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

egtp overcharge-protection [drop-all | transmit-all]
{ default | no | remove } egtp overcharge-protection

default

Disables overcharging protection.

no

Disables overcharging protection.

remove

Removes overcharging protection configuration.

overcharge-protection [drop-all | transmit-all]

drop-all: Configures overcharging protection to drop all packets received in LORC.

transmit-all: Configures overcharging protection to send all packets received in LORC mode to S-GW.

Usage Guidelines

Use this command to enable/disable the Overcharging Protection feature on an APN service.

When Overcharging Protection feature is configured at both P-GW service and APN, configuration at APN takes priority.



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

Example

The following command configures overcharging protection to drop all packets received in LORC"

egtp overcharge-protection drop-all

egtpc-qci-stats

Enables/disables an APN candidate list for the **apn-expansion** bulkstats schema.

Product

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

`[ no ] egtpc-qci-stats { all | qci1 | qci2 | qci3 | qci4 | qci5 | qci6 | qci7 | qci8| qci80 | qci82 |qci83| qci9 } +`
`default egtpc-qci-stats`

default

Disables an APN candidate list for the apn-expansion bulkstat schema.

no

Disables APN candidate list(s) for the apn-expansion bulkstat schema.

all

Configure apn-qci-egtpc statistics for all QCI.

qci1

Configure apn-qci-egtpc statistics for QCI 1.

qci2

Configure apn-qci-egtpc statistics for QCI 2.

qci3

Configure apn-qci-egtpc statistics for QCI 3.

qci4

Configure apn-qci-egtpc statistics for QCI 4.

qci5

Configure apn-qci-egtpc statistics for QCI 5.

qci6

Configure apn-qci-egtpc statistics for QCI 6.

qci7

Configure apn-qci-egtpc statistics for QCI 7.

qci8

Configure apn-qci-egtpc statistics for QCI 8.

qci80

Configure apn-qci-egtpc statistics for QCI 80.

qci82

Configure apn-qci-egtpc statistics for QCI 82.

qci83

Configure apn-qci-egtpc statistics for QCI 83.

qci9

Configure apn-qci-egtpc statistics for QCI 9.

+

More than one of the above keywords can be entered within a single command.

Usage Guidelines

Use this command to enable/disable an APN candidate list for the APN Expansion bulkstats schema. You can enable which APN collects granular statistics using this configuration. In those granular statistics, it is possible to decide which particular statistics to collect.



Caution Supporting more granular statistics/bulkstats on APN (up to 12 APNs are supported) has an impact on system performance. Statistics need to be obtained at regular intervals for a few minutes. Each of these retrievals can lead to gigabytes of information being gathered and consolidated. Due to this issue, granular bulkstats collection is restricted/controlled.

See the *APN Expansion Schema Statistics* chapter in the *Statistics and Counters Reference* for detailed information on these bulkstats.

Example

The following command configures all QCI bulkstats in the apn-expansion schema.

```
egtpc-qci-stats all
```

ehrpd-access

Configures the P-GW to exclude IPv6 traffic from being delivered to UEs, accessing PDNs from the eHRPD network that do not have IPv6 capabilities.

Product

P-GW

SAEGW

Privilege

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

[default | no] ehrpd-access drop-ipv6-traffic

[default | no]

Resets this command to its default setting of disabled.

drop-ipv6-traffic

Excludes IPv6 traffic from being delivered to UEs, accessing PDNs from the eHRPD network that do not have IPv6 capabilities.

Usage Guidelines

Use this command to exclude IPv6 traffic from being delivered to UEs on the eHRPD network that do not have IPv6 capabilities.

emergency-apn

Configures this APN as an emergency APN for Voice over LTE (VoLTE) based E911 support.

Product

GGSN

P-GW

SAEGW

Privilege

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

[default | no] emergency-apn

[default | no]

Resets this command to its default setting of disabled.

Usage Guidelines

Use this command to configure this APN as an emergency APN for VoLTE based E911 support. With this support, a UE is able to connect to an emergency PDN and make Enhanced 911 (E911) calls while providing the required location information to the Public Safety Access Point (PSAP).

E911 is a telecommunications-based system that is designed to link people who are experiencing an emergency with the public resources that can help. This feature supports E911-based calls across the LTE and IMS networks. In a voice over LTE scenario, the subscriber attaches to a dedicated packet data network (PDN) called EPDN (Emergency PDN) in order to establish a voice over IP connection to the PSAP. Both signaling and RTP media flow over a dedicated emergency bearer. Additionally, different than normal PDN attachment that relies on AAA and PCRF components for call establishment, the EPDN attributes are configured locally on the P-GW, which eliminates the potential for emergency call failure if either of these systems is not available.

end

Exits the current configuration mode and returns to the Exec mode.

Product All

Privilege Security Administrator, Administrator

Syntax Description **`end`**

Usage Guidelines Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product All

Privilege Security Administrator, Administrator

Syntax Description **`exit`**

Usage Guidelines Use this command to return to the parent configuration mode.

firewall policy

Enables or disables Stateful Firewall support for the APN.

Product All

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

```
firewall policy firewall-required
{ default | no } firewall policy
```

no

Disables Stateful Firewall support for this APN.

default

Configures the default setting for Stateful Firewall support.

Default: Disabled

Usage Guidelines

Use this command to enable or disable Stateful Firewall support for this APN.

Important This command is only available in StarOS 8.0. In StarOS 8.1 and later, this configuration is available in the ACS Rulebase Configuration Mode.

Important Unless Stateful Firewall support for this APN is enabled using this command, firewall processing for this APN is disabled.

Important If firewall is enabled, and the rulebase has no firewall configuration, Stateful Firewall will cause all packets to be discarded.

Example

The following command enables Stateful Firewall support for an APN:

```
firewall policy firewall-required
```

The following command disables Stateful Firewall support for an APN:

```
no firewall policy
```

fw-and-nat policy

Specifies the Firewall-and-NAT policy to be used for subscribers who use this APN.

Product

eWAG

PSF

NAT

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

fw-and-nat policy *fw_nat_policy*
{ default | no } fw-and-nat policy

default

Configures the default setting.

Default: The default Firewall-and-NAT policy configured in the rulebase is used for subscribers who use this APN.

no

Disables Firewall and NAT for the APN.

fw_nat_policy

Specifies the Firewall-and-NAT policy for the APN as an alphanumeric string of 1 through 63 characters. Note that this policy will override the **default Firewall-and-NAT policy** configured in the ACS rulebase.

Usage Guidelines

Use this command to configure the Firewall-and-NAT policy for the APN. Note that the policy configured in the subscriber mode will override the default policy configured in the ACS rulebase. If a policy is not configured in the subscriber mode, the default policy configured in the ACS rulebase will be used.

Important This command is customer-specific and is only available in StarOS 8.1.

Important This customer-specific command must be used to configure the Policy-based Firewall-and-NAT feature.

Example

The following command configures a Firewall-and-NAT policy named *standard* for the APN:

```
fw-and-nat policy standard
```

gsm-qos negotiate

Enables negotiation of the QoS Reliability Class attribute based on the configuration provided for Service Data Unit (SDU) Error Ratio and Residual Bit Error Ratio (BER) attributes in the 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

gsm-qos negotiate sdu-error-ratio *sdu-error-ratio-code* [**residual-ber** *residual-ber-code*]
[**no**] **gsm-qos negotiate sdu-error-ratio** [*sdu-error-ratio-code* [**residual-ber** *residual-ber-code*]]

no

Disables negotiation of the QoS Reliability Class attribute.

sdu-error-ratio *sdu-error-ratio-code*

Enables the negotiation of the QoS Reliability Class attribute based on Service Data Unit (SDU) Error Ratio attributes. *sdu-error-ratio-code* corresponds to distinct SDU Error ratio values within an integer range of 1 to 7.

residual-ber *residual-ber-code*

Enables the optional configuration of negotiation of the QoS Reliability Class attribute based on Residual Bit Error Ratio (BER) attributes. *residual-ber-code* corresponds to distinct Residual Bit Error Ratio values within an integer range of 1 to 9.

Usage Guidelines

This command configures the QoS attribute Reliability Class to be negotiated based on the configuration provided for SDU Error Ratio and Residual BER attributes. The derived Reliability Class and the configured values for SDU Error Ratio and Residual BER are sent back in CPC and UPC response.

The mapping for *sdu-error-ratio-code* is as follows:

Code	Value
1	10-2
2	7*10-3
3	10-3
4	10-4
5	10-5
6	10-6
7	10-1

Residual BER needs to be specified when SDU Error Ratio is set to codes 1, 2, 3 or 7 (Or, SDU Error Ratio is intended to be set to a value greater than 5*10-4), for determining the Reliability Class QoS attribute.

Otherwise, the Residual BER value received in the Create PDP context request QoS (or UPC request) would be used. The mapping for *residual-ber-code* is as follows:

Code	Value
1	5*10-2
2	10-2
3	5*10-3
4	4*10-3
5	10-3
6	10-4
7	10-5
8	10-6
9	6*10-8

Example

The following commands configures the negotiation of QoS attribute Reliability Class based on Service Data Unit (SDU) Error Ratio *3* attributes in the APN:

```
gsm-qos negotiate sdu-error-ratio 3
```

gtpp group

Enables a configured GTPP server group to an APN for CGF accounting functionality.



Important In releases prior to 11.0, only one GTPP group is allowed to be configured per APN. Releases 11.0 through 15.0, this CLI can be used to configure up to a maximum of 32 GTPP groups. In 16.0 and later releases, this CLI allows the user to configure only up to six GTPP groups.

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

gtpp group *group_name* [**accounting-context** *ac_context_name*]
default gtpp group
no gtpp group *group_name*

no

Removes all the configured GTPP groups for the specific APN.

group_name

Specifies the name of server group that is used for authentication/accounting for specific APN. *group_name* must be an alphanumeric string of 1 to 63 characters. It must be identical to the one configured earlier within the same APN context.

Important In Release 11.0 and later, if you have mistakenly configured a GTPP group, you should remove the initially configured group and configure the new desired group. However, in Releases prior to 11.0, there is no need to remove the incorrect configuration; instead you can directly reconfigure the desired GTPP group.

Important If a GTPP group entry is invalid, this GTPP group will be ignored and the next valid GTPP group in the APN will be used. If no valid GTTP group exists, then the default GTPP group in the accounting context specified by the GGSN service will be used.

accounting-context *ac_context_name*

Specifies the name of an accounting context on the system that processes accounting for PDP contexts handled by this GGSN service for accounting to specific APN.

ac_context_name must be an alphanumeric string of 1 through 79 characters that is case sensitive.

Note that if an accounting context is not specified here, the system uses the GGSN service context or the context configured by the **accounting context** command in the GGSN Service Configuration mode.

Usage Guidelines

This feature provides the GTPP server configuration parameters under a GTPP group node. Instead of having a single list of servers per context, this feature configures multiple server groups within a context and applies individual an GTPP server group for subscribers in that context. Each server group consists of a list of CGF (Charging Group Function) accounting servers.

In case no GTPP group is applied for the said APN or default APN template, then the default GTPP server group available at the context level is applicable for accounting of a specific APN.

Important When multiple GTPP groups are applied to the same APN, the load will be shared across these GTPP groups. Sessions for this APN will use all the configured GTPP groups in a round robin fashion.

Once a GTPP group is selected for a subscriber session, the GTPP group will never change under any circumstances. A request is initially sent to primary CGF server configured in that group. When the primary fails to respond, the request is sent to secondary CGF server.

The process of failover from primary to secondary is per the 3GPP standards. Multiple GTPP groups configuration is actually supported only for load sharing of sessions within an APN and not used for failover. When all CGFs are down in a GTPP group, the requests are archived either in hard disk or main memory depending on whether or not streaming is enabled.

The AAA proxy allocates a lot of memory on a per GTPP group basis statically regardless of the usage. So if the number of GTPP groups is reduced to around 3 then the issue with the AAA proxy going to warn memory state will not be observed.

In releases prior to 16.0, up to a maximum of 32 GTPP groups were allowed to be configured per APN. In 16.0 and later releases, there is a limit of configuring only up to six GTPP groups per APN. In case customers are using more than six GTPP groups, the AAAProxy will use more memory than is supported and will be in "warn" state of memory. With the reduction in the number of GTPP groups configured, there will no CDR loss due to AAA proxy kill as CDRs are archived in AAA manager when AAA proxy goes to warn state.

Example

The following command applies a previously configured GTPP server group named *star1* to an APN within the specific context:

```
gtpp group star1
```

The following command disables the applied GTPP server group for the specific APN:

```
no gtpp group star1
```

gtpp secondary-group

Enables or associates a pre-configured secondary GTPP server group to an APN for CGF (Charging Group Function) accounting functionality. By default it is disabled.

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

gtpp secondary-group *group_name* [**accounting-context** *actt_ctxt_name*]
[**default** | **no**] **gtpp secondary-group** *group_name*

default

Default: Enabled

Restores the default mode for secondary GTPP group for APN template.

no

Disables the configured/associated GTPP secondary group for specific APN.

group_name

Specifies the name of secondary GTPP server group that is used as an alternate for the primary GTPP group associated with a specific APN for storage of GTPP messages. *group_name* must be an alphanumeric string of 1 through 63 characters. It must be the same name as configured earlier within the same APN context.

accounting-context *actt_ctxt_name*

Specifies the name of an accounting context on the system that processes accounting for PDP contexts handled by this GGSN service for accounting to a specific APN.

actt_ctxt_name specifies the name of the context to be used for accounting as an alphanumeric string of 1 through 79 characters that is case sensitive.

Note that if an accounting context is not specified here, the system uses the GGSN service context or the context configured by the **accounting context** command in the GGSN Service Configuration mode.

Usage Guidelines

Use this feature to provide the secondary GTPP server group support for an APN.

When the secondary GTPP group is configured with this command, the GTPP messages will also be mirrored to the secondary servers.

This secondary group configuration is ignored, if the configured *group_name* is the same as the primary group. It will also be ignored, if the configured GTPP *group_name* and/or accounting context *ac_context_name* is invalid. In such cases, the call will be established successfully (unlike the primary group configuration where the call drops).

In the absence of a configured *ac_context_name* context, the GGSN service context is chosen by default.

The secondary group messages are low priority and thus are purged when there is no room for the new messages.

For more information on GTPP group, refer the description of the **gtpp group** command.

Example

The following command applies a previously configured GTPP server group named *star2* to as secondary GTPP group to an APN within the specific context:

```
gtpp secondary-group star2
```

The following command disables the applied secondary GTPP server group for the specific APN:

```
no gtpp secondary-group star2
```

idle-timeout-activity

Configures a session idle-timeout to be reset with uplink packets only, or with both uplink and downlink packets.

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

[no] idle-timeout-activity ignore-downlink
default idle-timeout-activity

default

Sets or restores the command to the default setting.

ignore-downlink

Sets the system to ignore the downlink traffic for consideration as activity for idle-timeout.

Usage Guidelines

If **idle-timeout-activity ignore-downlink** is configured, the downlink (network to subscriber) traffic will not be used to reset the idle-timeout. Only uplink (subscriber to network) packets will be able to reset the idle-timeout.

By default, **ignore-downlink** is negated by the **no** command so downlink traffic is also used to reset the idle-timeout.

Example

The following command causes both uplink and downlink traffic to reset a session idle-timeout:

default idle-timeout-activity

The following command causes the session idle-timeout to be reset with only uplink packets:

idle-timeout-activity ignore-downlink

ignore-alt-config

Configures preference to APN/AAA-defined behavior/parameters. If the parameters are not defined in APN/AAA, they will not be provisioned from any other source/configuration in the system, even if they are available there.

Product

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

`[ no ] ignore-alt-config { no-dns | no-s6b }`

no

Disables DNS server address preference or S6b authentication on a per-APN level.

no-dns

Gives preference to DNS server address configured in APN. If name server addresses is not found in APN configuration, it will not be provisioned from SGi context, even if it is configured there.

no-s6b

Enables/disables S6b authentication on a per-APN level.

Ignores alternate service-level configuration for S6b authorization when S6b authorization is disabled at APN.

Usage Guidelines

Use this command to enable/disable DNS server address preference or S6b authentication on a per-APN level.

Important Configuration in APN will take precedence over configuration in P-GW service configuration.

Example

The following command to give preference to DNS server address configured in APN:

`ignore-alt-config no-dns`

ikev2 tsr

Configures the Traffic Selector responder (TSr) negotiation behavior during IKEv2 Security Association (SA) establishment.

Product

PDG/TTG

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 `[ default ] ikev2 tsr { wildcard | user-specified }`

default

Specifies the default behavior, which is wildcard TSr negotiation.

wildcard

Specifies that during TSr negotiation, the PDG/TTG always returns an any-to-any IP address range, an any-to-any port range, and allows any protocol, irrespective of the traffic selector ranges received from the UE. This is the default behavior.

user-specified

Specifies that during TSr negotiation, the PDG/TTG responds to each UE request with the UE-specified IP address ranges. This enables split tunneling on the PDG/TTG, and enables the UE to tunnel only a specified traffic range to the PDG/TTG and send other traffic directly out the WLAN.

Usage Guidelines Use this command to specify the TSr negotiation behavior on the PDG/TTG.

Example

The following command enables user-specified TSr negotiation on the PDG/TTG:

```
ikev2 tsr user-specified
```

ims-auth-service

Applies an IMS (IP Multimedia Subsystem) authorization service to a subscriber through APN for Gx interface support and functionality.

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 `[ no ] ims-auth-service auth_service_name`

no

Disables the applied IMS authorization service for a specific APN.

auth_service_name

Specifies the name of the IMS authorization service name that is used for Gx interface authentication for a specific APN. *auth_service_name* must be a alphanumeric string of 1 through 63 characters preconfigured within the same context as this APN.

Usage Guidelines

This feature provides the IMS authorization service configuration for Gx interface in IMS service node.

Example

The following command applies a previously configured IMS authorization service named *gx_interface1* to an APN within the specific context:

```
ims-auth-service gx_interface1
```

The following command disables the applied IMS authorization service *gx_interface1* for the specific APN:

```
no ims-auth-service gx_interface1
```

iot-rate-control

Configures APN Rate Control attributes for all PDNs of the APN.

Important The APN Rate Control for CIoT Devices is a license-controlled feature. Contact your Cisco Account Representative for more information.

Product

C-SGN

P-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

```
iot-rate-control time-unit { unrestricted | mins | hours | days | week }
 downlink packet-count dl_packet_count uplink packet-count ul_packet_count aer
 aer_value
no iot-rate-control
```

no

Disables the APN rate control.

time-unit { unrestricted | mins | hours | days | week }

unrestricted: Applies the mode of time-unit as unrestricted.

mins: Applies the mode of time-unit in minutes.

hours: Applies the mode of time-unit in hours.

days: Applies the mode of time-unit in days.

week: Applies the mode of time-unit in weeks.

downlink

Applies the APN Rate Control in the downlink direction.

packet-count *dl_packet_count*

Specifies the allowed number of packets. The *dl_packet_count* must be an integer ranging from 0 through 16777215. Integer 0 disables rate control on downlink direction.

uplink

Applies the APN Rate Control in the uplink direction.

packet-count *ul_packet_count*

Specifies the allowed number of packets. The *ul_packet_count* must be an integer ranging from 0 through 16777215. Integer 0 disables rate control on uplink direction.

aer *aer_value*

Specifies the number of Additional Exception Reports (AER) in uplink direction. The *aer_value* must be an integer ranging from 1 through 65535.

Usage Guidelines

APN Rate Control allows Home Public Land Mobile Network (HPLMN) operators to control the amount of user data sent in Downlink (DL) and Uplink (UL). Use this command for policing the user data on a maximum number of user data packets per time-unit, and/or maximum number of user data octets per time-unit, for both DL and UL.

Example

The following command sets the mode of time-unit in minutes with the allowed downlink packet-count as 1200, uplink packet-count as 2500, and 4000 AER in uplink direction:

```
apn-rate-control time-unit 1 downlink packet-count 1200 uplink packet-count
 2500 aer 4000
```

ip access-group

Configures an IPv4/IPv6 access group for the current APN profile.

Product

ACS

eWAG

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

ip access-group *acl_group_name* **[in | out] [fallback-enabled]**
[no] ip access-group *acl_group_name* **[in | out]**

no

Removes a previously configured IPv4/IPv6 access group association.

acl_group_name

Specifies the name of the IPv4/IPv6 access group. *acl_group_name* is a previously configured ACL group expressed as an alphanumeric string of 1 to 79 characters.

in | out

Default: both (in and out)

Specifies the access-group as either inbound or outbound by the keywords **in** and **out**, respectively.

fallback-enabled

When invalid ACL is received from RADIUS during Context Activation, ACL in this APN will be applied so there is no loss of CDR or missing charging information.

By default, ACL fallback is disabled.

Usage Guidelines

Use this command to apply a single IPv4/IPv6 access control list to multiple subscribers via this APN for inbound or outbound IPv4/IPv6 traffic.

If no traffic direction is specified, the selected access control list will be applied to both directions.

Run command without **fallback-enabled** option to disable ACL fallback for a previously configured ACL applied to a particular APN.

Example

The following command associates the *sampleipv4Group* access group with the current APN profile for both inbound and outbound access.

```
ip access-group sampleipv4Group
```

The following command removes the outbound access group flag for *sampleipv4Group*.

```
no ip access-group sampleipv4Group out
```

ip address alloc-method

Configures the method by which this APN will obtain IP addresses for PDP contexts.

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

```
ip address alloc-method { dhcp-proxy [ allow-deferred ] [ prefer-dhcp-options ] | dhcp-relay | local [ allow-deferred ] | no-dynamic [ allow-deferred ] } [ allow-user-specified ]
default ip address allocation-method
```

default

Restores the APN ip parameters to the following default settings.

dhcp-proxy

Default: Disabled

Configures the APN to assign an IP address received from a DHCP server.

Important If this option is used, the system's DHCP parameters must be configured.

dhcp-relay

Configures the APN to forward DHCP packets received from the MS to a DHCP server. Default: Disabled

Important If this option is used, the system's DHCP parameters must be configured.

local

Configures the APN to allocate IP addresses from a pool configured in the destination context on the system. Default: Enabled

Important If this option is used, the name of the IP address pool from which to allocate addresses must be configured using the **ip address pool-name** command. If no pool name is specified, the system will attempt to allocate an address from any public pool configured in the destination context.

Important In the case of IPv6 , if the pool name is configured in an APN, then the call is rejected even if a static address is sent by the UE.

no-dynamic

Disables the dynamic assignment of IP addresses to PDP contexts using this APN. Default: Disabled

If a PDP context needing an IP address is received by an APN with this option enabled, it will be rejected with a cause code of 220 (Unknown PDP address or PDP type).

prefer-dhcp-options

If this keyword is specified with **dhcp-proxy** for IP address allocation configuration, the GGSN will prefer DHCP-supplied parameters over values provided by AAA server or by local configuration. This keyword controls the following parameters:

- primary and secondary Domain Name Server (DNS) addresses
- primary and secondary NetBIOS Name Server (NBNS) addresses

These values will be sent out in the PCO IE of a GTP Create PDP Response Message whenever the MS Requests them in A Create PDP Request Message.

Default: Disabled

Important This keyword is available only with dhcp-proxy ip allocation method as this functionality is implemented only for GGSN acting as DHCP proxy.

By default, this functionality is disabled. Hence, DNS and NBNS values received from a DHCP server will not be considered by the GGSN.

allow-deferred

Enables support for P-GW deferred address allocation. Default: Disabled

allow-user-specified

Enables support for PDP contexts requesting the use of specific (static) addresses. Default: Enabled

Important If this option is not enabled, PDP contexts requesting the use of a static address will be rejected with a cause code of 220 (Unknown PDP address or PDP type).

Usage Guidelines

Use this command to configure the method by which the APN profile will assign IP addresses to PDP contexts.

When the PDP context is being established and the APN name is determined, the system will examine the APN's configuration profile. Part of that procedure is determining how to handle IP address allocation. The figure in the Example section below displays the process used by the system to determine how the address should be allocated.

Example

The following command configures the APN to dynamically assign an address from a DHCP server and reject PDP sessions with static IP addresses:

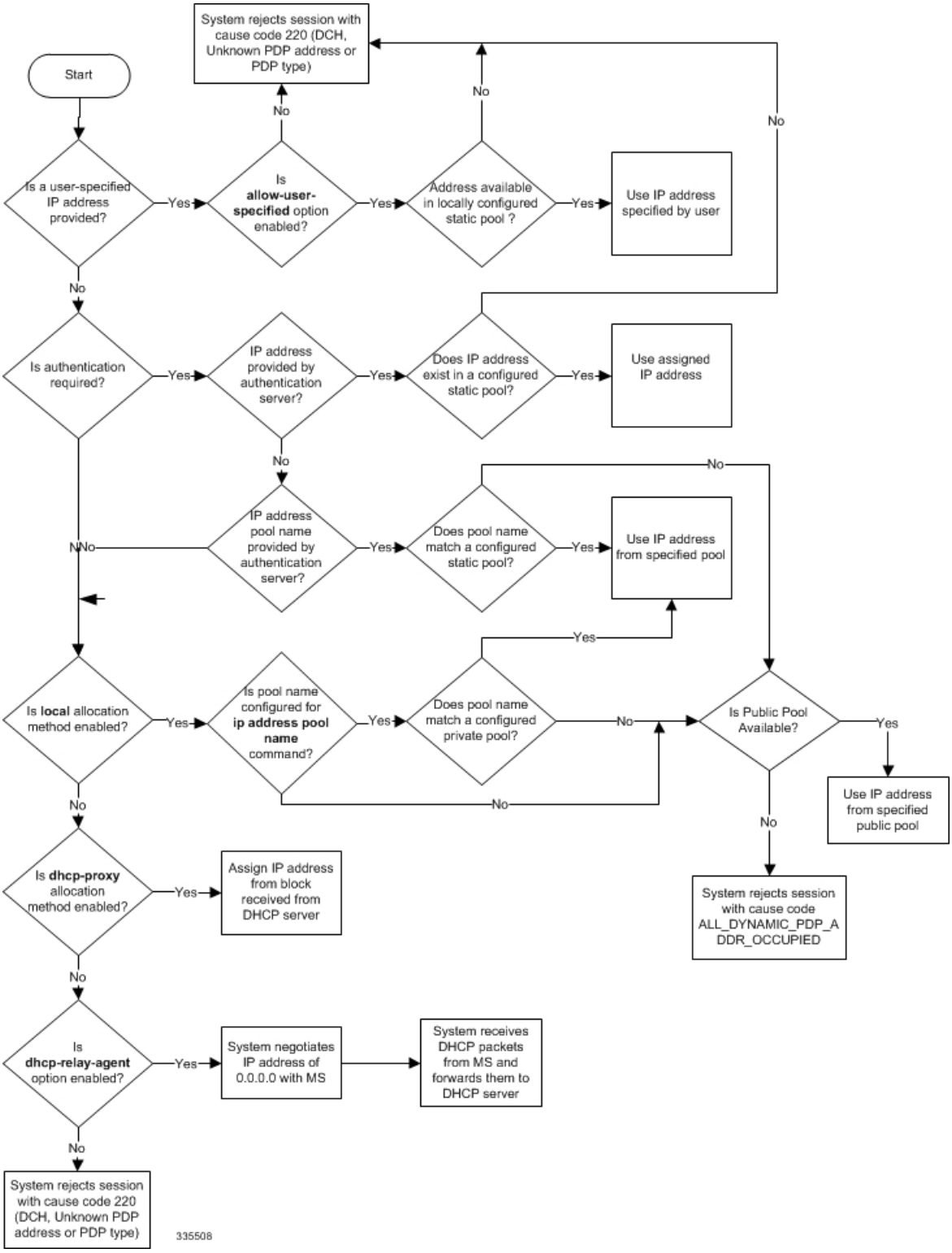
```
ip address alloc-method dhcp-proxy
```

The following command configures the APN to reject sessions requesting dynamically assigned addresses and only allow those with static addresses:

```
ip address alloc-method no-dynamic allow-user-specified
```

The following figure provides the IP address allocation process:

Figure 1: IP Address Allocation Process



ip address pool

Configures the name of an IP address pool configured on the system from which to assign an address for a PDP context.

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)#policy_name
```

Syntax Description

```
[ no ] ip address pool name pool_name
```

no

Removes a previously configured pool name.

pool_name

Specifies the name of the pool configured on the system from which an IP address will be assigned. The name is expressed as an alphanumeric string of 1 through 31 characters that is case sensitive.

Usage Guidelines

If the **ip address alloc-method** command is configured to allow the assignment of IP addresses from a local pool configured on the system. It command instructs the system as to which pool should be used.

The pool specified by this command must be a pool configured in the destination context on the system. Please refer to the **ip pool** command in the *Context Configuration Mode Commands* chapter for information on configuring IP address pools.

Multiple APNs can use the same IP address pool if required. In addition, this command could be issued multiple times to allow a single APN to use different address pools.

Caution From 14.0 onward for configuration of multiple IP pool in an APN, GGSN expects Framed-IP-Address and Framed-Pool from RADIUS.

Caution In pre-release 14.0, the maximum number of IP pools in an APN is 16 for static and dynamic type of pool. From 14.0 onward this limit has been changed for static address allocation to 1 and out of the maximum 16 pools which can be configured under a particular APN, the first IP pool should be a static pool, which is the only working static pool from an APN.

Example

The following command configures the system to use a pool named *private_pool1* for address allocation:

```
ip address pool private_pool1
```

ip address pool-exhaust-action

Configures the behavior to accept/reject a call if the IPv4 address pool is exhausted.

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

ip address pool-exhaust-action { **ipv6-accept** | **ipv6-reject** }

ipv6-accept

GGSN/P-GW will not reject the call; follows the standard behavior of allocating the available IP address.

ipv6-reject

Enables rejecting a call if GGSN/P-GW cannot allocate the IPv4 address for PDN type IPv4v6.

Usage Guidelines

As per the standard behavior, when a UE sends a Create Request to GGSN/P-GW with PDN type IPv4v6, it should allocate both IPv4 and IPv6 address to the UE. If GGSN/P-GW fails to allocate the IPv4 address due to IP pool exhaustion, then it allocates only IPv6 address and changes the PDN Type to IPv6 and the call continues. In order to control this behavior, this CLI has been introduced; when configured, the following behavioral scenarios will be in place:

- CLI executed with **ipv6-reject** option will reject a call if GGSN/P-GW cannot allocate the IPv4 address for PDN type IPv4v6.
- CLI executed with **ipv6-accept** option will not reject a call and follow the standard behavior.

Example

The following command will reject a call if IPv4 type address allocation is not possible by GGSN/P-GW:

```
ip address pool-exhaust-action ipv6-reject
```

ip context-name

Configures the name of the destination context to use for subscribers accessing 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

[no] ip context-name *ctxt_name*

no

Removes a previously configured context name.

ctxt_name

Specifies the name of the context through which subscriber data traffic will be routed. *ctxt_name* must be an alphanumeric string from 1 to 79 characters.

Usage Guidelines

Use this command to specify the name of a destination context configured on the system through which to route all subscriber data traffic. This context will be used for subscribers accessing this APN. If no name is specified, the system will use the context in which the APN is configured as the destination context.

When the APN is used to support Mobile IP functionality, this command is used to indicate the context in which the FA (foreign Agent) service is configured. If no name is specified, the context in which the GGSN service facilitating the subscriber PDP context is used.

Example

The following command configures the system to route subscriber traffic for the APN through a context called isp1:

```
ip context-name isp1
```

ip header-compression

Configures IP packet header compression parameters for 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

```
ip header-compression vj
default ip header-compression
no ip header-compression
```

default

Disables Van-Jacobson header compression.

no

Disables Van-Jacobson header compression.

vj

Enables Van-Jacobson header compression for IP packets. Default: Enabled

Usage Guidelines

IP header compression reduces packet header overhead resulting in more efficient utilization of available bandwidth.

Example

The following command disables packet header compression for the APN:

```
no ip header-compression
```

ip hide-service-address

Renders the IP address of the GGSN unreachable from mobile stations (MSs) using this APN. This command is configured on a per-APN basis.

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

```
[ default | no ] ip hide-service-address
```

default

Sets the default behavior of this command. By default this function is disabled.

no

Disables this functionality. This is the default setting.

Usage Guidelines

This hides the GGSN IP address from the mobile station for security purposes.

Example

The following command enables this functionality. Does not allow the GGSN's IP address to be viewed by the mobile station:

```
ip-hide-service-address
```

ip local-address

Configures the local-side IP address of the subscriber's point-to-point connection.

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

```
ip local-address ip_address
no ip local-address
```

no

Removes a previously configured IP local-address.

ip_address

Specifies an IP address configured in a destination context on the system through which a packet data network can be accessed. *ip_address* must be expressed in IPv4 dotted-decimal notation.

Usage Guidelines

This parameter specifies the IP address on the system that the MS uses as the remote-end of the PPP connection. If no local address is configured, the system uses an unnumbered scheme for local-side addresses.

Example

The following command configures a local address of 192.168.1.23 for the MS:

```
ip local-address 192.168.1.23
```

ip multicast discard

Configures the IP multicast discard packet behavior.

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

```
[ default | no ] ip multicast discard
```

default

Restores the APN IP parameters to the default multicast settings, which is to discard PDUs.

no

Removes a previously configured IP multicast discard.

Usage Guidelines

This command specifies if IP multicast discard is enabled or disabled.

Example

The following command enables IP multicast discard for an APN:

```
ip multicast discard
```

ip-pool-mgmt-policy

Configures the IP Pool management policy.

Product CUPS

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 **ip-pool-mgmt-policy** *policy_name*

policy_name

Specifies the IP Pool Management Policy name and must be a string of size 1-32.

Usage Guidelines For more information, see the *DNS Based UP Selection* chapter.

ip qos-dscp

Configures the quality of service (QoS) differentiated service code point (DSCP) used when sending data packets of a particular 3GPP QoS class over the Gi interface.

Product 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

```
ip qos-dscp { qci { 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 } { dscp } } +
default ip qos-dscp
no ip qos-dscp { qci { 1 | 2 | 3 | 4 | 5 { allocation-retention-priority
 { 1..3 } } | 6 { allocation-retention-priority { 1..3 } } | 7 {
allocation-retention-priority { 1..3 } } | 8 {
allocation-retention-priority { 1..3 } } | 9 } } } +
```

default

Restores the APN IP parameters to the default setting *conversational ef streaming af11 interactive af21 background be*.

no

Restores the QoS parameter to its default setting.

allocation-retention-priority

Specifies the DSCP for interactive class if the allocation priority is present in the QoS profile.

allocation-retention-priority can be the integers 1, 2, or 3.

DSCP values use the following matrix to map based on traffic handling priority and Alloc/Retention priority if the allocation priority is present in the QoS profile.

Following table shows the DSCP value matrix for *allocation-retention-priority*.

Table 2: Default DSCP Value Matrix

Allocation Priority	1	2	3
Traffic Handling Priority			
1	ef	ef	ef
2	ef	ef	ef
3	af21	af21	af21
4	af21	af21	af21

Important If you only configure DCSP marking for interactive traffic classes without specifying ARP, it may not properly take effect. The CLI allows this scenario for backward compatibility. However, it is recommended that you configure all three values.

qci

Configures the QoS Class Identifier (QCI) attribute of QoS. Here the *qci_val* is the QCI for which the negotiate limit is being set; it ranges from 1 to 9.

dscp

Specifies the DSCP for the specified traffic pattern. *dscp* can be configured to any one of the following:

- **af11:** Assured Forwarding 11 per-hop-behavior (PHB)
- **af12:** Assured Forwarding 12 PHB
- **af13:** Assured Forwarding 13 PHB
- **af21:** Assured Forwarding 21 PHB
- **af22:** Assured Forwarding 22 PHB
- **af23:** Assured Forwarding 23 PHB
- **af33:** Assured Forwarding 33 PHB
- **af41:** Assured Forwarding 41 PHB
- **af42:** Assured Forwarding 42 PHB
- **af43:** Assured Forwarding 43 PHB
- **be:** Best effort forwarding PHB
- **ef:** Expedited forwarding PHB

- **af31:** Assured Forwarding 31 PHB
- **pt:** Pass through (ToS of user packet is not modified)
- **af32:** Assured Forwarding 32 PHB

Default: QCI:

- 1: ef
- 2: ef
- 3: af11
- 4: af11
- 5: ef
- 6: ef
- 7: af21
- 8: af21
- 9: be

+

More than one of the above keywords can be entered within a single command.

Usage Guidelines

DSCP levels can be assigned to specific traffic patterns in order to ensure that data packets are delivered according to the precedence with which they're tagged. The diffserv markings are applied to the IP header of every subscriber data packet transmitted over the Gi interface(s).

The traffic patterns are defined by QCI (1 to 9). Data packets falling under the category of each of the traffic patterns are tagged with a DSCP that further indicate their precedence as shown in following tables respectively:

Table 3: Class structure for assured forwarding (af) levels

Drop Precedence	Class			
	Class 1	**Class 2**	**Class 3**	**Class 4**
Low	af11	af21	af31	af41
Medium	af12	af22	af32	af41
High	af13	af23	af33	af43

Precedence (low to high)	DSCP
1	Best Effort (be)
2	Class 1
3	Class 2

Precedence (low to high)	DSCP
4	Class 3
5	Class 4
6	Express Forwarding (ef)

The DSCP level can be configured for multiple traffic patterns within a single instance of this command.

Important If a GGSN service is associated with a P-GW service, then the GGSN service will use the QCI-QoS mapping tables specified in the **qci-qos-mapping** command and assigned to its associated P-GW service.

Example

The following command configures the DSCP level for QCI to be Expedited Forwarding,**ef**:

```
ip qos-dscp qci 1 ef
```

ip source-violation

Enables or disables packet source validation for the current APN.

Product

tr

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

```
ip source-violation { ignore | check [ drop-limit limit ] [
exclude-from-accounting ]
[ drop-count-timeout time-interval ]  } [ traffic-type { ipv4 | ipv6 } ]
default ip source-violation
```

default

Enables the checking of source addresses received from subscribers for violations, with a drop limit of 10 invalid packets that can be received from a subscriber prior to their session being deleted.

ignore

Default: Disabled

Disables source address checking for the APN.

check [drop-limit *limit*]

Default: Enabled, limit = 10

Enables the checking of source addresses received from subscribers for violations.

A **drop-limit** can be configured to set a limit on the number of invalid packets that can be received from a subscriber prior to their session being deleted.

limit can be configured to any integer value between 0 and 10000. A value of 0 indicates that all invalid packets will be discarded, but the session will never be deleted by the system.

exclude-from-accounting

Default: Disabled

Excludes the packets identified with IP source violation from the statistics generated for accounting records.

check [drop-count-timeout time-interval]

Default: Default value is 120 seconds (2 minutes)

The drop-count-timeout is used to configure the value for time interval violation drop-count update timer. You must specify the time interval in seconds.

check [traffic-type { ipv4 | ipv6 }]

Default: Configurations is common for both IPv4 and IPv6.

This configuration specifies the packet traffic type as IPv4/v6.



Note The violation count increments even if the drop limit and timer values are zero. The session does not get deleted whereas, the violated packets are dropped. If the 'drop-count-timeout' is enabled then 'traffic-type' must be specified.

Usage Guidelines

Source validation is useful if packet spoofing is suspected or for verifying packet routing and labeling within the network.

Source validation requires the source address of received packets to match the IP address assigned to the subscriber (either statically or dynamically) during the session.

Example

The following command enables source address validation for the APN and configures a drop-limit of *15*:

```
ip source-violation check drop-limit 15
```

Example

The source violation behaviour for IPv4 and Ipv6 IP packets are as explained below:

```
ip source-violation check drop-limit 5 exclude-from-accounting
drop-count-timeout 120 traffic-type ipv4
```

```
ip source-violation check drop-limit 8 exclude-from-accounting
drop-count-timeout 60 traffic-type ipv6
```

IPv4 or IPv6: When a source violated packet is received, a timer is started. The packet drop counter increments for each packet violation. P-GW waits for [(N+1) * time-interval] minutes, then starts decreasing (divide by 2) the source violated packet drop counter until it reaches zero. When the drop counter reaches zero, the timer stops. The timer starts again when P-GW receives a new source violated packet.

ip user-datagram-tos copy

Controls the copying of the IP ToS octet value from user IPv4/IPv6 datagrams into the IP header of GTP tunnel encapsulations.

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

```
[ default | no ] ip user-datagram-tos copy
```

default

Sets the default behavior of this command. By default this function is disabled.

no

Removes the preconfigured parameter for this command.

Usage Guidelines

This command enables or disables the copying of the ToS byte from the inner IP header to the outer IP header for an RP connection.

When this function is enabled, the SGSN can detect the special ToS marking in the outer IP header of GTP tunnel packets and identify certain packets as control messages.

ipv6 access-group

Configures the IPv6 access group for the current APN profile which applies a single Access Control List (ACL) to multiple subscribers via the APN for IPv6 traffic.

Product

GGSN

ACS

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

ipv6 access-group *group_name* **[in | out] [fallback-enabled]**
[no] ipv6 access-group *group_name* **[in | out]**

no

Removes a previously configured IPv6 ACL applied to a particular APN for IPv6 traffic. If at least one of the two **{ in | out }** options is not selected for the ACL that will be removed, the ACL will be removed for both directions.

group_name

Specifies the name of the IPv6 access group as an alphanumeric string of 1 through 79 characters.

in | out

Default: both (in and out)

Specifies the access-group as either inbound or outbound by the keywords **in** and **out**, respectively.

If no direction is supplied in the base command, the specified IPv6 access control list will be applied to both directions.

fallback-enabled

When invalid ACL is received from RADIUS during Context Activation, ACL in this APN will be applied so there is no loss of CDR or missing charging information.

By default, ACL fallback is disabled.

Usage Guidelines

Use this command to apply a single IPv6 access control list to multiple subscribers via an APN for inbound or outbound IPv6 traffic.

If no traffic direction is specified, the selected access control list will be applied to both traffic directions.

Run command without **fallback-enabled** option to disable ACL fallback for a previously configured ACL applied to a particular APN.

Example

The following command associates the *sampleipv6Group* access group with the current APN profile for both inbound and outbound access:

```
ipv6 access-group sampleipv6Group
```

The following removes the outbound access group flag for *sampleipv6Group*:

```
no ipv6 access-group sampleipv6Group out
```

ipv6 address alloc-method

Controls the IPv6 address allocation method for a particular APN.

Product

All

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

```
ipv6 address alloc-method { dhcpv6-proxy [allow-prefix-delegation] | local
 | no-dynamic } [ allow-user-specified ]
[ default ] ipv6 address alloc-method
```

default

Configures the default address allocation method which is "local".

dhcpv6-proxy

Configures the IPv6 address from DHCP server for the APN.

allow-prefix-delegation

Configures the APN to allow DHCPv6 prefix-delegation.

local

Configures the IPv6 address from the local pool configured.

no-dynamic

Configures the IPv6 address as indicated by the authentication server.

allow-user-specified

When any of the above three options is specified with **allow-user-specified**, the static IP address proviced by UE takes priority and allocated/configured.

Usage Guidelines

With the support of DHCPv6 and dual PDP IPv4v6, the separate allocation methods are required for IPv4 and IPv6. Earlier the IPv6 address was allocated through locap pool or RADIUS Returned, but with the new options: local, no-dynamic, and DHCPv6-proxy, the IPv6 address allocation can be done for a particular APN. The static address allocation can be enabled by the use of **allow-user-specified** keyword with the above three options.

From 15.0 onward the support of prefix delegation for DHSCv6 is added to assign a network address prefix to a user site, configuring the user's router with the prefix to be used for each interface it is attached to. This is one of the methods for delegating IPv6 address prefixes to an IPv6 subscriber's network.

Example

The following command provides an example of allocating the IP address from DHCP server:

```
ipv6 address alloc-method dhcpv6-proxy allow-user-specified
```

The following commands configures the prefix-delegation for DHCPv6 with 52 bit length:

```
ipv6 address alloc-method dhcpv6-proxy allow-prefix-delegation
ipv6 address prefix-delegation-len 52
```

ipv6 address delegate-prefix-pool

Configures the private pool name to be used for delegate prefix allocation.

Product

All

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

ipv6 address delegate-prefix-pool *pool_name*
[no] ipv6 address delegate-prefix-pool

delegate-prefix-pool:

Configures a pool of IPv6 address delegated prefix.

pool_name:

Name of the pool with IPv6 address delegated prefix.

no

Disables the pool of IPv6 address delegated prefix.

Usage Guidelines With this command, configure the IPv6 private pool name to enable the prefix delegation from the local pool.

Example

The following command provides an example of creating a pool of IPv6 address delegated prefix:

```
ipv6 address delegate-prefix-pool pool1
```

ipv6 address prefix-delegation-len

Configures the supported prefix length to 48/52/56 bit length per-APN for DHCPv6 prefix-delegation support.

Product All

Privilege Security Administrator, Administrator

Syntax Description

```
[ no ] ipv6 address prefix-delegation-len {48 | 52 | 56}
```

no

Removes the configured prefix-delegation length to allow DHCPv6 prefix delegation.

Usage Guidelines Use this command to configure the length of prefix (48/52/56) to allow with DHCPv6 prefix delegation.

Example

The following command sets the allowed prefix length to 52 bit for DHCPv6 prefix delegation support:

```
ipv6 address prefix-delegation-len 52
```

ipv6 address pool-exhaust-action

Configures the behavior to accept/reject a call if the IPv6 address pool is exhausted.

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

ipv6 address pool-exhaust-action { **ipv4-accept** | **ipv4-reject** }

ipv4-accept

GGSN/P-GW will not reject the call; follows the standard behavior of allocating the available IP address.

ipv4-reject

Enables rejecting a call if GGSN/P-GW cannot allocate the IPv6 address for PDN type IPv4v6.

Usage Guidelines

As per the standard behavior, when a UE sends a Create Request to GGSN/P-GW with PDN type IPv4v6, it should allocate both IPv4 and IPv6 address to the UE. If GGSN/P-GW fails to allocate the IPv6 address due to IP pool exhaustion, then it allocates only IPv4 address and changes the PDN Type to IPv4 and the call continues. In order to control this behavior, this CLI has been introduced; when configured, the following behavioral scenarios will be in place:

- CLI executed with **ipv4-reject** option will reject a call if GGSN/P-GW cannot allocate the IPv6 address for PDN type IPv4v6.
- CLI executed with **ipv4-accept** option will not reject a call and follow the standard behavior.

Example

The following command will reject a call if IPv6 type address allocation is not possible by GGSN/P-GW:

```
ipv6 address pool-exhaust-action ipv4-reject
```

ipv6 dns

Configures primary and secondary IPv6 Domain Name Service (DNS) servers.

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

[**no**] **ipv6 dns** { **primary** | **secondary** } { *ipv6_dns_address* }

no

Deletes a previously configured DNS server.

primary

Configures the IPv6 address of primary DNS server for the APN.

secondary

Configures IPv6 address of the secondary DNS server for the APN. Only one secondary DNS server can be configured.

ipv6_dns_address

The IP address of the DNS server entered using IPv6 colon-separated-hexadecimal notation.

Usage Guidelines

DNS servers are configured on a per-APN profile basis. This allows each APN profile to use specific servers in processing PDP contexts.

The DNS can be specified at the APN level in APN configuration as well as at the Context level in Context configuration mode with **ip name-servers** command, 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 has the third preference
4. DNS values configured at context level with **ip name-servers** command has the last preference.



Important The same preference would be applicable for the NBNS (NetBIOS Name Service) servers to be negotiated via ICPC (Initial Connection Protocol Control) with the LNS (L2TP Network Server).

Example

The following command provides an example of setting the primary DNS server:

```
ipv6 dns primary fe80::c0a8:a04
```

ipv6 egress-address-filtering

Enables or disable IIPv6 egress address filtering. This function filters out packets not meant for the mobile interface ID. The GGSN records the source interface ID of all the packets received from the mobile node. When packets sent to the mobile node are received, the destination interface ID is compared against the list of recorded interface IDs and with the local interface-ID assigned to the MS during IPv6CP. If no match is found, the packet is dropped.

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

[no] ipv6 egress-address-filtering

no

Disables IPv6 egress address filtering.

Usage Guidelines

Used to filter packets that arrive from the internet to a particular site.

Example

The following command provides an example disabling egress address filtering:

no ipv6 egress-address-filtering

ipv6 initial-router-advt

Creates an IPv6 initial router advertisement interval for the current 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

ipv6 initial-router-advt { **interval** *int_value* | **num-advts** *num_value* **| option mtu** | **value }**
[**default**] **ipv6 initial-router-advt** { **interval** | **num-advts| option mtu | value }**
no ipv6 initial-router-advt option mtu

default

Resets interval or num-advts to their default setting.

interval *int_value*

Specifies the time interval (in milliseconds) when the initial IPv6 router advertisement is sent to the mobile node as an integer from 100 through 16000. Default: 3000ms

num-advts value *num_value*

Specifies the number of initial IPv6 router advertisements sent to the mobile node as an integer from 1 through 16. Default: 3

Usage Guidelines

This command is used to set the advertisement interval and the number of advertisements. Using a smaller advertisement interval increases the likelihood of router being discovered more quickly when it first becomes available.

option mtu

Enables the gateway to send the IPv6 MTU option in RAs for IPv6 and IPv4v6 PDN types towards the UE. As a result, the UE can send uplink data packets based on the configured MTU and perform fragmentation at the source, if required.

option mtu value

Specifies that the configured value is sent in the RA packet rather than the data tunnel MTU. The configured value must be in *octets -integer 1280-2000*. This value is used only for advertisement in RA packet and the gateway need not enforce this value.

The default setting is enabled.

The **no** keyword disables this feature. The IPv6 MTU option in RAs for IPv6 and IPv4v6 PDN types will not be sent towards the UE.

Example

The following command specifies the initial ipv6 router interval to be 2000ms:

```
ipv6 initial-router-advt interval 2000
```

l3-to-l2-tunnel address-policy

Configures the address allocation/validation policy, when subscriber L3 (IPv4/IPv6) sessions are tunneled using an L2 tunneling protocol, such as L2TP.

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

l3-to-l2-tunnel address-policy { **alloc-only** | **alloc-validate** | **no-alloc-validate** }
default l3-to-l2-tunnel address-policy

default

Restores the layer 3-to-layer 2 tunnel address policy parameter to the default setting of validation with no allocation.

alloc-only

Specifies that the system locally allocates and validates subscriber addresses. Default: Disabled

alloc-validate

Specifies that the system allocates addresses when IP addresses are dynamically assigned. The system does not validate the address specified by the subscriber. Default: Disabled

no-alloc-validate

Specifies that the system does not allocate or validate subscriber addresses locally for such sessions; it passes the address between remote tunnel terminator to the mobile node. Default: Enabled

Usage Guidelines

This command can be useful for MIP HA sessions tunneled from the system using L2TP tunnels, or GGSN PDP contexts of type IP tunneled using L2TP to a remote LNS.

Example

The following command configures the system to locally allocate and validate subscriber addresses:

```
l3-to-l2-tunnel address-policy alloc-only
```

loadbalance-tunnel-peers

Configures how tunnel-peers are selected for 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

`loadbalance-tunnel-peers { balanced | prioritized | random }`
`default loadbalance-tunnel-peers`

default

Restores the loadbalance-tunnel-peers parameter to the default setting of random.

balanced

Tunnel-peer selection is made without regard to prioritization, but in a sequential order that balances the load across the total number of peer nodes available. Default: Disabled

prioritized

Tunnel-peer selection is made based on the priority configured for the peer. Default: Disabled

random

Tunnel-peer selection is random in order. Default: Enabled

Usage Guidelines

Use this command to configure the load-balancing algorithm that defines how the tunnel-peers are selected by the APN when multiple peers are configured in the APN.

Example

The following command sets the APN to connect to tunnel-peers in a sequential order:

`load-balancing balanced`

long-duration-action detection

Sets the detection of a session that exceeds the long duration timer and sends notification.

Product

All

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

`long-duration-action detection`
`default long-duration-action`

default

Restores the long-duration-action parameter to its default setting of detection.

long-duration-action detection

Detects long duration sessions and sends SNMP TRAP and CORBA notification. This is the default behavior.
Default: Enabled

Usage Guidelines

Use this command to detect a session that exceeds the limit set by the long duration timer.

Refer to the **timeout idle** and **timeout long-duration** commands for information on setting the long duration timer.

Example

Use the following command to enable detecting the session that exceeds the long duration timer:

```
long-duration-action detection
```

long-duration-action disconnection

Specifies what action is taken when the long duration timer expires.

Product

All

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

long-duration-action disconnection [**suppress-notification**] [**dormant-only**] +

long-duration-action disconnection

Detects a long duration session and disconnects the session after sending SNMP TRAP and CORBA notification.
Default: Disabled

suppress-notifiaction

Suppress the SNMP TRAP and CORBA notification after detecting and disconnecting a long duration session.
Default: Disabled

dormant only

Disconnects the dormant sessions after long duration timer and inactivity time with idle time-out duration expires. It sends the SNMP TRAP and CORBA notification after disconnecting a long duration session. Default: Disabled

Usage Guidelines

Use this command to determine what action is taken when a session exceeds the limit set by the long duration timer.

Refer to the **timeout idle** and **timeout long-duration** command for information on setting the long duration timer.

Example

Use the following command to enable disconnecting sessions that exceed the long duration timer:

```
long-duration-action disconnection
```

Use the following command to disconnect the session that exceed the long duration timer without sending SNMP TRAP and CORBA notification:

```
long-duration-action disconnection suppress-notification
```

Use the following command to disconnect the session that exceed the long duration timer and also inactivity timer for idle time-out duration and send SNMP TRAP and CORBA notification:

```
long-duration-action disconnection dormant-only
```

Use the following command to disconnect the session that exceed the long duration timer and also inactivity timer for idle time-out duration without sending any SNMP TRAP and CORBA notification. If the session is idle and the session-idle-time >= inactivity time the session gets disconnected. Even if session is idle when the long-duration timed-out and session-idle time < inactivity time the timer value is reset to idle-timeout time.

```
long-duration-action disconnection dormant-only suppress-notification
```

lte-s2bgtp-first-uplink

Configures LTE to Wi-Fi (S2bGTP) handover timer .

Product

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

```
lte-s2bgtp-first-uplink timeout
{ default | no } lte-s2bgtp-first-uplink
```

default

Enables the LTE to Wi-Fi handover completion to occur when the Create Session Response is sent on the Wi-Fi tunnel.

no

Disables the feature and handover completion occurs on Create Session Response.

lte-s2bgtp-first-uplink *timeout*

Configures LTE to Wi-Fi (S2bGTP) handover completion timeout in multiple of 100 milliseconds. The valid range is from 100 to 3000. The recommended configuration is 1000 milliseconds.

Usage Guidelines

By default, the LTE to Wi-Fi handover completion happens when Create Session Response is sent on the Wi-Fi tunnel. However, after handover timeout is configured, the handover is delayed until timeout or on receipt of uplink data on Wi-Fi tunnel.

Example

The following command configures the LTE to Wi-Fi (S2bGTP) handover completion timeout in *1000* milliseconds:

```
lte-s2bgtp-first-uplink 1000
```

mbms bmsc-profile

Applies a configured Broadcast-Multicast Service Center (BM-SC) profile to subscribers through APN for Multimedia Broadcast Multicast Service (MBMS) support and functionality.

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

mbms bmsc-profile name *bmsc_profile_name*
[default | no] mbms bmsc-profile

default

Applies the default BMSC profile to the subscribers through the APN.

no

Deletes a previously associated BM-SC profile with this APN.

name *bmsc_profile_name*

Specifies a name for the BM-SC profile already configured in BMSC configuration mode. *bmsc_profile_name* is an alphanumeric string of 1 through 79 characters that may contain dots (.) and/or dashes (-).

Usage Guidelines

Use this command to associate a configured BM-SC profile to use for MBMS contexts with this APN for MBMS feature support.

For more information on BM-SC profile configuration, refer to the *BMSC Profile Configuration Mode Commands* chapter.

This command also configures the specific BM-SC profile to use for Internet Group Management Protocol (IGMP) JOIN requests received from PDP contexts with this APN.

Example

Following command applies a previously configured BM-SC profile named *bm_sc_1* to an APN within the specific context.

```
mbms bmsc-profile name bm_sc_1
```

mbms bearer timeout

Configures the session timeout values for the Multimedia Broadcast Multicast Service (MBMS) bearer contexts with this MBMS 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

```
mbms bearer timeout { absolute | idle } time
[ default | no ] mbms bearer timeout { absolute | idle }
```

default

Sets the default value for the followed option for MBMS bearer context timeout.

no

Returns the timeout parameter to its default setting. If neither the absolute or idle keywords are used in conjunction with this keyword, both timeout options will be returned to their default settings.

absolute

Configures the absolute maximum time (in seconds) an MBMS bearer context may exist in any state (active or idle). Default: Disabled

idle

Default: Disabled

Configures the maximum amount of time (in seconds) an MBMS bearer context may be idle.

time

time can be any integer value between 0 and 4294967295. A time of 0 disables timeouts for this APN. Default: 0

Usage Guidelines

Use this command to limit the amount of time that an MBMS bearer context session can remain connected.

Example

The following commands enables an absolute time timeout of *60000* seconds for MBMS bearer context:

```
mbms bearer timeout absolute 60000
```

mbms ue timeout

Configures the session timeout values for the Multimedia Broadcast Multicast Service (MBMS) user equipment (UE) contexts with this MBMS 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

mbms ue timeout absolute *time*
[default | no] mbms ue timeout absolute

default

Set the default value for the followed option for MBMS UE context timeout.

no

Returns the timeout parameter to its default setting. If neither the absolute or idle keywords are used in conjunction with this keyword, both timeout options will be returned to their default settings.

absolute *time*

Configures the absolute maximum time (in seconds) an MBMS UE context may exist in any state (active or idle). *time* can be any integer value between 0 and 4294967295. A time of 0 disables timeouts for this APN. Default: 0

Usage Guidelines

Use this command to limit the amount of time that an MBMS UE context session can remain connected.

Example

The following commands enables an absolute time timeout of *60000* seconds for MBMS UE context:

```
mbms bearer timeout absolute 60000
```

mbr

Configures token replenishment interval for MBR enforcement at the APN level.

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

```
[ no ] mbr rate-limit token-replenishment-interval { 10ms [
multiplication-factor < 2..100 > ] }
```

no

Disables token replenishment interval at the APN level.

mbr

Configures MBR attributes for all PDNs of the APN.

rate-limit

Configures rate-limit parameters.

token-replenishment-interval

Configures token-replenishment-interval. The available values range from 10 ms to 1000 ms (1 sec).

multiplication-factor

Configures multiplication factor of 10 ms as token replenishment interval. Multiplication-factor is configurable only if token replenishment interval is 10 ms.

Usage Guidelines

Use this command to configure token replenishment interval for MBR enforcement at the APN level. By default, this CLI is disabled.

Example

The following commands generates peak-data-rate in Bytes of token every 1 sec (1000 ms).

```
mbr rate-limit token-replenishment-interval 10ms multiple-factor 100
```

mediation-device

Enables the use of a mediation device and specifies the system context to use for communicating with the device.

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

```
mediation-device [ context-name context_name ] [ delay-GTP-response ] [
no-early-PDUs ] [ no interims ] +
[ default | no ] mediation-device
```

+

Indicates that more than one of the options can be specified with a single execution of the command.

default

Changes the mediation device to no context-name configured and restores the mediation device's default properties.

no

Deletes the mediation-device configuration.

context-name *context_name*

Configures the mediation VPN context for this APN as an alphanumeric string of 1 through 79 characters that is case sensitive. If not specified, the mediation context is the same as the destination context of the subscriber. Default: The subscribers destination context.

delay-GTP-response

When enabled, delays the CPC response until an Accounting Start response is received from the mediation device. Default: Disabled

no-early-pdus

Specifies that the system delays PDUs from the MS until a response to the GGSN accounting start request is received from the mediation device. The PDUs are queued, not discarded. Default: Disabled

If "no-early-PDUs" is enabled, the chassis does not send uplink/downlink data from/to a MS until it receives the Acct-Rsp Start for the same from the mediation device. On receiving the Acct-Rsp, pending PDUs are forwarded. The chassis buffers up to two PDUs per call. As soon as the third PDU comes, the buffering is disabled and all the PDUs are forwarded for that call.

Configures the system to queue up to two PDUs until the mediation device returns a response to the system's accounting START request per 3GPP standards. On receiving the Accounting response message, the system forwards the subsequent PDUs without discarding any of the packets.



Important For StarOS 10.0 and earlier releases, the system buffers up to four PDUs and queues or discards the remaining PDUs.



Important For StarOS 11.0 and later releases, the system is configured so that none of the PDUs are discarded.

no-interims

Disables sending interims to the mediation server. Default: Disabled



Important Different commands are used to disable RADIUS interims for RADIUS accounting and mediation accounting. To disable RADIUS interims for mediation accounting, use the following command: **mediation-device context-name** *context_name* **no-interims**. To disable RADIUS interims for RADIUS accounting, use the following command: **accounting-mode radius-diameter no-interims**.

Usage Guidelines

This command enables mediation device support for the APN. Mediation devices can be either deep-packet inspection servers or transaction control servers.

Keywords to this command can be used in combination to each other, depending on configuration requirements.

Example

The following command enables mediation device support for the APN and uses the protocol configuration located in an system context called *ggsn1*:

```
mediation-device context-name ggsn1
mediation-device context-name ggsn1 no-interims no-early-pdus
mediation-device no-early-pdus no-interims
mediation-device no-interims no-early-pdus
```

The following command enables mediation device support for the APN and uses the protocol configuration located in the subscribers destination context:

```
mediation-device
```

mobile-ip home-agent

Configures the IP address of the home agent (HA) used by the current APN to facilitate subscriber Mobile IP sessions.

Product

GGSN

FA

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

```
mobile-ip home-agent ip_address [ alternate ]
no mobile-ip home-agent ip_address alternate
default mobile ip home-agent
```

default

Restores the APN mobile-ip parameters to the default setting, no HA address defined.

no

Removes a previously configured HA address.

ip_address

Specifies the IP address of the HA expressed in IPv4 dotted-decimal notation.

alternate

Designates this Mobile IP HA as the alternate that will be used in the event of a fail-over.

Usage Guidelines

If the APN is configured to support Mobile IP for all PDP contexts it is facilitating, this command specifies the IP address of the HA that is to be used.

Example

The following command configures an HA IP address of 192.168.1.15:

```
mobile-ip home-agent 192.168.1.15
```

mobile-ip min-reg-lifetime-override

Specifies the minimum registration timer to override the platform-wide default on an enterprise basis. This feature is associated with 4G LTE scenarios employing Network Mobility (NEMO) routing.

Product

P-GW

HA

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

```
mobile-ip min-reg-lifetime-override { seconds | infinite }
default mobile-ip min-reg-lifetime-override
no mobile-ip min-reg-lifetime-override
```

default

Sets the minimum registration time to 600 seconds.

no

Deletes the registration interval entered via this command.

seconds

Specifies the minimum registration interval in seconds as an integer from 1 through 65534. Default = 600

infinite

Sets the minimum registration interval as "infinite" (forever) for this subscriber.

Usage Guidelines

Specify the minimum registration timer to override the platform-wide default on an enterprise basis. With this command, NEMO traffic could be re-routed symmetrically to an alternate carrier within the specified number of seconds following a failure on the primary communication path.

Example

The following command sets the minimum registration override interval to 900 seconds:

```
mobile-ip min-regreg-lifetime-override 900
```

mobile-ip mn-aaa-removal-indication

Configures the system to remove various information elements when relaying Registration Request messages to the HA.

Product

GGSN

FA

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

```
[ default | no ] mobile-ip mn-aaa-removal-indication
```

default

Sets the default setting for mobile IP MN-AAA-Removal-Indication.

no

Disables this functionality. This is the default setting.

Usage Guidelines

When this functionality is enabled, the MN-FA challenge and MN-AAA authentication extensions are removed when relaying a Registration Request (RRQ) to the HA.

mobile-ip mn-ha-hash-algorithm

Designates the encryption algorithm to use for Hash-based Message Authentication Code (HMAC).

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

`mobile-ip mn-ha-hash-algorithm { hmac-md5 | md5 | rfc2002-md5 }`
`default mobile-ip mn-ha-hash-algorithm`

default

Designates the default encryption algorithm to use.

hmac-md5 | md5 | rfc-2002-md5

Default: hmac-md5

The encryption algorithms that may be used.

Usage Guidelines

Provides security by encrypting the data.

Example

The following command sets encryption for md5:

`mobile-ip mn-ha-hash-algorithm md5`

mobile-ip mn-ha-shared-key

Configures the subscriber MobileNode-Home Agent (MN-HA) shared key.

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

mobile-ip mn-ha-shared-key *key*
no mobile-ip mn-ha-shared-key

no

Disables this functionality. This is the default setting.

key

Specifies the subscriber MN-HA shared key as either an alphanumeric string or a hexadecimal number sequence beginning with "0x". The string or sequence consists of 16 to 127 characters.

Usage Guidelines

Configures a shared key for the APN.

Example

The following command configures a shared key as the alphanumeric string *sfd23408imi9yn*:

mobile-ip mn-ha-shared-key sfd23408imi9yn

mobile-ip mn-ha-spi

Configures the Mobile IP Security Parameter Index (SPI).

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

mobile-ip mn-ha-spi *spi_number*
no mobile-ip mn-ha-spi

no

Disables this functionality. This is the default setting.

spi_number

Specifies the SPI as an integer from 256 through 4294967295.

Usage Guidelines Configures an SPI for the APN.

Example

The following command configures an SPI of *151111111111111111111111111111111*:

```
mobile-ip mn-ha-spi 151111111111111111111111111111111
```

mobile-ip required

Enables support for Mobile IP functionality for all PDP contexts facilitated by the current APN.

Product

GGSN

FA

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

```
[ default | no ] mobile-ip required
```

default

Applies the default setting for mobile-ip for the APN. Default is disabled.

no

Disables mobile-ip for the APN.

Usage Guidelines Mobile IP functionality for IP PDP contexts is only supported at the APN-level. This command enables or disables Mobile IP support for the APN.

When Mobile IP is performed, the system authenticates the subscriber and the Mobile IP FA.

If this option is enabled, the system deletes all PDP contexts attempting to access the APN for which a Mobile IP session can not be established.

mobile-ip reverse-tunnel

Configures the system to support reverse-tunneling for Mobile IP sessions facilitated by the current APN.

Product

GGSN

FA

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

`[ default | no ] mobile-ip reverse-tunnel`

default

Designates the default reverse tunnel for the APN. The default is enabled.

no

Disables this functionality.

Usage Guidelines

Use this command to enable support for Mobile IP reverse tunneling for the APN. Reverse tunneling is enabled by default.

nai-construction

Configures the Network Access Identifier (NAI) construction parameters on a per-APN basis only, rather than by per-aaa-group when constructed NAI authentication is enabled.

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

nai-construction { imsi | msisdn } [override-null-username] [encrypted password *encrypt_password* **| use-shared-secret-password | password** *password* **]**
no nai-construction

no

Disables the NAI construction at the APN level.

imsi

Enables NAI construction using IMSI for authentication for a user. GGSN constructs NAI using IMSI when no user-name is received. This is the default setting. Default: Enabled

msisdn

Enables NAI construction using Mobile Station International ISDN Number (MSISDN) for authentication for a user. GGSN constructs NAI using MSISDN when no user-name is received.

override-null-username

Enables NAI construction using IMSI/MSISDN for authentication for a user or when empty user name is received.

encrypted password

Specifies an encrypted password is to be used for this NAI-constructed user. *string* is an alphanumeric string of 0 through 63 characters.

password

Configures the authentication user-password for this NAI-constructed user. *password* is an alphanumeric string of 0 through 63 characters.

use-shared-secret-password

Specifies use of the RADIUS authentication shared secret password for this NAI-constructed user.

Usage Guidelines

NAI-construction defines the behavior for construction at the APN level. If defined for a particular APN, this command works independently and overwrites the behavior of aaa constructed-nai defined at the context level for calls involving this APN.

Note that NAI construction using IMSI or MSISDN, where either no user name is received or a blank user name is received for authentication, is applicable only when NAI constructed authentication is enabled using the **aaa nai-construction authentication** command in Context Configuration Mode.

Example

The following command enables NAI-construction using IMSI as the authentication type with an encrypted password:

```
nai-construction imsi encrypted password s1289sf980333jwwdo97342
```

nbns

Configures and enables use of NetBios Name Service (NBNS) for the 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

`[ no ] nbns { primary | secondary }` *`IP_address`*

no

Removes/disables use of a previously configured NetBios Name Service.

primary

Designates primary NBNS server. Must be followed with an IPv4 address in dotted-decimal notation.

secondary

Designates secondary/failover NBNS server. Must be followed with an IPv4 address in dotted-decimal notation.

IP_address

Specifies the IP address in IPv4 dotted-decimal notation.

Usage Guidelines

This command specifies NBNS parameters. The NBNS option is present for both pdp type IP and pdp type PPP for GGSN.

The system can be configured to use NetBios Name Service for the APN.

Example

The following command configures the APN's NetBios Name Service to primary IP 192.168.1.15.

```
nbns primary 192.168.1.15
```

netloc-s2b-ue-ip-udp-port-always

Renders the "uELocalIPAddress" and "uDPSourcePort" always in Gy messages and CDR for dedicated bearer. This option is disabled by default.

Product

P-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

`[ no ] netloc-s2b-ue-ip-udp-port-always`

no

Disables the feature and its the default configuration.

Usage Guidelines

When this CLI is configured and P-GW receives UDP-Source-Port or UE-Local-IP-Address in CBRsp/UBRsp/DBRsp messages for WiFi calls, the P-GW will always generate CDR with "uELocalIPAddress" and "uDPSourcePort" for dedicated bearer, even if values of these IEs are unchanged. For changes in UE IP and/or UDP port, the behavior remains the same as existing behavior without the CLI configured.

network-behind-mobile

Allows enabling/disabling the Network Behind Mobile Station (NBMS) for the 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

`network-behind-mobile { max-addresses-behind-mobile` *`max_addrs`* **`| max-subnets`** *`max_subnets`* **`}`**
`[ default | no ] network-behind-mobile`

default

Enables the default settings for this function. It enables NBMS with max-subnets as 10 and max-addresses-behind-mobile as 16,777,214 default values.

no

Disables the network behind mobile station functionality on the APN.

max-addresses-behind-mobile *max_addrs*

Configures the maximum number of addresses that are allowed in a single Network/subnet Behind MS.

max_addrs must be an integer from 1 through 16,777,214.

Default: 16,777,214

max-subnets *max_subnets*

Specifies the maximum number of subnets that can be enabled for a call in the APN.

max_subnets must be an integer from1 through 16.

Default: 10

Usage Guidelines

Use this command to enable or disable NBMS for the APN.

Example

The following command enables NBMS and allows a maximum of 16 routes to be installed on the APN wherein maximum 268,435,454 host addresses are allowed in each network:

```
network-behind-mobile max-subnets 16
```

nexthop-forwarding-address

Configures the next hop forwarding address for the 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

nexthop-forwarding-address *ipv4_address | ipv6_address*
no nexthop-forwarding-address

no

Disables this function. This is the default setting.

ipv4_address

Specifies the next hop forwarding address for the APN. Must be an IPv4 address in dotted-decimal notation.

ipv6_address

Specifies the next hop forwarding address for the APN. Must be an IPv6 address in colon-separated-hexadecimal notation.

Ensure the route is available for this next hop address and its directly connected host. Use of an arbitrary address can cause a routing loop within the host and lead to dropped packets.

Usage Guidelines

Use this command to configure the next hop forwarding address for the APN.

Example

The following command configures the next hop forwarding address to 10.1.1.1:

```
nexthop-forwarding-address 10.1.1.1
```

The following command configures the next hop forwarding IPv6 address:

```
nexthop-forwarding-address 2A01:C000:0009:4080:0:0:0:2
```

npu qos

Configures an NPU QoS priority queue for packets facilitated by the 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

npu qos traffic priority { best-effort | bronze | derive-from-packet-dscp | gold | silver }
default npu qos traffic priority

default

Configures the default NPU QoS traffic priority.

traffic priority { best-effort | bronze | derive-from-packet-dscp | gold | silver }

best-effort: Assigns the best-effort queue priority. This is the lowest priority.

bronze: Assigns the bronze queue priority. This is the third-highest priority.

derive-from-packet-dscp: Specifies that the priority is to be determined from the DSCP (Differentiated Services Code Point) field in the packet's TOS octet. Default: Enabled

gold: Assigns the gold queue priority. This is the highest priority.

silver: Assigns the silver queue priority. This is the second-highest priority.

Usage Guidelines

This command is used in conjunction with the Network Processing Unit (NPU) Quality of Service (QoS) functionality.

The system can be configured to determine the priority of a subscriber packet either based on the configuration of the APN, or from the differentiated service (DS) field in the packet's TOS octet (representing the differentiated service code point (DSCP) value).

Refer to the *GGSN Administration Guide* for additional information on NPU QoS functionality.

Example

The following command configures the APN's priority queue to be *gold*:

```
npu qos traffic priority gold
```

outbound

Configures the APN host username and password.

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

```
outbound { [ encrypted ] password pwd | username name }
no outbound password | username
```

no

Removes previously configured outbound information for the APN.

encrypted

The **encrypted** keyword is intended only for use by the chassis while saving configuration scripts. The system displays the **encrypted** keyword in the configuration file as a flag that the variable following the **password** keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file.

password *pwd*

Specifies the password to use for session authentication as an alphanumeric string of 1 through 127 characters and are case sensitive.

username *name*

Specifies the username to use for session authentication as an alphanumeric string of 1 through 127 characters and are case sensitive.

Usage Guidelines

This command can be used to provide a username and password for authentication when the subscriber does not supply one in accordance with 3GPP standards. In addition, it can be used to create a PPP session when using L2TP to tunnel IP PDP contexts.

If only a username is specified using this command, the password is determined based on the setting of the **aaa constructed-nai** command in the Context Configuration mode. That command is also used to determine the password if an outbound username and password are configured for the APN when the imsi-auth keyword is specified for the **authentication** command in this mode.

Example

The following commands configures an APN username of *isp1* and a password of *secRet123*.

```
outbound username isp1
outbound password secRet123
```

paging-policy-differentiation

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

Product

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

[default | no] paging-policy-differentiation

default

Restores the PPD functionality to its default setting of disabled.

no

Disables this option. This is the default setting.

paging-policy-differentiation

User-datagram packet DSCP value is unaltered by P-GW for downlink data. The PPD feature is supported only for S5/S8 interface. For all Handoff scenarios from other interface to S5/S8 interface, the PPD feature will get enabled if APN had it during its call setup time at that interface.

If PPD feature is enabled for the call and handoff happens from S5/S8 interface to any other interface, PPD feature should get disabled. Now, if handoff happens and this call will come back to S5/S8 interface, PPD feature should become enabled.

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

Usage Guidelines

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

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

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

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

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

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

Example

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

paging-policy-differentiation

p-cscf

Enables use of locally configured Proxy Call Session Control Function (P-CSCF) addresses or a Fully Qualified Domain Name (FQDN).

Product

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

In StarOS V14.x and earlier:

```
p-cscf { fqdn fqdn | primary [ ip IPv4_address | ipv6 IPv6_address ] | secondary
 [ ip IPv4_address | ipv6 IPv6_address ] }
no p-cscf { fqdn | primary [ ip | ipv6 ] | secondary [ ip | ipv6 ] }
```

In StarOS V15.0 and later:

```
p-cscf { fqdn fqdn | priority address_ priority [ ip IPv4_address | ipv6
IPv6_address ] }
no p-cscf { fqdn fqdn | priority address_ priority [ ip | ipv6 ] }
```

no

Disables use of previously configured P-CSCF addresses or FQDN.

fqdn *fqdn*

Configures the P-CSCF FQDN server name for the APN as an alphanumeric string of 1 through 256 characters.

primary [ip*IPv4_address* | ipv6 *IPv6_address*]

Specifies the primary P-CSCF address for the APN.

IPv4_address must be expressed in IPv4 dotted-decimal notation.

IPv6_address must be expressed in IPv6 colon-separated-hexadecimal notation.

secondary [ip *IPv4_address* | ipv6 *IPv6_address*]

Specifies the secondary P-CSCF address for the APN.

IPv4_address must be expressed in IPv4 dotted-decimal notation.

IPv6_address must be expressed in IPv6 colon-separated-hexadecimal notation.

priority *address_ priority* [ip *IPv4_address* | ipv6 *IPv6_address*]

Specifies the priority for P-CSCF address for the APN.

address_ priority is an integer from 1 to 3. 1 is the highest priority.

IPv4_address must be expressed in IPv4 dotted-decimal notation.

IPv6_address must be expressed in IPv6 colon-separated-hexadecimal notation.

Usage Guidelines

Use this command to specify the P-CSCF addresses or FQDN server name associated with this APN.

Example

The following command enables a P-CSCF with the primary IPv4 address *10.2.3.4* for the APN:

```
p-cscf primary ip 10.2.3.4
```

The following command enables a P-CSCF with FQDN server name *pcscfalias1.ind.pun.cisco.com* for the APN:

```
p-cscf fqdn pcscfalias1.ind.pun.cisco.com
```

The following command enables a P-CSCF with the IPv4 address *10.2.3.4* at the highest priority of 1 for the APN:

```
p-cscf priority 1 ip 10.2.3.4
```

pco-options

The following commands are explained below:

- pco-options custom1
- pco-options custom2
- pco-options custom3
- pco-options custom4
- pco-options custom5

pco-options custom1

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

GGSN

P-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

```
pco-options { custom1 [ ue-requested ] | link-mtu bytes [ non-ip bytes ] [
 roamer 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*

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.

bytes must be an integer from 1280 to 2000.

Default: 1500

roamer *bytes*

Configures the link MTU for roaming subscribers. The *bytes* value must be an integer from 1280 to 2000. The default MTU value is 1500.

If the **no pco-options link-mtu roamer** command is configured, the system will revert to the default MTU value of 1500 bytes for roaming subscribers.

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
```

pco-options custom2

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

Product

GGSN

P-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

[no] pco-options { custom2 [ue-requested] value *custom_value* **| value** *custom_value* **}**

no

Removes PCO configuration at APN configuration mode

custom2

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.

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.

Example

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

```
pco-options custom2
```

pco-options custom3

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

Product

GGSN

P-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

[no] pco-options { custom3 [ue-requested] value *custom_value* **| value** *custom_value* **}**

no

Removes PCO configuration at APN configuration mode

custom3

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.

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.

Example

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

```
pco-options custom3
```

pco-options custom4

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

Product GGSN

P-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 **[no] pco-options { custom4 [ue-requested] value** *custom_value* **| value** *custom_value* **}**

no

Removes PCO configuration at APN configuration mode

custom4

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.

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.

Example

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

```
pco-options custom4
```

pco-options custom5

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

Product

GGSN

P-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

`[ no ] pco-options { custom5 [ ue-requested ] value` *`custom_value`* **`| value`** *`custom_value`* **`}`**

no

Removes PCO configuration at APN configuration mode

custom5

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.

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.

Example

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

```
pco-options custom5
```

pdn-behavior

Configures specific PDN behavior.

Product

P-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

```
pdn-behavior  { custom1 | ims | lapi }
[ default | no ] pdn-behavior
```

default | no

Configures APN as "Normal".

custom1

Configures APN as a Custom1 (well-known) APN. Re-auth Requested reason code returned for PDN disconnect.

ims

Configures APN as an IMS APN. Re-auth Requested reason code returned for PDN disconnect.

lapi

Configures the APN as a Low Access Priority Indicator (LAPI) APN. Use this command in conjunction with the **backoff-timer value** command in *APN Configuration Mode*. Together, they configure the node's behavior for the APN Backoff Timer feature.



Caution Do not configure the emergency APN and **pdn-behavior lapi** settings in the same APN, as these two settings are mutually exclusive. If both settings are configured in the same APN, the **pdn-behavior lapi** configuration takes priority. As a result, if both settings are configured and the system is overloaded, the call will be rejected. To determine if both settings are configured in the same APN, execute the **show configuration error verbose** command in Exec Mode. The command output contains a warning if both settings are configured in the same APN.



Important The APN Backoff Timer feature requires that the M2M license be enabled on the P-GW/SAEGW. Contact your Cisco account or support representative for licensing details.

Usage Guidelines

Use this command to configure specific PDN behavior.

Example

The following command configures APN as an IMS APN which returns reason code Re-auth Requested for PDN disconnect:

```
pdn-behavior ims
```

pdn validate-post-switchover

Enables or disables the dynamic rule check for the auto correction of the VoLTE session. This feature should be configured only for the VoLTE/IMS APNs for which auto recovery is required.

Product

P-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

`[no] pdn validate-post-switchover`

no

Disables the dynamic rule check for the auto correction of the VoLTE session.

pdn validate-post-switchover

Validates the dynamic rules for automatic recovery after a switchover.

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
```

permission

Enables or disables the ability to use authorized services for the current APN.

Product

P-GW

SAEGW

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

`[ no ] permission { nemo | pmipv6-interception }`
`default permission`

no | default

Disables the usage of the specified service.

nemo

Enables the ability to use NEMO functionality.



Important Use of the **nemo** keyword requires that a valid license key be installed. Contact your local Sales or Support representative for information on how to obtain a license.

pmipv6-interception

Allows APN to access the external Local Mobility Anchor (LMA) over Proxy Mobile IPv6 (PMIPV6).

Usage Guidelines

Use this command to enable support for NEMO or PMIPv6 functionality on the APN. These options are disabled by default.

Example

The following command enables NEMO functionality:

`permission nemo`

The following command disables NEMO functionality:

`no permission nemo`

pgw fqdn

Configures both the primary and the secondary FQDN string in the configuration.

Product

HSGW

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

```
pgw fqdn primary  primary-fqdn-name secondary secondary-fqdn-name
default pgw fqdn
no pgw fqdn
```

default

Resets the command to its default setting of disabled.

no

Disables the previously configured pgw fqdn configuration.

primary *primary_fqdn_name*

Configures the primary static fqdn string for the HSGW to select the P-GW.

secondary *secondary_fqdn_name*

Configures the secondary static fqdn string. The primary fqdn will be tried before trying the secondary fqdn.

Usage Guidelines

Use this command to configure both the primary and the secondary FQDN string in the configuration.

With with command, DNS resolution is triggered simultaneously for both the primary and secondary P-GW FQDN. Therefore, it is possible for both DNS resolutions to be successful. The focus is on the primary FQDN. However in the case of primary FQDN resolution failure, P-GW selection happens based on the secondary FQDN.



Important If the above CLI command is not configured then, the HSGW uses DNS to select the serving P-GW. The HSGW receives a list of all the P-GWs that serve the given APN. Then, the HSGW compares a list of P-GWs with the locally configured FQDN and selects the best matching P-GW.

Example

The following command enables the primary FQDN string in the configuration.

```
pgw fqdn primary  primary-fqdn-name
```

pilot-packet

Configures Pilot packet. The maximum number of pilot packet servers that can be configured is 8. Attempting to configure a 9th pilot packet server will result in the following error message:

```
Failure: Maximum number of Pilot packet servers that can be configured is 8. Limit exceeded
```

Note These IP destinations are IPv4 nodes. IPv6 is not supported

Product

P-GW

SAEGW

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration

configure > context *context_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] pilot-packet name *pserver* **source-ip-address** *ip_address* **destination-ip-address** *ip_address* **destination-udp-port** *port_number* **dscp-marking** *dscp_value*

no

Disables the usage of Pilot packets.

pilot-packet

Configures Pilot packet.

name *pserver*

Configures Pilot packet.

source-ip-address *ip_address*

Configures source ip address for sending Pilot packets.

destination-ip-address *ip_address*

Configures destination ip address for sending Pilot packets.

destination-udp-port *port_number*

Configures destination UDP port number for sending Pilot packets.

dscp-marking *dscp_value*

Configures DSCP value for Pilot packets.

Usage Guidelines

Use this command to configure Pilot packet.

Example

The following command enables Pilot packet functionality:

```
pilot-packet
```

The following command disables Pilot packet functionality:

```
no pilot-packet
```

pilot-packet attribute

Configures specific attributes to be included in the Pilot packet.

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

```
configure
   context context_name
     pilot-packet { attribute { foreign-agent-ip-address | nai | rat-type
 | serving-nw-id | flexible-services-container | apn-name |
virtual-apn-name } | name server_name source-ip-address source_ip_address
 | trigger rat-change generate { nat-info-only | user-info-and-nat-info
| user-info-only } }
     default pilot-packet { attribute { foreign-agent-ip-address | nai |
 rat-type | serving-nw-id | flexible-services-container } | trigger
rat-change }
     no pilot-packet { attribute { foreign-agent-ip-address | nai |
rat-type | serving-nw-id | flexible-services-container | apn-name |
virtual-apn-name } | name server_name | trigger rat-change }
     end
```

no

Disables the usage of Pilot-packet attribute.

pilot-packet attribute

Configures specific attributes to be included in the Pilot packet.

foreign-agent-ip-address

Sends the Foreign Agent IP Address in the Pilot packets.

nai

Sends the Network Access Identifier (NAI) in the Pilot packets.

rat-type

Sends the Radio Access Technology (RAT) type in the Pilot packets.

serving-nw-id

Sends the Serving Network Identifier in the Pilot packets.

flexible-services-container

Sends the optional flexible-services-container TLV in Pilot packets, which includes enterprise-level information such as Enterprise Customer Profile Database Identification (ECPD ID) and Account Number.

apn-name

Sends the APN name in the Pilot packets.

virtual-apn-name

Sends the virtual APN name in the Pilot packets.

server_name source-ip-address source_ip_address

Configures the source IP address for sending Pilot packets.

rat-change generate nat-info-only

Generates Pilot packets on RAT change with NAT information only.

rat-change generate user-info-and-nat-info

Generates Pilot packets on RAT change with both user information and NAT information.

rat-change generate user-info-only

Generates Pilot packets on RAT change with user information only.

rat-change generate user-info-only

Generates Pilot packets on RAT change with user information only.

policy

Configures the Mobile IPv6 policy to set the action to be taken when IPv4/IPv6 subscriber packets need to be tunneled and the encapsulated packets exceed the tunnel maximum transmission unit (MTU).

Product

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

policy ipv6 tunnel mtu exceed { fragment [inner] | notify-sender } [default | no] policy ipv6 tunnel mtu exceed

default

IPv6: System will do a Path MTU (PMTU) discovery and send "ICMPv6 Packet Too Big" to the original sender if the subscriber packet exceeds MTU after encapsulation.

IPv4: System will do an outer IPv6 fragmentation if the packet exceeds MTU after encapsulation.

no

Disables this functionality.

ipv6 tunnel mtu exceed { fragment [inner] | notify-sender }

fragment: System will do an outer IPv6 fragmentation if the subscriber packet exceeds MTU after encapsulation.

inner:



Important When **policy ipv6 tunnel mtu exceed fragment inner** CLI command is configured, the ASR 5500 (without VPP) fragments the IPv6 fragments if the packet size is greater than the MTU that is configured under APN. If the packet is already fragmented, it results in two fragment headers for the IPv6 packet. This scenario can be avoided by either retaining the default settings of the configuration or by ensuring the MTU on P-GW matches the one configured on the peer.

For example, if MTU is set to 1500 between a SIP server and P-GW, and APN is configured with **data tunnel mtu 1300**:

- The SIP server sends a packet (say, SIP Invite) towards the UE with the size of 3000. As MTU is 1500, the packet is fragmented and received as two packets at P-GW with size of 1500 each.
- As P-GW is configured with MTU of 1300, it fragments these packets once again. As a result, there are four packets: 1300 + 200 + 1300 +200

As per IPv6 specifications, these double-fragmented packets cannot be reassembled and generates a reassembly-timeout message at the endpoint.

Note that this is a simplified example. In actual scenarios, when the GGSN/P-GW/SAEGW is configured with **data tunnel mtu 1300**, a smaller MTU is used that is based on tunnel overhead.

For more details, refer the *P-GW Administration Guide*.

IPv6: System will do a PMTU discovery and send "ICMPv6 Packet Too Big" to the original sender if the subscriber packet exceeds MTU after encapsulation.

IPv4: If packet will exceed tunnel MTU after encapsulation, based on DF bit and ignore-df config, the original IPv4 packet will be fragmented and then encapsulated so that it will not exceed MTU, or ICMP Error will be sent if IPv4 packet fragmentation is not allowed.

notify-sender:

IPv6: System will do a PMTU discovery and send "ICMPv6 Packet Too Big" to the original sender if subscriber packet exceeds MTU after encapsulation.

IPv4: System will do an outer IPv6 fragmentation if packet exceeds MTU after encapsulation.

Usage Guidelines

This command sets the Mobile IPv6 policy for the action to be taken when IPv4/IPv6 subscriber packets need to be tunneled and the encapsulated packets exceed tunnel MTU size.

Example

The following command causes the system to do outer IPv6 fragmentation if the subscriber packet exceeds MTU after encapsulation:

```
policy ipv6 tunnel mtu exceed fragment
```

ppp

Configures the Point-to-Point Protocol (PPP) options for the current 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

```
ppp { data-compression { protocols protocols | mode modes } | keepalive seconds
| min-compression-size min_octets | mtu max_octets | l2tp allow-auth-without-pco
 }
default ppp { data-compression protocols | keepalive | min-compression-size
 | mtu | l2tp allow-auth-without-pco  }
no ppp { data-compression protocols | keepalive seconds | mtu | l2tp
allow-auth-without-pco }
```

default

Configures the default PPP parameters for the specified APN.

no

Resets the option specified to its default setting.

data-compression { mode *modes* | protocols *protocols*}

Configures the data compression or the compression protocol to use for the APN. Default: all protocols enabled

mode *modes*: Sets the compression mode to one of the following:

- **normal**: Packets are compressed using the packet history for automatic adjustment and for best compression.
- **stateless**: Each packet is compressed individually.

protocols *protocols*: Sets the compression protocol to one of the following:

- **deflate**: DEFLATE algorithm
- **mppc**: Microsoft Point-to-Point Compression
- **stac**: STAC LZS algorithm

keepalive *seconds*

Specifies the frequency of sending the Link Control Protocol (LCP) keep alive messages. *seconds* must be either 0 or an integer from 5 through 14400. The special value 0 disables the keep alive messages entirely. Default: 30

min-compression-size *min_octets*

Specifies the smallest packet to which compression may be applied as an integer from 0 through 2000. Default: 128

mtu *max_octets*

Specifies the maximum transmission unit (MTU) for packets accessing the APN as an integer from 100 through 2000. Default: 1500



Important The MTU refers to the PPP payload which excludes the two PPP octets. Therefore, an MTU of 1500 corresponds to the 3GPP standard MTU of 1502 for GTP packets with PPP payloads.

l2tp

Configures PPP L2TP specific parameters

allow-auth-without-pco

Allows P-GW PPP authentication for a L2TP call to be successful when PCO IE is not received in Create Session Request.

Usage Guidelines Adjust packet sizes and compression to improve bandwidth utilization. Each network may have unique characteristics such that determining the best packet size and compression options may require system monitoring over an extended period of time.

Example

The following command configures the ppp data-compression mode for the APN to be *stateless*:

```
ppp data-compression mode stateless
```

The following command configures an MTU of *500* for the APN:

```
ppp mtu 500
```

Example

The following command configures PPP L2TP specific parameters and allows P-GW PPP authentication for a L2TP call to be successful when PCO IE is not received in Create Session Request:

```
ppp l2tp allow-auth-without-pco
```

proxy-mip

Configures support for Proxy Mobile IP functionality for the APN.

Product GGSN

FA

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 `[ default | no ] proxy-mip { required | null-username static-homeaddr }`

default

Configures the default proxy MIP setting for the specified APN

no

Disables this functionality.

required

Default: Disabled.

Enables proxy-mip for all subscribers using this APN.

null-username static-homeaddr

Configures handling of RRQ to enable the acceptance without an NAI extension in this APN. Default: Disabled

Usage Guidelines

This command requires that Proxy Mobile IP functionality be performed for all PDP contexts facilitated by the APN.

When Proxy Mobile IP is performed, the system performs subscriber authentication but not Mobile IP FA authentication. It can be configured to handling of RRQ without NAI extension in an APN.

More information about Proxy Mobile IP support for the GGSN can be found in the *GGSN Administration Guide*.

Example

The following command causes the system to support Proxy Mobile IP for all PDP contexts facilitated by the APN:

```
proxy-mip required
```

The following command will enables the accepting of RRQ without NAI extensions in this APN.

```
proxy-mip null-username static-homeaddr
```

qci

Specifies the QoS Class Index (QCI) value to be used to mark bearers classified as IMS media for preferential treatment during session recovery and ICSR switchover.

Product

GGSN

P-GW

S-GW

SAE-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

qci *value_bytes* **ims-media**
no qci *value_bytes* **ims-media**

no

Disables this IMS QCI feature.

ims-media

Marks bearers classified as IMS media for preferential treatment during session recovery and ICSR switchover.

value_bytes

Specifies the QCI value an integer from 1 through 254.

Usage Guidelines

Use this command to specify the QCI value to be used to mark bearers classified as IMS media for preferential treatment during session recovery and ICSR switchover.

The following prerequisites apply to the implementation of this feature:

- A dedicated APN must be reserved for VoLTE traffic.
- A call connected to this APN will not be classified as Active VoLTE unless there is a dedicated bearer matching the VoLTE-configured QCI.
- Preferential treatment would be given to only those calls which are active VoLTE.
- A GGSN call connected to this APN will not be classified as Active VoLTE unless there is network initiated bearer matching the VoLTE-configured QCI.
- VoLTE marking is preserved across a Gn-Gp handoff.

When this feature is enabled via a CLI command, the actions are taken:

- During bearer creation
  - New bearer QCI is matched against APN configuration.
  - If the QCI matches an APN configuration, the bearer is marked for preferential treatment.
  - Flow_entries are modified with this information (if this is first VoLTE bearer).
  - Egtpu_session is updated with the VoLTE tag during a rx_setup request.
  - An indication message informs ECS about the VoLTE tagging.
- During bearer deletion
  - Flow_entry is updated with VoLTE information if this is the last VoLTE bearer.
  - ECS is informed of the deletion via an indication message.

Example

The following command enables preferential treatment for IMS bearers with a QCI of 9:

```
qci 9 ims-media
```

qos negotiate-limit

Cconfigures the QoS profile to provide the peak and committed data rate limits that the GGSN assigns to the APN. The GGSN sends the QoS profile to the SGSNs in response to GTP Create/Update PDP Context requests for traffic shaping and policing functionality.

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

```
qos negotiate-limit direction { downlink | uplink } [ qci qci_val ] [
peak-data-rate bps [ committed-data-rate bps ] | committed-data-rate [
peak-data-rate bps ] ]
no qos negotiate-limit direction { downlink | uplink } [ qci qci_val ] }
```

no

Disables the QoS Profile for the APN.

direction { downlink | uplink }

downlink: Apply the specified limits and actions to the downlink (to-Gn direction).

uplink: Apply the specified limits and actions to the uplink (to-Gi direction).

qci *qci_val*

qci_val is the QoS Class Identifier (QCI) for which the negotiate limit is being set. QCI ranges from 1 to 9. If no qci-val is configured, it will be handled as an undefined-qci (same as undefined-qos class).

committed-data-rate *bps*

Default: See the *Usage* section for this command

The committed data rate (guaranteed-data-rate) in bps (bits per second).

bps must be an integer from 1 through 16000000 for the downlink direction or 1 through 8640000 for the uplink direction. The value must also correspond to one of the permitted values identified the tables below. If a non-permitted value is entered for this parameter, the system rounds the value to the nearest lower supported value, except in the case where value is less than 1,000 bps. In this case, the system rounds the value to 1,000 bps. In addition, if the configured committed rate is lower than the value configured for the peak-data-rate, the system uses the configured peak rate for this parameter.



Important System measurements for this value exclude the GTP and outer packet headers. In addition, some traffic classes have both a committed rate and a peak rate, while other traffic classes have just a peak rate. If a committed rate is not applicable (such as, the traffic class is **background** or **interactive**), an error occurs if this option is configured. If the committed-rate is applicable (such as, the traffic class is **conversational** or **streaming**), the values supplied by the SGSN are used if this option is not configured.

peak-data-rate *bps*

Default: See the *Usage* section for this command

Specifies the peak data-rate for the subscriber in bps (bits per second).

bps must be an integer from 1 through 16000000 for the downlink direction or 1 through 8640000 for the uplink direction. The value must also correspond to one of the permitted values identified in the tables below. If a non-permitted value is entered for this parameter, the system rounds the value to the nearest lower supported value, except in the case where value is less than 1,000 bps. In this case, the system rounds the value to 1,000 bps.

Usage Guidelines

This command configures the APN quality of service (QoS) profile. This feature enables configuring and enforcing bandwidth limitations on individual PDP contexts of a particular traffic class. Traffic classes are defined in 3GPP TS 23.107 and are negotiated during PDP context activation. Bandwidth enforcement is configured and enforced independently for the downlink and the uplink directions.

The profile information is sent to the SGSN(s) in response to GTP Create/Update PDP Context Request messages. If the QoS profile requested by the SGSN is lower than the configured QoS profile configured, the profile requested by the SGSN is used. If the QoS profile requested by the SGSN is higher, the configured rates are used.

Note that the values for the uplink/downlink committed-data-rate and peak-data-rate parameters are exchanged in the GTP messages between the GGSN and the SGSN. Therefore, the values used may be lower than the configured values. When negotiating the rate with the SGSN(s), the system convert this to a value that is permitted by GTP as shown in the tables below.

Table 4: Permitted Values for Committed and Peak Data Rates in GTP Messages

Value (bps)	Increment Granularity (bps)
From 1000 to 63,000	1,000 (e.g 1000, 2000, 3000, ... 63000)
From 64,000 to 568,000	8,000 (e.g. 64000, 72000, 80000, ... 568000)
From 57,6000 to 8,640,000	64,000 (e.g. 576000, 640000, 704000, ... 86400000)
From 8,700,000 to 16,000,000	100,000 bps (e.g. 8700000, 8800000, 8900000, ... 16000000)

The command can be entered multiple times to specify different combinations of direction and class. If this command is not configured at all, the GGSN does not perform traffic policing or QoS negotiation with the SGSN.

Additional information on the QoS traffic shaping functionality is located in the *System Administration Guide*.

Default Values:

Example

The following command sets an uplink peak data rate of 128000 bps for QoS negotiation limit:

```
qos negotiate-limit direction uplink peak-data-rate 128000
```

qos rate-limit

Configures the action on a subscriber traffic flow that violates or exceeds the peak/committed data rate under traffic policing functionality.

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

```
qos rate-limit direction { downlink | uplink } [ qci qci_val ] [ burst-size
 { bytes | auto-readjust [ duration dur ] } ] [ exceed-action { drop |
lower-ip-precedence | transmit } [ violate-action { drop |
lower-ip-precedence | shape [ transmit-when-buffer-full ] | transmit } ]
 ] | [ violate-action { drop | lower-ip-precedence | shape [
transmit-when-buffer-full ] | transmit } [ exceed-action { drop |
lower-ip-precedence | transmit } ] ] +
no qos rate-limit direction { downlink | uplink } [ qci qci_val ]
```

no

Disables the QoS data rate limit configuration for the APN.

Important When no Qos Profile is configured, the system defaults to using the information provided by the SGSN.

qos rate-limit direction { downlink | uplink }

downlink: Apply the specified limits and actions to the downlink (the Gn direction).

uplink: Apply the specified limits and actions to the uplink (the Gi direction).

qci *qci_val*

qci_val is the QoS Class Identifier (QCI) for which the negotiate limit is being set. QCI ranges from 1 to 9 or 80, 82 and 83.

If no qci-val is configured, it will be handled as an undefined-qci (same as undefined-qos class).

burst-size { *bytes* | auto-readjust [duration *dur*] }

Default: See *Usage* section for this command.

The burst size allowed, in bytes for peak data rate and committed data rate.

bytes must be an integer from 1 through 6000000.



Important It is recommended that the minimum value of this parameter be configured to the greater of the following two values: 1) three times greater than packet MTU for the subscriber connection, OR 2) 3 seconds worth of token accumulation within the "bucket" for the configured peak-data-rate. In addition, if the committed-data-rate parameter is specified, the burst-size is applied to both the committed and peak rates.

auto-readjust [duration *dur* **]** keyword provides the option to calculate the Burst size dynamically while configuring the rate-limit. Whenever this keyword is enabled to calculate burst size, the GGSN QoS negotiated rate is enforced for this calculation.

Whenever there is a change in the rates (due to a QoS update), the burst sizes will be updated accordingly.

This keyword also provides two different burst sizes. One burst size for peak rate and another for committed rate.

By default this keyword is disabled.

duration *dur* describes the duration of burst in seconds. If duration is not specified this keyword will use 1 second as default value.

dur must be an integer between 1 through 30.

exceed-action { drop | lower-ip-precedence | transmit }

The action to take on the packets that exceed the committed-data-rate but do not violate the peak-data-rate. The following actions are supported:

- **drop**: Drop the packet.
- **lower-ip-precedence**: Transmit the packet after lowering the ip-precedence.
- **transmit**: Transmit the packet.

violate-action { drop | lower-ip-precedence | shape [transmit-when-buffer-full] | transmit }

The action to take on the packets that exceed both the committed-data-rate and the peak-data-rate. The following actions are supported:

- **drop**: Drop the packet.
- **lower-ip-precedence**: Transmit the packet after lowering the IP precedence.
- **shape [transmit-when-buffer-full]**: This keyword is not supported in this release.



Important Traffic Shaping is not supported on the GGSN, P-GW, or SAEGW.

- **transmit**: Transmit the packet.

+

More than one of the above keywords can be entered within a single command.

Usage Guidelines

This command configures APN quality of service (QoS) through traffic policing. This command enables the actions on subscriber flows exceeding or violating the allowed peak/committed data rate.

Important This command is not intended for bearer level policing

Important If the exceed/violate action is set to "lower-ip-precedence", this command may override the configuration of the **ip qos-dscp** command in the GGSN Service Configuration mode for packets from the GGSN to the SGSN. In addition, the GGSN service **ip qos-dscp** command configuration can override the APN setting for packets from the GGSN to the Internet. Therefore, it is recommended that this command not be used in conjunction with this action.

The command can be entered multiple times to specify different combinations of direction and class. If this command is not configured at all, the GGSN does not perform traffic policing or QoS negotiation with the SGSN. (It accepts all of the SGSN-provided values for the PDP context.)

To calculate the burst size dynamically, an optional keyword **auto-readjust** [**duration** *dur*] is provided with the **burst-size** keyword. By default, the burst size is fixed if defined in bytes with this command. Regardless of the rate being enforced, burst-size is fixed as set by the **burst-size** *bytes* parameter.

The **auto-readjust** [**duration** *dur*] keyword enables variable burst size depending on the rate being enforced. The system calculates burst size using a per token bucket algorithm calculation as T=B/R, where T is the time interval, B is the burst size and R is the Rate being enforced. It also provides different burst size for Peak and Committed data rate-limiting.

If the **auto-readjust** keyword is not used, a fixed burst size must be defined which will be applicable for peak data rate and committed data rate regardless of the rate being enforced.

If the **auto-readjust** keyword is provided without specifying the duration, a default duration of 1 second will be used for burst size calculation.

Example

The following command lowers the IP precedence when the committed-data-rate and the peak-data-rate are violated in uplink direction:

```
qos rate-limit direction uplink violate-action lower-ip-precedence
```

qos-renegotiate

This command is obsolete.

qos traffic-police

This command is obsolete. This functionality is now supported through **qos negotiate-limit** and **qos rate-limit** commands.

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)#
```

radius

This command is obsolete.

radius group

This command is obsolete.

radius returned-framed-ip-address

Sets the policy whether or not to reject a call when the RADIUS server supplies 255.255.255.255 as the framed IP address and the MS does not supply an address.

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

```
radius returned-framed-ip-address 255.255.255.255-policy {
accept-call-when-ms-ip-not-supplied | reject-call-when-ms-ip-not-supplied
 }
default radius returned-framed-ip-address 255.255.255.255-policy
```

default

Set the policy to its default of rejecting calls when the RADIUS server supplies framed IP address as 255.255.255.255 and the MS does not supply an address.

{ accept-call-when-ms-ip-not-supplied | reject-call-when-ms-ip-not-supplied }

accept-call-when-ms-ip-not-supplied: Accept calls when the RADIUS server supplies framed IP address as 255.255.255.255 and the MS does not supply an address.

reject-call-when-ms-ip-not-supplied: Reject calls when the RADIUS server supplies framed IP address as 255.255.255.255 and the MS does not supply an address.

Usage Guidelines

Use this command to set the behavior in the APN when the RADIUS server supplies 255.255.255.255 as the framed IP address and the MS does not supply an address.

Example

Use the following command to set the APN to reject calls when the RADIUS server supplies framed IP address as 255.255.255.255 and the MS does not supply an address:

```
radius returned-framed-ip-address 255.255.255.255-policy
reject-call-when-ms-ip-not-supplied
```

radius returned-username

Configures the username that is returned in accounting messages. If the username is not available in the Protocol Configuration Options (PCO), the RADIUS returned username is preferred to the constructed username (imsi@apn, msisdn@apn, or outbound username).

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

```
radius returned-username { override-constructed-username |
prefer-constructed-username }
default radius returned-username
```

default

The default value for the RADIUS returned-username is prefer-constructed-username. The constructed username (imsi@apn, msisdn@apn) will be used.



Important If the username is available in the PCO, that username will be used regardless of the setting for this command (radius returned-username).

override-constructed-username

If the RADIUS server returns a username in the Access-Accept message and that username is not available in the Protocol Configuration Options (PCO), the new username from the RADIUS server will be used.

prefer-constructed-username

If the username is not available in the PCO, a constructed username (imsi@apn, msisdn@apn) will be used regardless of the username from the RADIUS server. This is the default.

Usage Guidelines Use this command to configure the username that is returned in accounting messages

Example

Following command sets the default value for the RADIUS returned-username is prefer-constructed-username [constructed username (imsi@apn, msisdn@apn)]:

```
default radius returned-username
```

radius rulebase-format

This command enables/disables the Rulebase Concatenation feature at APN level. This feature is used to merge the prepaid attribute and SN1-Rulebase as a new rulebase and then apply the new rulebase to the session. If the Rulebase Concatenation feature is not enabled, the last received rulebase is applied to the session.



Important This command is license dependent. For more information, contact your Cisco account representative.

Product GGSN

PDSN

P-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

```
radius rulebase-format { custom1 | standard }
default radius rulebase-format standard
```

default

Disables the Rulebase Concatenation feature. The default setting is **standard**.

custom1

Specifies the rulebase as a custom value derived from multiple RADIUS attributes in the RADIUS Access-Accept response message.

standard

Specifies the rulebase as a single attribute value as obtained in RADIUS Access-Accept response message. This is the default setting.

Usage Guidelines

Currently, the Wireless Mobile Private Network (MPN) configures a dedicated rulebase per service. The Enterprise that utilizes this service has the rulebase per subscriber in 3G or signaled from AAA server with SN1-Rulebase attribute. In the case of a prepaid service, the rulebase name will be the customer-specific prepaid policy attribute received from the AAA server.

When both the RADIUS attributes are received, the last received attribute is considered and applied to the subscriber session. This CLI command is used to merge prepaid attribute and SN1-Rulebase as a new rulebase and then apply the new rulebase to the session on the gateway.



Important Rulebase Concatenation is a customer-specific feature and it requires a valid license to enable the feature. For more information, contact your Cisco account representative.

In 18 and earlier releases, rulebase was a single attribute value as obtained in the RADIUS Access-Accept response message. That is, only one rulebase can be applied with either SN1-Rulebase AVP or customer-specific prepaid policy AVP, whichever comes last.

In 19 and later releases, when both the attributes are received, the rulebase name will be a concatenation of the attributes as received in the Access-Accept response message. If only one of the attributes is received, the current behavior is applicable i.e. the last received attribute will be selected as the rulebase and it will be applied to the session.

If the concatenated rulesbase is not matching with the rulebase configured on the gateway, and/or if both the attributes are present more than once, then the session is rejected.

This feature implementation helps the MPN to customize the rulebase and combine prepaid service with additional services like Service Based Access (SBA).

Example

The following command merges the RADIUS attributes and installs the new concatenated rulebase.

```
radius rulebase-format custom1
```

reporting-action

Enables the reporting of APN-related events to a log. By default, reporting events to a log is disabled.

Product P-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 **`[ default | no ] reporting-action event-record`**

default

Disables reporting of events to a log. By default, reporting is disabled.

no

Disables reporting of events to a log if reporting has been enabled.

Usage Guidelines Use this command to enable the reporting of APN-related events to a log. By default, reporting is disabled.

Example

The following command enables reporting of events to a log:

`reporting-action event-record`

restriction-value

Configures the level of restriction to ensure controlled co-existence of the Primary PDP Contexts.

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 **`restriction-value`** *`value`*
`[ default | no ] restriction-value`

default | no

Default: no restriction-value

Entering either **default** or **no restriction-value** sets the internal value to zero (0) so that connection to any APN is allowed.

value

Specifies a unique number that identifies the type of network supported for primary PDP contexts facilitated by this APN. The following values are supported:

- *1*: Value used for Wireless Application Protocol (WAP) or Multimedia Messaging Service (MMS) type of networks. This corresponds to APN type public-1.
- *2*: Value used for Internet or Packet-Switched Public Data Network (PSPDN) type of networks. This corresponds to APN type public-2.
- *3*: Value used for corporate customers who use MMS. This corresponds to APN type private-1.
- *4*: Value used for corporate who do not use MMS. This corresponds to APN type private-2.

Usage Guidelines

Restricts the ability to have connections to public access and certain private APNs as required by the APN configuration. Also allows co-existence of the Primary PDP Contexts in a controlled manner.

It does not restrict the total number of Primary PDP Contexts for the user. It also configures a method for preventing hackers in the public domain from using the UE as a router.

Access is provided based on the following rules:

- If *value* = 1, then PDP contexts with restriction values of 0, 1, 2, and/or 3 are allowed
- If *value* = 2, then PDP contexts with restriction values of 0, 1 and/or 2 are allowed
- If *value* = 3, then PDP contexts with restriction values of 0 and/or 1 are allowed
- If *value* = 4, then PDP contexts with no restriction values are allowed
- If **default** or **no** syntax is entered, then no PDP contexts have restriction

In the event that a Maximum APN Restriction value is received from the SGSN as part of a PDP Context Create (CPCR) or Update (UPCR) message, the GGSN allows the request based on the following matrix:

- If maximum = 0, then allow connection to any APN
- If maximum = 1, then allow APN Restriction values of 0, 1, 2, and/or 3
- If maximum = 2, then allow APN Restriction values of 0, 1 and/or 2
- If maximum = 3, the allow APN Restriction values of 0 and/or 1
- If maximum = 4, then always reject
- If maximum = anything else, then allow all APN Restriction values (1, 2, 3, and/or 4)

Refer to 3GPP 23.060 version 6.9.0 for more information.

Example

The following command sets the restriction value of the APN to *2*:

```
restriction-value 2
```

secondary ip pool

This command specifies a secondary IP pool to be used as backup pool for Network Address Translation (NAT).

Important This command is license dependent. For more information please contact your Cisco account representative.

Product

NAT

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

secondary ip pool *pool_name*
no secondary ip pool

no

Removes the previous secondary IP pool configuration.

pool_name

Specifies the secondary IP pool name.

pool_name must be an alphanumeric string of 1 through 31 characters.

Usage Guidelines

Use this command to configure a secondary IP pool for NAT subscribers, which is not overwritten by the RADIUS supplied list. The secondary pool configured will be appended to the RADIUS supplied IP pool list / APN provided IP pool list whichever is applicable during call setup.

Example

The following command configures a secondary IP pool named *test123*:

```
secondary ip pool test123
```

selection-mode

Configures the level of verification that will be used to ensure a mobile station's subscription to use 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

selection-mode { chosen-by-sgsn | sent-by-ms | subscribed } + default selection-mode

default

Sets the default selection mode as "subscribed".

chosen-by-sgsn

Default: Disabled

The MS's subscription will not be verified and the APN will be provided by the SGSN.

sent-by-ms

Default: Disabled

The MS's subscription will not be verified and the APN will be provided by the MS.

subscribed

Default: Enabled

The MS's subscription will be verified by the SGSN.

+

More than one of the above keywords can be entered within a single command.

Usage Guidelines

Use this command to specify the level of verification that will be used to ensure a MS's subscription to use this APN. This setting must mach the corresponding setting on the SGSN. If the two settings are not identical, the GGSN rejects the session with a cause code of 201 (D1H, User authentication failed).

Example

The following command specifies that the MS's subscription will not be verified and that the APN name will be supplied by the SGSN:

```
selection-mode chosen-by-sgsn
```

stats-profile

Associates a statistics profile with a configured APN to support the Per QCI Packet Drop Counters and ARP Granularity for QCI Level Counters feature.



Important ARP Granularity for QCI Level Counters is a license-controlled feature. Per QCI Packet Drop Counters functionality does not require a license. Contact your Cisco account or support representative for licensing details.

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

[no] stats-profile *stats_profile_name*

no

disassociates the statistics profile with the specified APN.

stats-profile *stats_profile_name*

Specifies the existing statistics profile to associate with this APN. Statistics profiles are configured in *Global Configuration Mode* with the **stats-profile** command.

Usage Guidelines

Statistics profiles enable operators to monitor QoS statistics that identify multiple services running with the Statistics profiles enable operators to monitor QoS statistics that identify multiple services running with the same QCI value. In addition, packet drop counters have been introduced to provide the specific reason the Enhanced Charging Service (ECS) dropped a packet. The packet drop counters provide output on a per ARP basis. This provides additional information that operators can use to troubleshoot and identify network issues that may be affecting service.

For detailed information on this feature, refer to the *Per QCI Packet Drop Counters and ARP Granularity for QCI Level Counters* chapter in the *P-GW Administration Guide* or the *SAEGW Administration Guide*.

Example

The following command associates the stats-profile STATS with the APN:

stats-profile *STATS*

timeout

Configures the session timeout values for 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

timeout { absolute | qos-renegotiate } *time* **[del-cause { none | reactiv-req }]**
[default | no] timeout [absolute | qos-renegotiate] [del-cause]

default

Set the default value for the followed option.

no

Returns the timeout parameter to its default setting. If neither the absolute or idle keywords are used in conjunction with this keyword, both timeout options will be returned to their default settings.

absolute

Configures the absolute maximum time a session may exist in any state (active or idle).

qos-renegotiate

This keyword is obsolete.

time

Default:

- absolute = 0 (Disabled)
- qos-renegotiation = 300

Measured in seconds, the time can be configured to any integer value between 0 and 4294967295.

A time of 0 disables timeouts for this APN.

del-cause { none | reactiv-req }

When subscribers are deleted due to APN timeouts, the GGSN/P-GW/SAEGW may include "Cause-IE" in the resulting Delete Bearer/Delete PDP Context Requests generated for default bearer.

none: Omit GTP "Cause-IE" in DBR/DPC when timeout occurs on default bearer.

reactiv-req: The DBR/DPC will include "Cause-IE" with GTP cause code "Reactivation Requested".

This behavior is applicable only if Delete Bearer Request is sent for default bearer, or Delete PDP Context is sent to delete the PDN connection or its last PDP context.

The behavior for "Cause-IE" specified in this CLI shall override the cause-code set by existing features.

By default, the **del-cause** option is not defined and existing behavior is retained.



Important This option is only valid when Cause IE Enhancement for Delete Bearer Request license is enabled. Contact your Cisco account representative for more information.

Usage Guidelines Use this command to limit the amount of time that a subscriber session can remain connected or as a QoS renegotiation dampening timer.

Example

The following commands enables an absolute time timeout of *60000* seconds:

```
timeout absolute 60000
```

timeout bearer-inactivity

This command configures the bearer inactivity timer and the threshold value of the traffic through an APN. The bearer inactivity timer can also be configured to exclude default bearer/primary bearer from monitoring bearer inactivity.

Product GGSN

P-GW

SAEGW

SGW

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

In StarOS 15.0 and later releases:

```
timeout bearer-inactivity [ gbr | non-gbr ] dur_seconds volume-threshold {
 downlink | total | uplink } bytes
timeout bearer-inactivity del-cause { none | reactiv-req }
timeout bearer-inactivity exclude-default-bearer
[ default | no ] timeout bearer-inactivity [ del-cause |
exclude-default-bearer | gbr | non-gbr ]
```

In StarOS 14.x and earlier releases:

```
timeout bearer-inactivity dur_seconds volume-threshold total bytes
[ default | no ] timeout bearer-inactivity
```

default

Sets the bearer inactivity timer to disabled mode.

no

Removes the configured bearer inactivity timer values and traffic threshold limit.

timeout

Specifies that a bearer time out value will be configured for this APN.

gbr

Specifies that the GGSN/GW will check for low activity on a GBR bearer.

non-gbr

Specifies that the GGSN/GW will check for low activity on a non-GBR bearer.



Important P-GW only supports non-GBR bearer type sessions.

dur_seconds

Specifies the timeout duration in seconds to check inactivity on the bearer.

In StarOS 16.0 and later releases:

dur_seconds must be an integer value from 300 to 2592000 (5 minutes to 720 hours). The minimum configurable value of bearer inactivity timer was reduced from 900 seconds to 300 seconds.

In StarOS 15.0 releases:

dur_seconds must be an integer value from 900 to 2592000 (15 minutes to 720 hours). The minimum configurable value of bearer inactivity timer was reduced from 3600 seconds to 900 seconds.

In StarOS 14.x and earlier releases:

dur_seconds must be an integer value from 3600 through 2592000.

volume-threshold

This keyword sets the volume threshold in bytes to check the low activity on the bearer.

downlink

Threshold value of the downlink data traffic in a bearer.

total

Specifies that the total of both uplink and downlink data will be used as a volume threshold.

uplink

Threshold value of the uplink data traffic in a bearer.

bytes

bytes must be an integer value from 1 through 4294967295.

del-cause { none | reactiv-req }

When subscribers are deleted due to APN timeouts, the GGSN/P-GW/SAEGW may include "Cause-IE" in the resulting Delete Bearer/Delete PDP Context Requests generated for default bearer.

none: Omit GTP "Cause-IE" in DBR/DPC when timeout occurs on default bearer.

reactiv-req: The DBR/DPC will include "Cause-IE" with GTP cause code "Reactivation Requested".

This behavior is applicable only if Delete Bearer Request is sent for default bearer, or Delete PDP Context is sent to delete the PDN connection or its last PDP context.

The behavior for "Cause-IE" specified in this CLI shall override the cause-code set by existing features.

By default, the **del-cause** option is not defined and existing behavior is retained.



Important This option is only valid when Cause IE Enhancement for Delete Bearer Request license is enabled. Contact your Cisco account representative for more information.

exclude-default-bearer

Ignore bearer inactivity handling for default/primary bearer.

Usage Guidelines

Use this command to configure the bearer inactivity timer and the threshold value of the traffic through an APN. This enables the deletion of bearers experiencing less data traffic than the configured threshold value. Bearer inactivity timer is started only when time and volume threshold is configured.

Important Only one threshold is allowed to be configured per APN which is to monitor total, uplink, or downlink traffic.

The bearer inactivity timer can also be configured to exclude default bearer/primary bearer from monitoring bearer inactivity.

Example

The following command enables the inactivity time on the bearer with a timeout duration of *7200* seconds and the total traffic volume of *256000* bytes in uplink and downlink directions as thresholds:

```
timeout bearer-inactivity 7200 volume-threshold total 25600
```

timeout emergency-inactivity

Configures the emergency session inactivity-timeout for this APN. The APN must be configured as an emergency APN for Voice over LTE (VoLTE) E911 support.

Product

All

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

timeout emergency-inactivity *seconds*
[default | no] timeout emergency-inactivity

default | no

Indicates the timeout specified is to be returned to its default behavior. If no specific timeout is specified, then all are set to their default behavior.

seconds

Default: 0 (disabled)

Specifies the timeout duration, in seconds, to check inactivity on the emergency session.

seconds must be an integer value from 1 through 3600.

Usage Guidelines

Use this command to set the emergency session inactivity-timeout for this APN.

At reception of an IP CAN Session Modification Request triggered by the Policy and Charging Rules Function (PCRF) for an IP-CAN (IP Connectivity Access Network) session serving an IMS emergency session that removes all PCC rules with a QCI other than the default bearer QCI and the QCI used for IMS signalling, the Policy and Charging Enforcement Function (PCEF) shall start a configurable inactivity timer (to enable PSAP

Callback session). When the configured period of time expires, the PCEF shall initiate an IP-CAN Session Termination Request for the IP-CAN session serving the IMS Emergency session.

If a PCRF-Initiated IP-CAN Session Modification Request provides new PCC rule(s) with a QCI other than the default bearer QCI and the QCI used for IMS signalling, the PCEF shall cancel the inactivity timer.

Refer to the **emergency-apn** command in this chapter for additional information.

Example

The following command sets the emergency inactivity timeout duration to *450* seconds.

```
timeout emergency-inactivity 450
```

timeout idle

Configures the idle timeout duration for the long duration timer associated with a subscriber session.

Product

All

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

timeout idle *idle_dur* **[del-cause { none | reactiv-req }]**
[default | no] timeout idle [del-cause]

default | no

Indicates the timeout specified is to be returned to its default behavior. If no specific timeout is specified, then all are set to their default behavior.

idle_dur

Default: 0

Designates the maximum duration of the session (in seconds). After expiry the system considers the session as dormant or idle and terminates the session.

idle_dur must be an integer value in the range from 0 through 4294967295.

The special value 0 disables the timeout specified.

del-cause { none | reactiv-req }

When subscribers are deleted due to APN timeouts, the GGSN/P-GW/SAEGW may include "Cause-IE" in the resulting Delete Bearer/Delete PDP Context Requests generated for default bearer.

none: Omit GTP "Cause-IE" in DBR/DPC when timeout occurs on default bearer.

reactiv-req: The DBR/DPC will include "Cause-IE" with GTP cause code "Reactivation Requested".

This behavior is applicable only if Delete Bearer Request is sent for default bearer, or Delete PDP Context is sent to delete the PDN connection or its last PDP context.

The behavior for "Cause-IE" specified in this CLI shall override the cause-code set by existing features.

By default, the **del-cause** option is not defined and existing behavior is retained.



Important This option is only valid when Cause IE Enhancement for Delete Bearer Request license is enabled. Contact your Cisco account representative for more information.

Usage Guidelines Use this command to set the idle time duration for subscriber session to determine the dormant session.

Refer to the **long-duration-action detection** and **long-duration-action disconnection** command in this chapter for additional information.

Example

Following command sets the idle timeout duration to *450* seconds.

```
timeout idle 450
```

timeout idle micro-checkpoint-deemed-idle

Sends an event-based idlesec micro-checkpoint from an Active to a Standby chassis when the session state changes from active to idle or from idle to active.

Product All

Privilege Administrator, Security 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

```
timeout idle idle_dur [  micro-checkpoint-deemed-idle time_in_seconds  ]
{ default | no } timeout idle
```

default

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

no

Disables the timeout idle functionality.

timeout idle *idle_dur*

Designates the maximum duration of the session (in seconds). After expiry, the system considers the session as dormant or idle and terminates the session.

idle_dur must be an integer value in the range from 0 through 4294967295.

Default: 0

The special value 0 disables the timeout specified.

micro-checkpoint-deemed-idle *time_in_seconds*

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

time_in_seconds must be an integer from 10 to 1000.

Default: 180

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

Usage Guidelines

Use **micro-checkpoint-deemed-idle** to send an idlesec micro-checkpoint from an active to standby chassis when the session state changes from active to idle or from idle to active. The micro-checkpoint carries information about the time when the session became active or idle. Upon receipt of the micro-checkpoint, the standby chassis updates the active/idle time. This process enables the active and standby chassis to be synchronized with respect to when a particular session became active or idle. Since this feature is event-based, it enables the chassis to send micro-checkpoints only when an event occurs, as opposed to sending micro-checkpoints based on a configured time duration, which sends the micro-checkpoints regardless of whether a session state change occurred or not.

Using **micro-checkpoint-deemed-idle** results in a more efficient event-based sending of micro-checkpoints to the standby chassis and also increases SRP bandwidth.

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

Example

This command sets the **timeout idle** value to 300 seconds and the **micro-checkpoint-deemed-idle** setting to 180 seconds.

```
timeout idle 300 micro-checkpoint-deemed-idle 180
```

timeout idle micro-checkpoint-periodicity

Enables configuration of periodic idle seconds micro checkpoint timer on a per-APN basis.

Product

All

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

timeout idle *idle_dur* **[micro-checkpoint-periodicity** *time_in_seconds* **]**
{ default | no } timeout idle

default

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

no

Disables the timeout idle functionality.

idle_dur

Designates the maximum duration of the session (in seconds). After expiry, the system considers the session as dormant or idle and terminates the session.

idle_dur must be an integer value in the range from 0 through 4294967295.

Default: 0

The special value 0 disables the timeout specified.

micro-checkpoint-periodicity time_in_seconds

Configures periodic idle seconds micro-checkpoint timer on a per-APN basis.

Idle seconds micro-checkpoints are sent at the configured regular intervals to the standby chassis; otherwise, they are sent at intervals of 10 seconds, which is the default value.

time_in_seconds must be an integer value in the range from 0 through 4294967295.

Default: 10

Important

- The **micro-checkpoint-periodicity** value should be less than **idle timeout** value.
- When the **micro-checkpoint-periodicity** value is configured, the idle timeout timer starts *after* the micro checkpoint periodicity times out. If the **micro-checkpoint-periodicity** value is not configured, the session drops after the defined *idle_dur*.

Usage Guidelines

Use this command to set the idle time duration and micro-checkpoint-periodicity timer for subscriber session to determine the dormant session. Operators can configure this setting to a large value to suit their need to reduce the number of micro-checkpoints on the SRP link. When this CLI command is configured, idleseconds

micro-checkpoints are sent at configured regular intervals to the standby chassis. If not configured, micro-checkpoints are sent at intervals of 10 seconds, which is the default.



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

Example

Following command sets the idle timeout duration to 10 seconds and micro-checkpoint-periodicity to 15 seconds.

```
timeout idle 10 micro-checkpoint-periodicity 15
```

timeout long-duration

Configures the long duration timeout and inactivity duration for subscriber sessions.

Product All

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

```
timeout long-duration ldt_timeout [ inactivity-time inact_timeout ]
no timeout long-duration
```

no

Indicates the timeout specified is to be returned to its default behavior. If no specific timeout is specified then all timeouts are set to their default behavior.

ldt_timeout

Default: 0

Designates the maximum duration of the session (in seconds) before the system automatically reports/terminates the session.

Specifies the maximum amount of time (in seconds) before the specified timeout action is initiated.

ldt_timeout must be an integer value in the range from 0 through 4294967295.

The special value 0 disables the timeout specified.

inactivity-time *inact_timeout*

Specifies the maximum amount of time (in seconds) before the specified session is marked as dormant.

inact_timeout must be an integer value in the range from 0 through 4294967295.

The special value 0 disables the inactivity time specified.

Usage Guidelines

Use this command to set the long duration timeout period and inactivity timer for subscriber sessions. Reduce the idle timeout to free session resources faster for use by new requests.

Refer to the **long-duration-action detection** and **long-duration-action disconnection** commands in this chapter for additional information.

Example

The following command sets the long duration timeout duration to *300* seconds and the inactivity timer for subscriber session to *45* seconds.

```
timeout long-duration 300 inactivity-time 45
```

tpo policy

The Traffic Performance Optimization (TPO) in-line service is not supported in this release.

tunnel address-policy

This command specifies the address allocation/validation policy for all tunneled calls (IP-IP, IP-GRE) except L2TP calls. This means that GGSN IP address validation could be disabled for specified incoming calls.

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

```
tunnel address-policy { alloc-only | alloc-validate | no-alloc-validate
}
default tunnel address-policy
```

default

Resets the tunnel address-policy to alloc-validate.

alloc-only

IP addresses are allocated locally and no validation is done.

alloc-validate

Default.

The VPN Manager allocates and validates all incoming IP addresses from a static pool of IP addresses.

no-alloc-validate

No IP address assignment or validation is done for calls arriving via L3 tunnels. Incoming static IP addresses are passed. This allows for the greatest flexibility.

Usage Guidelines

This command supports scalable solutions for Corporate APN deployment as many corporations handle their own IP address assignments. In some cases this is done to relieve the customer or the mobile operators from the necessity of reconfiguring the range of IP addresses for the IP pools at the GGSN.

For calls coming through L2TP tunnels, the command **l3-to-l2-tunnel address policy** as defined in the APN Configuration mode, will be in effect.

Example

Use the following command to reset the IP address validation policy to validate against a static pool of address:

```
default tunnel address-policy
```

Use the following command to disable all IP address validation for calls coming through tunnels:

```
tunnel address-policy no-alloc-validate
```

tunnel gre

Configures Generic Routing Encapsulation (GRE) tunnel parameters between the GGSN and an external gateway for the 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

tunnel gre peer-address *peer_address* **local-address** *local_addr* **[preference** *num* **]**
no tunnel gre peer-address *peer_address*

no

Disables GRE tunneling for the APN.

peer-address *peer_address*

Specifies the IP address of the external gateway terminating the GRE tunnel.

peer_address must be expressed in dotted decimal notation.

local-address *local_addr*

Specifies the IP address of the interface in the destination context of the GGSN originating the GRE tunnel.

local_addr must be expressed in IPv4 dotted-decimal notation.

preference *num*

Default: 1

This option can be used to assign a preference to the tunnel.

preference can be configured to any integer value from 1 to 128.

Important Only one GRE tunnel per APN is supported. Therefore, the preference should always be set to "1".

Usage Guidelines

Subscriber IP payloads are encapsulated with IP/GRE headers and tunneled by the GGSN to an external gateway.

Example

The following command configures the system to encapsulate subscriber traffic using GRE and tunnel it from a local address of *192.168.1.100* to a gateway with an IP address of *192.168.1.225*:

```
tunnel gre peer-address 192.168.1.225 local-address 192.168.1.100
preference 1
```

tunnel ipip

Configures IP-in-IP tunnelling parameters between the GGSN and an external gateway for the 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

tunnel ipip peer-address *peer_address* **local-address** *local_addr* **[preference** *num* **]**
no tunnel ipip

no

Disables IP-in-IP tunneling for the APN.

peer-address *peer_address*

Specifies the IP address of the external gateway terminating the IP-in-IP tunnel.

peer_address must be expressed in IPv4 dotted-decimal notation.

local-address *local_addr*

Specifies the IP address of the interface in the destination context of the GGSN originating the IP-in-IP tunnel.

local_addr must be expressed in IPv4 dotted-decimal notation.

preference *num*

Default: 1

If multiple tunnels will be configured, this option can be used to assign a preference to the tunnel.

preference can be configured to any integer value from 1 to 128.

Usage Guidelines

Subscriber IP payloads are encapsulated with IP-in-IP headers and tunneled by the GGSN to an external gateway.

Example

The following command configures the system to encapsulate subscriber traffic using IP-in-IP and tunnel it from a local address of *192.168.1.100* to a gateway with an IP address of *192.168.1.225*:

```
tunnel ipip peer-address 192.168.1.225 local-address 192.168.1.100
preference 1
```

tunnel ipsec

This command configures sessions for the current APN to use an Internet Protocol Security (IPSec) tunnel based on the IP pool corresponding to the subscribers assigned IP address.

Product 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 **[no] tunnel ipsec use-policy-matching-ip-pool**

no

Disables the use of the IPSec policy that matches the IP pool that the assigned IP address relates to.

Usage Guidelines Use this command to set the APN to use an IPSec policy that is assigned to the IP pool that the subscribers assigned IP address relates to.

Example

The following command enables the use of the policy that matches the IP pool address:

tunnel ipsec use-policy-matching-ip-pool

tunnel l2tp

Configures Layer 2 Tunnelling Protocol (L2TP) parameters between the GGSN and an external gateway for the 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

tunnel l2tp [peer-address *lns-address* **[[encrypted] secret** *l2tp_secret* **] [preference** *num* **] [tunnel-context** *name* **] [local-address** *ip-address* **] [crypto-map** *map_name* **{ [encrypted] isakmp-secret** *crypto_secret* **}] [local-hostname** *hostname* **]**
no tunnel [peer-address *lns-address***]**

no

Disables L2TP, or secure L2TP tunneling for the APN if a specific peer-address is not specified, or, if a peer-address is specified, this keyword removes the peer-address configuration from the APN.

peer-address *lns-address*

Specifies the IP address of the LNS node that the LAC service connects to.

lns-address must be expressed in IPv4 dotted-decimal notation.



Important A maximum of four LNS peers can be configured per APN.

encrypted

This keyword is intended only for use by the system while saving configuration scripts. The system displays the encrypted keyword in the configuration file as a flag that the variable following the secret keyword is the encrypted version of the plain text secret. Only the encrypted secret is saved as part of the configuration file.

secret *l2tp_secret*

Specifies the shared secret (password) between the L2TP Access Concentrator (LAC) service (configured on the system) and the LNS node.

l2tp_secret must be an alphanumeric string of 1 through 127 characters and is case sensitive.

preference *num*

Default: 1

Specifies the preference of the tunnel if the LAC service communicates with multiple LNS nodes.

preference can be configured to any integer value from 1 to 128.

tunnel-context *name*

Specifies the name of the destination context on the system in which the LAC service(s) is configured.

name must be an alphanumeric string of 1 through 79 characters and is case sensitive.



Important If this option is not configured, the system will attempt to determine the name of the destination context from the **ip context-name** parameter configured for the APN.

local-address *ip-address*

Specifies the IP address of an interface that is bound to a LAC service. This is a mechanism to dictate which LAC service to use to facilitate the subscriber's L2TP session.

address is the IP address of the interface in IPv4 dotted-decimal notation.

Important If the address configured does not exist or is not bound to a LAC service, the system will automatically choose a LAC service to use.

local-hostname *hostname*

This keyword configures LAC-Hostname to be used for the communication with the LNS peer for this APN.

When Tunnel parameters are not received from the RADIUS server, Tunnel parameters configured in APN are considered for the LNS peer selection. When APN Configuration is selected, local-hostname configured with the "tunnel l2tp" command in the APN for the LNS peer will be used as a LAC Hostname.

Important For this configuration to take effect **allow aaa-assigned-hostname** command, which is used to configure LAC-Hostname based on the "Tunnel-Client-Auth-ID" attribute received from the RADIUS server, needs to be configured in the LAC Service Configuration mode.

hostname is name of the local host for the LNS peer and must be an alphanumeric string of 1 through 127 characters.

When Tunnel parameters are not received from the RADIUS Server, Tunnel parameters configured in APN will be considered for the LNS peer selection. When APN Configuration is selected, the local hostname *hostname* configured with this command in the APN for the LNS peer will be used as a LAC Hostname.

crypto-map *map_name* { [encrypted] secret *crypto_secret* }

Configures the IPSec crypto-map policy that is to be associated with this L2TP tunnel configuration for secure L2TP.

map_name is the name of a crypto-map policy configured on the system expressed as an alphanumeric string of 1 through 127 characters and is case sensitive.

encrypted is intended only for use by the system while saving configuration scripts. The system displays the encrypted keyword in the configuration file as a flag that the variable following the secret keyword is the encrypted version of the plain text secret. Only the encrypted secret is saved as part of the configuration file.

secret specifies the secret associated with the crypto-map policy. *crypto_secret* can be from 0 to 255 bytes.

Usage Guidelines

This command can be used to configure the GGSN to tunnel subscriber traffic to one or more peer LNSs using L2TP or L2TP with IPSec.

When using L2TP, the system functions as a L2TP access Concentrator (LAC) and tunnels traffic to a peer L2TP Network Server (LNS). LAC functionality is supported through the configuration of LAC Services defined in destination contexts configured on the system.

When using crypt-map policies, the system functions in the same fashion as with L2TP, with the exception that the encapsulated L2TP traffic is further encrypted using IPSec. IPSec functionality is supported through the definition of crypto maps configured in the same destination context as the LAC services.

A maximum of four LNS peers can be configured per APN. If no peer is specified, the system will use the LAC Service(s) configured in the same destination context as the APN.

Example

The following command configures L2TP support for the APN. It configures the APN to tunnel traffic to an LNS with an IP address of 192.168.1.50 through a LAC service bound to an interface with an IP address 192.168.1.201 configured in a destination context on the system called pdn1. The shared secret between the system and the LNS is 5496secRet. This will be the only LNS configured so the default preference of 1 will not be changed.

```
tunnel l2tp peer-address 192.168.1.50 secret 5496secRet tunnel-context
pdn1 local-address 192.168.1.201
```

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
```

user-plane-group

Configures a User Plane group for the APN.

Product

CUPS

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

[no] user-plane-group *group_name*

no

Disables User Plane group for the APN.

Usage Guidelines

Use this command to configure a User Plane group for the APN.

virtual-apn gdcr

This command defines which APN (Gn or virtual) should be used in charging records.

Product

eWAG

GGSN

IPSG

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

virtual-apn { gcdr apn-name-to-be-included { gn | virtual }| truncate-s6b-vapn delimiter { dot [hyphen] | hyphen [dot] } }

default virtual-apn gcdr apn-name-to-be-included

no virtual-apn truncate-s6b-vapn delimiter [dot [hyphen] | hyphen [dot]]

default

Returns the CDR related parameters to the default values.

gcdr apn-name-to-be-included { *gn* | *virtual* }

Defines which APN is to be sent in charging records (CDR).

- **gn**: Use the Gn APN name received in the Create PDP Context Request message from SGSN or the S5 APN name received in the PDN Connectivity Request from MME.
- **virtual**: Use the virtual APN selected by the GGSN/P-GW. This is the default.

truncate-s6b-vapn delimiter { dot [hyphen] | hyphen [dot] }

Truncates virtual APN received from S6b at the configured character delimiter.

- **dot**: Configures the delimiter to dot (.) for truncation of S6b-VAPN
- **hyphen**: Configures the delimiter to hyphen (-) for truncation of S6b-VAPN

Both dot and hyphen delimiters can be configured in the same line or a new line. If the separator character is not present in the received S6b virtual APN name, then the whole virtual APN name will be considered for configuration look-up.

If AAA server returns both hyphen and dot delimiters or the same delimiter twice or more as a virtual-apn, then the first delimiter will be considered as a separator. For example, if the AAA server returns the virtual-apn as xyz-cisco.com, then hyphen is the separator.

This CLI command takes effect only when S6b server returns virtual APN name in Authentication Authorization Accept (AAA) message. By default this feature will be disabled and no delimiter will be configured.

For more information on the Virtual APN Truncation feature for Rf Records, see the administration guide for the product that you are deploying.

no

Disables the truncation of virtual APN name. If a particular delimiter needs to disabled, it should be done explicitly.

Usage Guidelines Defines which APN is to be sent in charging records (CDR), either the APN received in the Create PDP Context Request from the SGSN, or the APN received in the PDN Connectivity Request from the MME.

Example

The following command configures the gateway to use the APN supplied by the SGSN or MME.

```
virtual-apn gcdr apn-name-to-be-included gn
```

virtual-apn preference

Defines one or more criteria used to redirect a call received on a particular APN to another APN.

Product

GGSN

eWAG

IPSG

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 In StarOS 20.2 and later releases:

```
virtual-apn preference priority dcnrapn apn_name [ IPv4 { ip_address |
ipv4_address/mask } ] [ IPv6 ipv6_address | ipv6_address/mask } ] [
bearer-access-service service_name ] [ cc-behavior cc_behavior_value ] [
cc-profile cc_profile_index [ pre-rel-9.1-cc-behavior cc_behavior_value ] ] [
domain domain_name ] [ mcc mcc_number mnc mnc_number [ msin-range from
msin_range_from to msin_range_to ] ] [ msisdn-range from msisdn_start_range to
msisdn_to_range ] [ pdp-type { ipv4 | ipv6 | ipv4v6 } ] [ rat-type { eutran
 | gan | geran | hspa | utran | wlan } ] [ roaming-mode { home | roaming
 | visiting } ] [ tracking-area-code-range tac_range ][ serv-gw-plmnid
mccmcc_number mnc mnc_number ] +
no virtual-apn preference priority
```

In StarOS 20.1 and earlier releases:

```
virtual-apn preference priority apn apn_name  rat-type lte-m [ IPv4 { ip_address
 | ipv4_address/mask } ] [ IPv6 ipv6_address | ipv6_address/mask } ] [
bearer-access-service service_name ] [ cc-behavior cc_behavior_value [ rat-type
 { eutran | gan | geran | hspa | utran | wlan } ] ][ cc-profile
```

cc_profile_index **[pre-rel-9.1-cc-behavior** *cc_behavior_value* **] [rat-type { eutran | gan | geran | hspa | utran | wlan }]][domain** *domain_name* **] [mcc** *mcc_number* **mnc** *mnc_number* **[cc-behavior** *cc_behavior_value* **| cc-profile** *cc_profile_index* **[pre-rel-9.1-cc-behavior** *cc_behavior_value* **] | msin-range from** *msin_range_from* **to** *msin_range_to* **| rat-type { eutran | gan | geran | hspa | utran | wlan }] [msisdn-range from** *msisdn_start_range* **to** *msisdn_to_range* **[rat-type { eutran | gan | geran | hspa | utran | wlan }] [pdp-type { ipv4 | ipv6 | ipv4v6 } [roaming-mode roaming]] [rat-type { eutran | gan | geran | hspa | utran | wlan }] [roaming-mode { home | roaming | visiting }] [uut-profile** *profile_name* **]**
no virtual-apn preference *priority*

no

Removes a previously configured "virtual" APN.

preference *priority*

Specifies the order in which the referenced APNs are compared by the system.

priority specifies the order and can be configured to any integer value from 1 (highest priority) to 1000 (lowest priority).

apn *apn_name*

Specifies the name of an alternative APN configured on the system that is to be used for PDP contexts or PDN connections with matching properties.

apn_name is the name of the alternative APN expressed as an alphanumeric string of 1 through 62 alphanumeric characters and is case insensitive. It may also contain dots (.) and/or dashes (-).

dcnr

associates the DCNR profile with APN in CUPS.

rat-type lte-m

Enables LTE-M as an additional RAT-type.

IPv4 { *ipv4_address* | *ipv4_address/mask* }

Configures subnet range for subscriber IP.

ipv4_address must be an IPv4 address in dotted-decimal notation.

ipv4_address/mask must be an IPv4 address in dotted-decimal notation with network-host mask separation.

IPv6 { *ipv6_address* | *ipv6_address/mask* }

Configures subnet range for subscriber IP.

ipv6_address must be an IPv6 address in colon-separated-hexadecimal notation.

ipv6_address/mask must be an IPv6 address in colon-separated-hexadecimal notation with network-host mask separation.

access-gw-address { *ip_address* | *ip_address/mask* }

Specifies the Access Gateway (SGSN/S-GW/Other) IP address (or network) for this virtual APN.

ip_address must be an IPv4 address in dotted-decimal or an IPv6 address in colon-separated-hexadecimal notation.

ip_address/mask must be an IPv4 address in dotted-decimal or an IPv6 address in colon-separated-hexadecimal notation with network-host mask separation.

bearer-access-service *service_name*

Specifies the Bearer Access Service (GGSN/P-GW/Other) name. This service name is unique across the context.

service_name must be an alphanumeric string of 1 through 63 characters.

Important For eWAG and IPSG, this option is not supported in this release.

cc-behavior *cc_behavior_value*

Specifies the behavior charging characteristics bits in 16 bit format, post 3GPP release 9.1. For example, if cc-behavior is configured as 0x3412, then 0x34 corresponds to B15-B8 [MSB] and 0x12 corresponds to B7-B0 [LSB] of charging char)

cc_behavior_value must be a hex value in the range 0x0000 to 0xFFFF.

Important This option is supported only on GGSN, P-GW, and SAEGW in this release.

cc-profile *cc_profile_index*

Specifies the charging characteristics (CC)-profile index.

cc_profile_index must be an integer from 1 to 15.

Important For eWAG and IPSG, this option is not supported in this release.

domain *domain_name*

Specifies the domain name (realm). This is compared with the domain name portion of subscriber's username (user@domain).

domain_name must be an alphanumeric string of 1 through 79 characters, is case sensitive and can contain all special characters.

Important For eWAG and IPSG, this option is not supported in this release.

mcc *mcc_number* mnc *mnc_number*

mcc : Specifies the mobile country code (MCC) portion of the PLMN's identifier.

mcc_number is the PLMN MCC identifier and can be configured to any 3-digit integer value between 100 and 999.

mnc : Specifies the mobile network code (MNC) portion of the PLMN's identifier.

mnc_number is the PLMN MNC identifier and can be configured to any 2- or 3-digit integer value between 00 and 999.

Important For eWAG and IPSG, this option is not supported in this release.

msin-range from *msin_range_from* to *msin_range_to*

Important This option is supported only for the GGSN.

Specifies the IMSI MSIN range.

msin_range_from is the start prefix of the IMSI MSIN range and can be configured between 0 and 9999999999.

msin_range_to is the end prefix of the IMSI MSIN range and can be configured as a string of size 1 to 10 digits between 0 and 9999999999.

msin-range should obey the following rules:

- Start prefix (such as *msin_range_from*) and end prefix (such as *msin_range_from*) must be of the same length.
- Total length of mcc + mnc + msin-range <= 15 digits.

msisdn-range from *msisdn_start_range* to *msisdn_to_range*

Specifies the MSISDN range.

msisdn_start_range is the starting MSISDN number which a string of size 2 to 15 and its value ranges between 00 and 999999999999999.

msisdn_to_range is the ending MSISDN number which is also a string of size 2 to 15 and its value ranges between 00 and 999999999999999.

Important For eWAG, this option is not supported in this release.

pre-rel-9.1-cc-behavior *cc_behavior_value*

Specifies the behavior charging characteristics bits in 12 bit format, post 3GPP release 9.1. For example, if cc-behavior is configured as 0x341, then 0x34 corresponds to B12-B5 [MSB] and 0x1 corresponds to B4-B1 [Least significant nibble] of CC behavior).

cc_behavior_value must be a hex value in the range 0x0000 to 0xFFFF.

Important This option is supported only on GGSN, P-GW, and SAEGW in this release.

pdp-type { ipv4 | ipv4v6 | ipv6n }

Configures pdp-type rule.

The available options include:

- **ipv4**: Configures VAPN Rule for IPv4.
- **ipv4v6**: Configures VAPN Rule for IPv4v6.
- **ipv6**: Configures VAPN Rule for IPv6.

rat-type { eutran | gan | geran | hspa | utran | wlan }

The type of the Radio Access Technology (RAT).

The available options include:

- **eutran**
- **gan**
- **geran**
- **hspa**
- **utran**
- **wlan**

Important For eWAG, the rat-type keyword is not supported in this release.

roaming-mode { home | roaming | visiting }

Supports separate PDP context or PDN connection processing for roaming, visiting, and home subscribers.

Important For eWAG and IPSG, this option is not supported in this release.

serv-gw-plmnid

Specifies the Serving Gateway PLMN ID.

+

Keywords can be repeated or combined as needed in a single virtual-apn preference rule.

If the same option is provided multiple times in the same rule, then later option value will be considered for selection.

tracking-area-code-range *tac_range*

Configures APN for Tracking Area Code range. The *tac_range* is an integer value ranging from 0 to 65535.

uut-profile *profile_name*

Associates UE Usage Type (UUT) profile with APN. The *profile_name* is an integer value ranging from 1 to 65535.

Usage Guidelines

This command simplifies the configuration process for mobile operators allowing them to provide subscribers with access to a large number of packet data networks, characterized by APN templates, while only having to configure a small number of APNs on the HLR.

Each "virtual" APN is a reference, or a link, to an alternate APN configured on the system. Each reference is configured with a rule that subscriber PDP contexts or PDN connections are compared against and a priority that dictates the comparison order.

A maximum of 2048 virtual APN rules can be added across all APNs.



Important To modify an existing virtual APN rule, the current rule should be removed and a new rule with appropriate options added.

GGSN

The references works as follows:

1. A Create PDP Context Request message is received by the GGSN. The message specifies an APN configured in the HLR.

2. The GGSN determines whether its own matching APN configuration contains "virtual" APN references.

3. The system determines the priority of the references and compares the associated information pertaining to the PDP context against the configured rules.

4. If the rule matches, the parameters in the APN specified by the reference are applied to the PDP context. If not, the rules in the reference with the next highest priority are compared against the PDP context. This occurs until a match is found. If none of the references match, then the parameters within the current APN are applied to the PDP context.

The GGSN supports a maximum of 1023 Virtual APN mapping configurations in a system. A single Gn APN can be configured with up to 1000 mapping rules. Multiple Gn APNs are supported - each requiring Virtual APN mapping configurations. The limit imposed is that the total virtual APN mappings across all Gn APNs should not exceed 1023.

The functionality provided by this command can also be used to restrict access to particular APNs. To restrict access based on a particular criteria (domain name, mcc/mnc, etc.), the "virtual" APN reference should refer to an APN that is not configured on the system and contains the desired rule. All calls matching the configured rule would then be denied with a reason code of 219 (DBH), Missing or Unknown APN.

eWAG

For eWAG, in this release only the **access-gw-address** Virtual APN configuration option is supported.

For information on how virtual APN configuration can be used in eWAG deployments, refer to the *Enhanced Wireless Access Gateway Administration Guide*.

IPSG

For IPSG, in this release only the following Virtual APN configuration options are supported:

- **access-gw-address** (RADIUS client in the case of IPSG)

- **msisdn-range from** *msisdn_start_range* **to** *msisdn_to_range*
- **rat-type**

All these attributes are sent in access-request in Auth-Proxy mode or Acct-Start in other modes to trigger Virtual APN selection.

The functionality provided by this command can also be used to restrict access to particular APNs. To restrict access based on a particular criteria (domain name, mcc/mnc, etc.), the "virtual" APN reference should refer to an APN that is not configured on the system and contains the desired rule. All calls matching the configured rule would then be denied with a reason code of 219 (DBH), Missing or Unknown APN.

P-GW/SAEGW

The Virtual APN feature allows a carrier to use a single APN to configure differentiated services. The APN that is supplied by the MME is evaluated by the P-GW in conjunction with multiple configurable parameters. Then, the P-GW selects an APN configuration based on the supplied APN and those configurable parameters.

APN configuration dictates all aspects of a session at the P-GW. Different policies imply different APNs. After basic APN selection, however, internal re-selection can occur based on the following parameters:

- S-GW address: **access-gw-address**
- Service name: **bearer-access-service**
- Call control profile index: **cc-profile**
- Domain name part of username (user@domain): **domain**
- MCC-MNC of IMSI: **mcc** *mcc_number* **mnc** *mnc_number*
- MSISDN range: **msisdn-range from** *msisdn_start_range* **to** *msisdn_to_range*
- Subscriber type: **rat-type**



Important In StarOS v12.x and earlier, the P-GW supports a maximum of 1024 Virtual APNs in a system. In StarOS v14.0 and later, the P-GW supports a maximum of 2048 Virtual APNs in a system.

The functionality provided by this command can also be used to restrict access to particular APNs. To restrict access based on a particular criteria (domain name, mcc/mnc, etc.), the "virtual" APN reference should refer to an APN that is not configured on the system and contains the desired rule. All PDN connections matching the configured rule would then be denied with a reason code of 219 (DBH), Missing or Unknown APN.

Example

The following commands configure two "virtual" APNs. Priority 1 references the *bigco* APN with a domain rule of *bigco.com*. Priority 2 references the *bigtown* APN with a mobile country code rule of *100* and a mobile network code rule of *50*.

```
virtual-apn preference 1 apn bigco domain bigco.com
virtual-apn preference 2 apn bigtown mcc 100 mnc 50 msin-range from
4000000000 to 4999999999
virtual-apn preference 3 apn bigco.com access-gateway-address 192.168.62.2
```

```
virtual-apn preference 4 apn bigco.co.kr access-gateway-address
192.168.60.2/24
```