APN Profile Configuration Mode

Essentially, an APN profile is a template that consists of a set of APN-specific commands that may be applicable to one or more APNs. When a subscriber requests an APN that has been identified in a selected operator policy, the set of commands in the associated APN profile will be applied. The same APN profile can be associated with multiple APNs and multiple operator policies.

The SGSN and the MME each support a total of 1,000 APN profile configurations per SGSN/MME; up to 50 APN profiles can be associated with a single operator policy. For additional SGSN limit information, refer to Engineering Rules in the SGSN Administration Guide.

The APN Profile configuration mode defines a set of parameters controlling the SGSN or MME behavior when a specific APN is received or no APN is received in a Request. An APN profile is a key element in the Operator Policy feature and an APN profile is not used or valid unless it is associated with an APN and this association is specified in an operator policy (see the Operator Policy Configuration Mode Commands).

Command Modes

Exec > Global Configuration > APN Profile Configuration

configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:

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

Important

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

- accounting context, page 4
- accounting mode, page 5
- active-charging rulebase, page 6
- address-resolution-mode, page 8
- apn-resolve-dns-query, page 10
- apn-restoration, page 11
- apn-type, page 13
• associate accounting-policy, page 15
• associate qci-qos-mapping, page 16
• associate quality-of-service-profile, page 17
• associate sgw-paging-profile, page 19
• cc, page 20
• dedicated-bearers, page 22
• description, page 24
• dhcp lease, page 25
• direct-tunnel, page 27
• dns, page 28
• dns-extn, page 30
• end, page 33
• exit, page 34
• gateway-address, page 35
• gateway-selection, page 37
• gn-gtp-version, page 39
• gtp, page 41
• idle-mode-acl, page 43
• ip, page 45
• ip access-group, page 48
• ip address pool, page 49
• ip context-name, page 50
• isr-sequential-paging, page 51
• ipv6, page 52
• local-offload, page 54
• location-reporting, page 55
• mobility-protocol, page 56
• ntsr, page 57
• overcharge-protection, page 59
• pdp-data-inactivity, page 61
• pdp-type-ipv4v6-override, page 63
• pgw-address, page 64
• qos allow-upgrade, page 66
• qos apn-ambr, page 68
• qos class, page 69
• qos dedicated-bearer, page 76
• qos default-bearer, page 77
• qos pgw-upgrade, page 79
• qos prefer-as-cap, page 81
• qos rate-limit direction, page 83
• ranap allocation-retention-priority-ie, page 88
• restrict access-type, page 91
• sm t3396, page 93
• timeout bearer-inactivity, page 95
• timeout idle, page 97
• twan, page 99
• virtual-mac, page 100
accounting context

This command allows you to define the name of the accounting context and associate a GTPP group with this APN profile.

Product
SaMOG

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > APN Profile Configuration
configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:

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

Syntax Description
accounting context context_name gtpp group group_name
remove accounting context

remove
Removes the accounting configuration from this profile's configuration.

context_name
Specifies the accounting context. context_name must be an alphanumeric string of 1 through 79 characters.

gtpp group group_name
Identifies the GTPP group, where the GTPP related parameters have been configured in the GTPP Group Configuration mode, to associate with this SaMOG APN profile.

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

Usage Guidelines
Use this command to associate a predefined GTPP server group, including all its associated configuration, with a specific SaMOG APN profile. Even if an accounting context is also specified in a call control profile, the priority is given to the accounting context of the APN profile.

Examples
The following command identifies an accounting context called account1 and associates a GTPP server group named roaming with defined charging gateway accounting functionality:

accounting context account1 gtp group roaming
accounting mode

This command allows you to define the mode of accounting to be performed for this SaMOG APN profile.

**Product**
SaMOG

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > APN Profile Configuration
  configure > apn-profile *profile_name*
Entering the above command sequence results in the following prompt:
  [local] *host_name*(apn-profile-*profile_name*)#

**Syntax Description**
accounting mode { gtpp | none }
  { default | remove } accounting mode

  default
  Resets the accounting mode to GTPP.

  remove
  Removes the accounting mode from this profile's configuration.

  gtpp
  Specifies that GTPP accounting is performed. This is the default method.

  none
  Specifies that no accounting will be performed for the APN profile.

**Usage Guidelines**
Use this command to specify the accounting mode for an SaMOG APN profile to generate bearer-based SaMOG CDRs. Even if an accounting mode is also specified in a call control profile, the priority is given to the accounting mode of the APN profile.

**Examples**
The following command specifies that no accounting will be used for the APN profile:
accounting mode none
active-charging rulebase

Configure the name of the rulebase that contains the charging action for the HTTP redirection and the URL for the portal for SaMOG web authorization, and/or the rulebase that contains the NAT policy for the SaMOG Local Breakout feature.

Product
SaMOG

Privilege
Administrator

Command Modes
Exec > Global Configuration > APN Profile Configuration
_configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:
[local]host_name(apn-profile-profile_name)#

Syntax Description
active-charging rulebase rulebase_name
no active-charging rulebase

rulebase rulebase_name
Specifies the active charging rulebase to be used.

rulebase_name must be the name of an ACS rulebase, and must be an alphanumeric string of 1 through 63 characters, and can contain punctuation characters.

Usage Guidelines
Use this command to configure the name of the rulebase that contains the charging action for the HTTP redirection and the URL for the authentication portal to facilitate HTTP redirection to the authorization portal during the pre-authentication phase, and/or the rulebase that contains the NAT policy for the SaMOG Local Breakout feature. The ACS rulebase specified in this configuration will be used only if the AAA server does not specify the ACS rulebase during the pre-authentication phase.

Important
This command is license dependent. Contact your Cisco account representative for more information on SaMOG feature license requirements.
Examples

The following command configures the rulebase `webauthredir`:

```
active-charging rulebase webauthredir
```
address-resolution-mode

Identifies the address resolution mode for this APN profile.

**Important**
From release 16.2 onwards, the S4-SGSN also supports this command.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > APN Profile Configuration
configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:

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

**Syntax Description**
```
address-resolution-mode { fallback-for-dns | local }
default address-resolution-mode
```

**default**
Resets the configuration to the default value, that is, **fallback-for-dns**.

**fallback-for-dns**
Instructs the system to try DNS resolution. If the DNS query fails, the SGSN will use locally configured addresses, if they have been configured. The pgw-address configured under apn-profile will be treated as fallback for dns address and will used only after dns failure.

Default: enabled

**Important**
This address will be used on DNS SNAPTR Failure except on Service parameter mismatch.

If pgw-address-resolution-mode fallback-for-dns is not configured then the gateway-address will be treated as fallback for DNS address and UE will fallback to Gn-SGSN, if GPRS-Subscription is available.

**local**
Instructs the system to only use locally configured addresses and not to use DNS query.
Default: disabled

**Usage Guidelines**

Use this command to specify the DNS query or local address resolution for this APN profile.

**Examples**

The following command sets the address resolution mode to use local addresses *only if* the DNS query fails: `address-resolution-mode fallback-for-dns`
**apn-resolve-dns-query**

Command enables the SGSN to send Straightforward Name Authority Pointer (SNAPTR) type DNS query for APN resolution on a per APN basis.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > APN Profile Configuration
- **configure > apn-profile profile_name**
  Entering the above command sequence results in the following prompt:
  
  ```
  [local] host_name (apn-profile-profile_name) #
  ```

**Syntax Description**
- **apn-resolve-dns-query snaptr [ epc-ue | non-epc-ue ]**
- **remove apn-resolve-dns-query snaptr**

  **remove**
  Removes the DNS SNAPTR function from the configuration.

  **epc-ue**
  Configures the S-NAPTR queries to be applicable for EPC-capable UE.

  **non-epc-ue**
  Configures the S-NAPTR queries to be applicable for non-EPC-capable UE.

**Usage Guidelines**
SNAPTR filters based on the EPC-capability of the user equipment (UE). Use this command to enable SNAPTR type DNS query for APN resolution for 3G subscribers with EPC subscription. Configuration in this mode promotes control of this feature per APN.

If neither of the keywords is included with the configuration, then S-NAPTR query is applicable to all UE, both EPC-capable UE and non-EPC capable UE.

By default, this functionality is not enabled.

**Examples**
Enable the SGSN to select a PGW during APN resolution:
- **apn-resolve-dns-query snaptr**
apn-restoration

Configures the APN restoration priority value.

**Product**

MME  
SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > APN Profile Configuration  
configure > apn-profile *profile_name*

Entering the above command sequence results in the following prompt:

[local] *host_name*{apn-profile-*profile_name*}#  

**Syntax Description**

apn-restoration priority *priority_value*

remove apn-restoration priority

*remove*

Removes the APN restoration priority value from the configuration.

*priority priority_value*

Configures the APN restoration priority value. The reactivation of PDNs after a P-GW restart notification is processed in the order of this priority.

*priority_value*

The priority value is an integer value from 1 through 16. Where "1" is the highest priority and "16" is the lowest priority. Default: 16 (lowest priority).

**Usage Guidelines**

The PGW Restart Notification (PRN) message is sent by the S-GW when it detects a peer P-GW has restarted. After the affected subscribers have been deactivated, the MME/S4-SGSN will prioritize the re-activation of impacted PDN connections based on subscribed APN restoration priority, if received from the HSS. If an APN restoration priority is not received from the HSS, then this locally configured value is used. If there is no local configuration then by default such PDNs will be assigned the lowest restoration priority.

The MME will only restore PDNs for which the APN restoration priority is configured and/or received from HSS. Otherwise PDNs will be released by regular deactivation.
For the MME, refer to the LTE Policy > LTE Emergency Profile > `apn` command to define a different APN restoration priority for emergency sessions for this APN profile.

**Examples**

The following command is used to configure the APN restoration priority value of "10" for an APN profile:

`apn-restoration priority 10`
**apn-type**

Identifies the type of APN as an IMS APN.

**Product**
- ePDG
- SGSN
- MME

**Privilege**
- Security Administrator, Administrator

**Command Modes**
- Exec > Global Configuration > APN Profile Configuration
- `configure > apn-profile profile_name`

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
apn-type { emergency | ims } [ pcscf-restoration { pco-update | pdn-deactivate } ]
remove apn-type ims
```

**remove**

Erases this identification configuration from the APN profile and resets the APN profile to the default behavior which disables the APN type as IMS.

**emergency**

Identifies the APN as EMERGENCY APN.

**ims**

Identifies the APN as IMS APN. If an IMS APN is present, Modify Bearer Req/Update PDP Req will be delayed during Inbound SRNS relocation for SGSN.

**pcscf-restoration { pco-update | pdn-deactivate }**

**pcscf-restoration**: The `pcscf-restoration` keyword in this command identifies P-CSCF restoration for IMS PDN. This keyword is functional only if the feature license is installed.

**pco-update**: The `pco-update` keyword selects P-CSCF restoration method as PDN Modification through PCO update.
**pdn-deactivate**: The pdn-deactivate keyword selects P-CSCF restoration method as PDN Deactivation. This is the default method.

**Important** If only "apn-type ims" is configured, then the default P-CSCF restoration method **pdn-deactivate** is enabled.

**Usage Guidelines** This command identifies the APN as an IMS APN. This enables the SGSN to delay sending Modify Bearer Request to the S-GW until after receiving the Forward Relocation Complete Ack from the peer during SRNS procedure.

Also, The following CLI identifies an APN as IMS APN and to configure to indicate whether the PGW supports optional extension or if the MME initiates PDN deactivation for HSS initiated P-CSCF restoration. To enable HSS-based P-CSCF Restoration, use the pcsf-restoration command under the Call Control Profile mode.

**Examples** Identify the APN for this profile as an IMS type APN:

```
apn-type ims
```

The following command selects pco-update as the P-CSCF Restoration method:

```
apn-type ims pcsf-restoration pco-update
```

The following command selects pdn-deactivate as the P-CSCF Restoration method:

```
apn-type ims pcsf-restoration pdn-deactivate
```
associate accounting-policy

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

**Product**
SaMOG

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > APN Profile Configuration

`configure > apn-profile profile_name`

Entering the above command sequence results in the following prompt:

```
[local] host_name/apn-profile-profile_name]#
```

**Syntax Description**

- `associate accounting-policy policy_name`
- `remove associate accounting-policy`  
- `policy_name`

  Specified the policy name to associate to the APN profile. `policy_name` must be an existing accounting policy, and must be an alphanumeric string of 1 through 63 characters.

**Usage Guidelines**

Use this command to associate the SaMOG APN profile with an accounting policy configured in this context to provide triggers to generate CDRs. The accounting policy configured under the APN profile takes priority over the accounting policy configured under the call control profile.

**Examples**

The following command associates this SaMOG APN with an accounting policy called `acct1`:

`associate accounting-policy acct1`
associate qci-qos-mapping

Provides operators with a configuration to associate a QoS Class Identifier (QCI) Quality of Service (QoS) mapping table with a specified APN profile configuration.

**Product**
- SGW
- SAE-GW

**Privilege**
- Security Administrator, Administrator

**Command Modes**
- Exec > Global Configuration > APN Profile Configuration
- configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:

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

**Syntax Description**
- `| remove | associate qci-qos-mapping mapping_table_name`

- `remove`

Removes the specified QCI to QoS mapping table association.

- `associate qci-qos-mapping mapping_table_name`

Instructs the application to associate the specified QCI QoS mapping to this APN profile.

**Usage Guidelines**
Associates a QCI QoS mapping table with an APN profile.

**Examples**
This example associates a QCI QoS mapping table with the APN Profile 'QCIQOSMap'.

```
associate qci-qos-mapping QCIQOSMap
```
**associate quality-of-service-profile**

Associates the specified Quality of Service profile with the APN profile.

**Product**
- MME
- SGSN

**Privilege**
- Administrator

**Command Modes**
- `Exec > Global Configuration > APN Profile Configuration`
- `configure > apn-profile profile_name`

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

- `associate quality-of-service-profile qos_profile_name access-type [ eps | gprs | umts ]`
- `remove associate quality-of-service-profile access-type [ eps | gprs | umts ]`

**remove**

Removes the association of the specified Quality of Service profile with the APN profile.

**access-type**

Configures the access-types to be associated with the QoS profile for this APN profile.

- **eps** identifies a 4G EPS network. (MME only)
- **gprs** identifies a 2G GPRS network.
- **umts** identifies a 3G UMTS network.

**qos_profile_name**

Identifies the name of the Quality of Service profile to be associated with the APN profile.

**Usage Guidelines**

This command identifies a specific Quality of Service profile to be associated with the APN profile.

**Examples**

Use this command to associate a 3G (UMTS) QoS profile named *test* with the APN profile.

```
associate quality-of-service-profile test access-type umts
```
Use this command to associate a 4G QoS profile named MMEqos1 with the APN profile.

```
associate quality-of-service-profile MMEqos1 access-type eps
```
associate sgw-paging-profile

This command allows the association of an SGW Paging Profile with an APN profile on the S-GW.

Product
S-GW

Privilege
Administrator, Security Administrator

Command Modes
Exec > Global Configuration > APN Profile Configuration

configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:

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

Syntax Description

| remove | associate sgw-paging-profile three-tupple |

remove
Removes the S-GW Paging Profile from the APN Profile.

associate sgw-paging-profile three-tupple
Associates an SGW Paging Profile with an APN profile on the S-GW. S-GW Paging Profiles are configured in Global Configuration Mode with the sgw-paging-profile three-tupple command.

Usage Guidelines
Use this command to associate an S-GW paging profile with an APN profile on the S-GW.

Examples
This example associates an S-GW paging profile with an APN profile on the S-GW.
associate sgw-paging-profile three-tupple
CC

Configures the charging characteristics (CC) for this APN profile.

Product
SGSN
S-GW
SAEGW

Privilege
Security Administrator, Administrator

Command Modes
Exec > Global Configuration > APN Profile Configuration
configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:
[local] host_name (apn-profile-profile_name) #

Syntax Description
cc { local-value-for-scdrs behavior bit_value profile index_bit | prefer { hlr-value-for-scdrs \ local-value-for-scdrs } } remove cc { local-value-for-scdrs | prefer }

remove
Removes the charging characteristics configuration from this APN profile.

local-value-for-scdrs behavior bit_value profile index_bit
Sets the value of the behavior bits and profile index for the charging characteristics for S-CDRs locally, when the Home Location Register (HLR) does not provide these values.
If the HLR provides the charging characteristics with behavior bits and profile index, and the operator wants to ignore what the HLR provides, then specify the prefer local-value-for-scdrs keyword with this command.
bit_value: must be a hexadecimal value between 0x0 and 0xFFF.
index_bit: must be an integer from 1 through 15.
Some of the index values are predefined according to 3GPP standard:

- 1 for hot billing
- 2 for flat billing
- 4 for prepaid billing
- 8 for normal billing
Defaults: $bit_value = 0x0; index_bit = 8$

`prefer { hlr-value-for-scdrs | local-value-for-scdrs }`

Specify what charging characteristic settings the system will use for S-CDRs.

- **hlr-value-for-scdrs**: instructs the system to use charging characteristic settings received from the HLR for S-CDRs.
- **local-value-for-scdrs**: instructs the profile preference to only use locally configured/stored charging characteristic settings for S-CDRs.

Default: **hlr-value-for-scdrs**

**Usage Guidelines**

Use this command to specify the charging characteristic for S-CDRs -- either from the HLR or locally from the SGSN.

These charging characteristics parameters for S-CDRs and M-CDRs are also configurable in the Call-Control Profile configuration mode. When CC parameters are specified in both types of profiles, then:

- For generation of M-CDRs, the parameters configured in the Call-Control Profile configuration mode will take precedence.
- For generation of S-CDRs, the parameters configured in the APN Profile configuration mode will take precedence.

**Examples**

The following command configures the APN profile to instruct the SGSN not to use charging characteristic settings received from the HLR for S-CDR generation:

`cc prefer hlr-value-for-scdrs`
**dedicated-bearers**

Configures the MME to either accept or reject dedicated GBR and Non-GBR bearers.

**Product**

MME

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > APN Profile Configuration

```plaintext
configure > apn-profile profile_name
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```plaintext
dedicated-bearers { gbr { accept | reject } | non-gbr { accept | reject } } | remove | dedicated-bearers { gbr | non-gbr }
```

**remove**

Removes the configuration, returning the system to the default setting where the MME accepts GBR or Non-GBR dedicated bearers.

```plaintext
gbr { accept | reject }
```

Configures the MME to accept or reject dedicated GBR bearers.

```plaintext
non-gbr { accept | reject }
```

Configures the MME to accept or reject dedicated Non-GBR bearers.

**Usage Guidelines**

The MME differentiates GBR and Non-GBR dedicated bearers as follows: GBR Bearers - QCI value ranges from 1 to 4; Non-GBR bearers - QCI value ranges from 5-9.

In the case of a UE-initiated Bearer Resource Allocation Reject, the ESM cause "EPS QOS not accepted" is used and the corresponding bearer allocation reject MME statistic is incremented.

In the case of a Create Bearer Request Reject, the EGTP cause "Service denied" is used and the corresponding EGTP statistic is incremented.

**Note:** Handling of multiple bearers in a Create Bearer request from S-GW for Partial accept/reject of GBR/Non-GBR dedicated bearers is a current limitation.
The following commands configure the MME to reject both GBR and Non-GBR dedicated bearers:

```
dedicated-bearers gbr reject
dedicated-bearers non-gbr reject
```


## description

Defines a descriptive string relevant to the specific APN profile.

### Product

- MME
- SGSN
- S-GW
- SAEGW

### Privilege

Security Administrator, Administrator

### Command Modes

- Exec > Global Configuration > APN Profile Configuration
- configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:

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

### Syntax Description

- `description description`
- `remove description`

`remove`

Removes the configured description from this APN profile.

### Usage Guidelines

Define information that identifies this particular APN profile.

### Examples

Indicate that APN profile `apnprof1` is to be used for customers in Saudi Arabia and that the profile was created on April 10th of 2010:

```
description "apnprof1 defines APNs for customers in Saudi Arabia (4/10/10)."
```
dhcp lease

Configures a lease period for the UE’s IP address during SaMOG Web Authorization pre-authentication and TAL phases.

**Important** This command requires the SaMOG Web Authorization feature license. For more information, contact your Cisco account representative.

**Product** SaMOG

**Privilege** Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > APN Profile Configuration

configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

dhcp lease { short duration | time duration }
default dhcp lease { short | time }
remove dhcp lease short

default
Restores the DHCP lease configuration for short lease time (pre-authentication phase) and DHCP lease time (TAL phase) to its default value.

remove
If previously configured, removes the DHCP short lease time configuration from this APN profile.

short duration
Specifies the DHCP short lease time for web authorization sessions to force the UE to initiate DHCP request after the pre-authentication phase completes.

duration must be an integer from 2 through 600.
Default: 20 seconds
**time duration**

Specifies the lease time for the UE's IP address during the web authorization TAL phase.

*duration* must be an integer from 600 through 4294967295.

Default: 4294967295 seconds

**Usage Guidelines**

Use this command to configure a lease period for the UE's IP address during SaMOG Web Authorization pre-authentication and TAL phases.

**Examples**

The following command configures a DHCP short lease period of 60 seconds and lease period of 3600 seconds:

```
dhcp lease short 60 time 3600
```
**direct-tunnel**

Defines the permission for direct tunnel establishment by GGSNs. This command is specific to the SGSN.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > APN Profile Configuration

```
configure > apn-profile profile_name
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**
direct-tunnel not-permitted-by-ggsn
remove direct-tunnel

remove
Removes the direct tunnel establishment configuration from this APN profile.

not-permitted-by-ggsn
Specifies that a direct tunnel is not permitted by the GGSN when resolved by this APN.
Default: disabled.

**Usage Guidelines**
Use this command to enable/disable the permission for establishment of direct tunnels between an RNC and a GGSN.

**Examples**
The following command instructs the SGSN not to permit establishment of a direct tunnel with a GGSN:

```
direct-tunnel not-permitted-by-ggsn
```
Configure the primary and secondary IPv4 or IPv6 address of the DNS servers.

**Product**
SaMOG

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > APN Profile Configuration

configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

- `dns [ipv6] {primary | secondary} ip_address`
- `no [ipv6] {primary | secondary}`

- `no`
If previously configured, removes the DNS primary or secondary IP address to be used for web authorization.

- `ipv6`
Specify IPv6 DNS server(s) to enable Flow-based Local Breakout GTPv2 sessions.

- `primary | secondary IP_address`
Specify the primary or secondary DNS server address using the `primary | secondary` keywords.

- `ip_address` must be expressed in IPv4 dotted-decimal or IPv6 colon-separated (when the `ipv6` keyword is configured) notation format.

**Usage Guidelines**

Use this command to configure the IPv4 or IPv6 address of the primary and secondary DNS servers to be used during session setup. The primary and secondary DNS servers specified in this configuration will be used only if the AAA server does not specify the same.

**Important**
This command is license dependent. Contact your Cisco account representative for more information on SaMOG feature license requirements.
The following command configures a primary DNS server with the IP address 162.123.23.1:
```
dns primary 162.123.23.1
```
Takes an offset group of digits from the MSISDN and appends the digits to the DNS query string to create a new APN intended to assist roaming subscribers to use the local GGSN.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > APN Profile Configuration

```
configure > apn-profile profile_name
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
dns-extn { charg-id { binary | decimal | hexadecimal } | lac-rac | msisdn start-offset start_digits end-offset end-digits | rnc-id [ charg-id { binary | decimal | hexadecimal } ] }
remove dns-extn { charg-id | lac-rac | msisdn | rnc-id | charg-id } 
```

**charg-id { binary | decimal | hexadecimal }**
Instructs the SGSN to take the profile index value of the charging characteristics, from the PDP subscription record (selected during APN selection) and include the profile index value in the APN name prior to sending out DNS queries. The operator can also specify the format (binary, decimal or hexadecimal) for the CC information to be included.

**lac-rac**
Enables the SGSN to append geographical information to the APN string that is being sent in the DNS query. This information is used during the DNS query process to select the geographically closest GGSN.

**msisdn start-offset start_digits end-offset end-digits**
Defines an offset group of digits from the MSISDN and appends the digits to create a new APN DNS query string that is intended to assist roaming subscribers to use the local GGSN.

- **start_digits** is an integer from 1 through 14 that identifies the position of the first digit in the MSISDN to start the offset.
- **end-digits** is an integer from 2 through 15 that identifies the position of the last digit in the MSISDN to be part of the offset.
rnc-id \ charg-id \{ binary | decimal | hexadecimal \} \}
Instructs the SGSN to include the ID of the calling RNC in the APN DNS query string. Optionally, the profile index value of the charging characteristics can be inserted into the APN name prior to sending out DNS queries. As well, the operator can specify the format (binary, decimal or hexadecimal) for the CC information to be included.

Usage Guidelines
With this command, the APN in the DNS query string, used for querying the GGSN address, can be appended with additional information, such as

- digits from the MSISDN
- LAC/RAC info
- RNC-ID
- profile index from the charging characteristics information (SCHAR)

This additional information allows some customization of the DNS query string to facilitate selecting a specific (usually local or nearest) GGSN.

For example, roaming subscribers using a specific APN may want to be directed to a specific GGSN. This can be achieved by having an operator policy for roaming subscribers associated with an APN profile that includes a configuration specifying certain digits, from the MSISDN or geographical information from the LAC/RAC, be appended to the APN. This is then used as the DNS query string.

In addition, the operator must configure appropriate DNS entries to enforce the selection of the required GGSN. After appending the MSISDN digits to the DNS query string, the string will have the form:

ni.<digits>.*mcc*.gprs

After appending the LAC/RAC information to the DNS query string, the string will have the form:

<apn_network_id>\.racAAAA.lacBBBB.<apn_operator_id>

where the AAAA and BBBB are Hex-coded digits (less than 4 significant digits and one or more zero ("0") digits will be inserted to the left side of the Hex to fill the 4-digit coding).

After appending the charging characteristic (SCHAR) information, the DNS string will take the following form:

<apn_network_id>.<profile_index>.<apn_operator_id>

The profile index in the following example has an integer value 10:

quicknet.com.uk.1010.mnc234.mcc027.gprs

If the RNC-ID information is configured to be a part of the APN name, and if inclusion of the profile index of the charging characteristics information is also enabled before the DNS query is sent, the profile index is included after the included RNC-ID and the DNS APN name will appear in the following form:

<apn_network_id>.<rnc_id>.<profile_index>.<apn_operator_id>

Once the DNS extension is defined, the selected extension is applicable when either the wildcard APN feature or the default APN feature are configured and used.

The information is appended to the DNS query and the actual APN string sent to the GGSN will not be modified in any way.
Examples

A sample MSISDN is '112233445566778' and a sample APN NI (network identifier) is 'wap98.testnetz.ca'. The following command instructs the SGSN to create a new APN with digits pulled from the MSISDN and appended to the APN:

```
msisdn start-offset 3 end-offset 9
```

The resulting APN DNS query string would have appended 7 digits (2233445) to the APN NI so that it would appear something like wap98.testnetz.ca.2233445.MNC009.MCC262.GPRS

Enable inclusion of geographical information in the APN string used for the DNS query to locate the closest GGSN:

```
lac-rac
```

In the following example, the DNS query for a subscriber using RNC 0321 with the profile index of value 8 would appear as:

```
quicknet.com.uk.0321.1000.mnc234.mcc027.gprs
```
**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.
**gateway-address**

Configures the IPv4 or IPv6 address of the GGSN supporting the APN associated with this APN profile. Also, use this command to create a secondary pool of GGSNs. This command is specific to the SGSN.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > APN Profile Configuration

configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name{apn-profile-profile_name}#

**Syntax Description**

```
gateway-address ip_address { priority priority | weight weight | secondary-pool } 
no gateway-address ip_address
```

**no**

Disables the GGSN address configured in this APN profile.

**ip_address**

Specifies the IP address for the GGSN in IPv4 dotted-decimal or IPv6 colon-separated notation.

**priority priority**

Specifies the priority, for the configured GGSN address, to be considered during address selection. If the highest priority GGSN fails to respond, the next priority level GGSN is selected. priority is an integer from 1 through 100. Note that the lower integer has the higher priority, so that 1 is the highest priority.

**weight weight | secondary-pool |**

Specifies the weight (preference) assigned to a GGSN to facilitate load balancing. weight is an integer from 1 to 100 where 1 is the least preferred and 100 is the most preferred.

If a weight is assigned to an address, then load balancing (of primary CPC requests) depends on the weight value. For example:

```
GGSN1 172.16.130.1 weight 30 and GGSN2 172.16.130.3 weight 70
```

With this configuration, 30% of the activation requests for this APN will go to GGSN1 and 70% of the requests will go to GGSN2. Also note that the sum of the weights does not need to be 100. The calculation of weight...
percentiles is carried out proportionately, so the following configuration will also yield the same 30% - 70%
results:
GGSN1 172.16.130.1 weight 6 and GGSN2 172.16.130.3 weight 14

**secondary-pool**

This optional keyword allows the operator to enable multiple GGSN pools by assigning the GGSN to a
secondary pool of GGSNs. The selection algorithm for GGSNs in a secondary pool is weight-based.

**Usage Guidelines**

Use this command to define priority or load balancing to be applied during GGSN selection. A maximum of
16 GGSN address can be configured for this APN profile.

Also use this command to setup GGSN pools - primary and secondary pools with up to 16 GGSNs in each
pool. By default, GGSNs will always be selected from the primary pool. However, working in tandem with
the `ggsn-fail-retry-timer` command configuration (SGTP service configuration mode) which enables the
local DNS feature, some of the primary GGSNs can be temporarily blacklisted if they become unavailable or
overburdened.

**Examples**

Set a GGSN address with a secondary priority level:

```
gateway-address 123.123.123.2 priority 2
```

Add a GGSN to the secondary GGSN pool and define selection weighting of 7th:

```
gateway-address 198.168.138.8 weight 7 secondary-pool
```
gateway-selection

Configures gateway selection related parameters for ePDG and SaMOG.

**Product**
ePDG
SaMOG

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > APN Profile Configuration
configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:
[local] host_name{apn-profile-profile_name}#

**Syntax Description**
For ePDG,

gateway-selection alternate-epdg strip-labels strip_labels max-alternate-pgw max_alternate_pgw_attempts

remove gateway-selection alternate-epdg strip-labels strip_labels max-alternate-pgw

For SaMOG,

gateway-selection max-alternate-pgw max_alternate_pgw_attempts
remove gateway-selection max-alternate-pgw

remove

If previously configured, disables the maximum number of P-GW address resolution for this APN profile.

**alternate-epdg**

**Important**
This keyword is license dependent. Contact your Cisco account representative for more information on ePDG feature license requirements.

(ePDG) Enables alternate ePDG selection.
strip-labels strip_labels

Important This keyword is license dependent. Contact your Cisco account representative for more information on ePDG feature license requirements.

(ePDG) Number of labels to be stripped off for domain matching.
strip_labels must be an integer between 0 to 10 separated by periods. Default value is 3.

max-alternate-pgw max_alternate_pgw_attempts
(ePDG/SaMOG) Configures maximum number of alternate P-GW attempts.
max_alternate_pgw_attempts must be an integer between 0 to 64.

Usage Guidelines
Use this command to configure the gateway selection related parameters.
For ePDG, use this command to configure the maximum number of labels to be stripped off for domain matching, and the maximum number of alternate P-GW attempts.
For SaMOG, use this command to configure the maximum number of alternate P-GW attempts during P-GW selection fall-back.

Examples
The following example to set the maximum alternate P-GW selection attempts to 8:
gateway-selection max-alternate-pgw 8
gn-gtp-version

This command enables the operator to prevent the SGSN from attempting GTPv0 Requests for GGSNs associated with specified APNs so that the SGSN tries activation with the next available GGSN if the current GGSN does not respond after the GTPv1 Request retries fail.

Product

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > APN Profile Configuration

cfgure > apn-profile profile_name

Entering the above command sequence results in the following prompt:

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

Syntax Description

| remove | gn-gtp-version v1-only

remove

Used with the command, this filter erases the previous GTPv1 configuration and returns the SGSN configuration to the default value of both GTPv1 and GTPv0.

v1-only

This extension must be included to complete the command. This extension disables GTPv0 fallback.

Usage Guidelines

During activation, the SGSN sends GTPv1 PDP Requests a GGSN and if no response is available from the GGSN after the maximum number of retransmissions and timeout, then before trying an alternate GGSN, the SGSN attempts to create GTPv0 PDP Requests and retries are carried out. Only after GTPv0 retransmissions and timeout would the SGSN try activation with the next available GGSN.

The SGSN supported GTPv0 fallback. After exhausting all configured retry attempts for GTPv1, the SGSN would retry the GTP-C Request using GTPv0. This fallback is conditional and is done only when the GTP version of a GGSN is unknown during the first attempt at activating a PDP context with the GGSN.

This command allows the operator to disable the GTPv0 fallback for GTP-C Requests to GGSNs corresponding to a specific APN, thus reducing unnecessary signalling if all known GGSN support GTPv1 only. Hence, if more than one GGSN address is returned by the DNS server during activation, then the SGSN more immediately attempts activation with the next GGSN after exhausting all the GTPv1 retry attempts. If only one GGSN address is returned, then the SGSN rejects the activation after exhausting all the configured GTPv1 retries.
Examples

The following command disables GTPv0 fallback:

`gn-gtp-version v1-only`

The following command deletes the previous configuration and re-enables the default so the SGSN will attempt activation via both GTPv1 and if needed GTPv0:

`remove gn-gtp-version v1-only`
**gtp**

Enables or disables the GTPC private extension for the Overcharging Protection feature. This command is specific to the SGSN.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > APN Profile Configuration

`configure > apn-profile profile_name`

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
[ remove ] gtp private-extension loss-of-radio-coverage send-to-ggsn | send-to-peer-sgsn |
```

- **remove**
  
  Disables the inclusion of the GTPC private extension, thereby disabling the Overcharging Protection feature.

- **private-extension loss-of-radio-coverage send-to-ggsn**
  
  Instructs the SGSN to set a proprietary GTPC private extension (in the LORC Intimation IEs) in the event of loss of radio coverage (LORC). These private extensions are only understood by a GGSN with an Overcharging Protection license.

  The mandatory **loss-of-radio-coverage send-to-ggsn** keyword set instructs the SGSN to forward the private extension flag to the GGSN in the event of a loss of radio coverage (LORC).

- **send-to-peer-sgsn**
  
  This optional keyword instructs the SGSN to also forward the LORC private extension to the peer SGSN.

**Usage Guidelines**

**gtp private-extension** is one of the two commands required to enable the Overcharging Protection feature.

The second command sets the RANAP cause code in the Iu Release to enable the SGSN to detect the LORC state of the MS/UE. This second command is configured in the IuPS service and is explained in the *IuPS Service Configuration Mode* chapter.

When there is a loss of coverage and the Overcharging Protection feature is enabled with the **gtp private-extension** command, the SGSN includes the proprietary private extension in the GTP LORC Intimation IE messages. This LORC IE is also included in UPCQ, DPCQ, and SGSN Context Response GTP messages.
Refer to the *SGSN Administration Guide* for additional information regarding the Overcharging Protection feature.

**Examples**

Use the following command to have the SGSN send the GGSN the GTPC private extension in the LORC Intimation IE:

```
gtp private-extension loss-of-radio-coverage send-to-ggsn
```
idle-mode-acl

Configures a group of access control lists (ACLs) that define rules to apply to downlink data destined for UEs in an idle mode.

Product
S-GW
SAEGW

Privilege
Administrator

Command Modes
Exec > Global Configuration > APN Profile Configuration
configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:

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

Syntax Description

| remove | idle-mode-acl { ipv4 | ipv6 } access-group acl_name |

remove
Removes the specified ACL name from the access group.

{ ipv4 | ipv6 } access-group acl_name
Specifies the ACL type to add to the access group.

- ipv4: Specifies that an IPv4 ACL is being added to the access group.
- ipv6: Specifies that an IPv6 ACL is being added to the access group.

access-group acl_name specifies the name of the ACL being added to the access group as an existing IPv4 or IPv6 ACL name expressed as an alphanumeric string of 1 through 47 characters.

Usage Guidelines

Use this command to create a group of ACLs that contain rules to apply to data sent to UEs that are currently in idle mode.
IPv4 ACLs are configured through the Context Configuration Mode using the ip access-list command.
IPv6 ACLs are configured through the Context Configuration Mode using the ipv6 access-list command.
Examples

The following command configures the APN profile to use an IPv4 ACL named *acl-3-permit* to apply rules to downlink data sent to UEs that are currently in idle mode:

```
idle-mode-acl ipv4 access-group acl-3-permit
```
ip

Defines the IP parameters for this APN profile.

**Product**
SGSN
S-GW
SAEGW

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > APN Profile Configuration

`configure > apn-profile profile_name`

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

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

---

**Important**

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

---

**default**

Resets the configuration to the default values.

**no**

Disables the specified IP QoS-DSCP mapping.

**qos-dscp**

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

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

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

**DSCP marking options**

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

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

Forwarding defaults for both uplink and downlink are:

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

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

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

- **discard** - discard errant packets, can include the following option:
  - **exclude-from-accounting** - excludes packets having an invalid source IP address from the statistics used in the accounting records.

- **ignore** - ignore checking of packets for MS/UE IP source violation.

**Usage Guidelines**

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

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

**Examples**

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

```
ip source-violation ignore
```
**ip access-group**

Configure the name of the access control list (ACL) for incoming and outgoing packets.

**Product**  
SaMOG

**Privilege**  
Administrator

**Command Modes**  
Exec > Global Configuration > APN Profile Configuration  
configure > apn-profile profile_name  
Entering the above command sequence results in the following prompt:  
[local]host_name (apn-profile-profile_name)#

**Syntax Description**  
| no | ip access-group group_name [ in | out ] |

- **no**  
  If previously configured, removes the IP access group.

- **group_name**  
  *group_name* must be an alphanumeric string of 1 to 47 characters.

- **in | out**  
  Specify the access group as inbound or outbound.

**Usage Guidelines**  
Use this command to configure the ACL name for incoming and outgoing packets to redirect HTTP packets, allow DNS packets and drop other packets. The IP access group specified in this configuration will be used only if the AAA server does not specify the same during authentication.

---

**Important**  
This command is license dependent. Contact your Cisco account representative for more information on SaMOG feature license requirements.

**Examples**  
The following command configures an IP access group called *webauthaccgroup* and sets it as inbound:  
```plaintext
ip access-group webauthaccgroup in
```
**ip address pool**

Configure the name of the IP address pool from which the IP address needs to be allocated to the user equipment (UE).

**Product**
SaMOG

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > APN Profile Configuration
`configure > apn-profile profile_name`

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
no | ip address pool name pool_name
```

- **no**
  If previously configured, removes the IP address pool to be used for web authorization.

- **pool_name**
  `pool_name` must be an alphanumerical string of 1 to 31 characters.

**Usage Guidelines**

Use this command to configure the name of the IP address pool from which the IP address is to be allocated to the UE during the pre-authentication phase. The IP address pool name specified in this configuration will be used only if the AAA server does not specify the same during the pre-authentication phase.

**Important**
This command is license dependent. Contact your Cisco account representative for more information on SaMOG feature license requirements.

**Examples**
The following command configures an IP address pool name of `wapool`:

```
ip address pool name wapool
```
ip context-name

Configure the name of the context where the IP pool configuration needs to be obtained from.

Product
SaMOG

Privilege
Administrator

Command Modes
Exec > Global Configuration > APN Profile Configuration
configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:
[local]host_name (apn-profile-profile_name) #

Syntax Description
ip context-name context_name
no ip context-name

no
If previously configured, removes the IP context name to be used for web authorization.

case context_name
context_name must be an alphanumeric string of 1 to 79 characters.

Usage Guidelines
Use this command to configure the name of the context where the IP pool configuration needs to be obtained from and provide the VPN through which the URL to the portal can be reached during the SaMOG web authorization pre-authentication phase, or the data can be offloaded for Local Breakout. If the IP context name is not configured here, and the AAA server does not provide one, the VPN context of the SaMOG service will be used.

Important
This command is license dependent. Contact your Cisco account representative for more information on SaMOG feature license requirements.

Examples
The following command configures the IP context name of wacxt
ip context-name wacxt
### isr-sequential-paging

Enables or disables the Intelligent Paging for ISR feature.

| **Product** | S-GW  
|             | SAEGW |
| **Privilege** | Administrator |

#### Command Modes

- `Exec > Global Configuration > APN Profile Configuration`
- `configure > apn-profile profile_name`

Entering the above command sequence results in the following prompt:

```
[local] host_name{apn-profile-profile_name}#
```

#### Syntax Description

- `| remove | isr-sequential-paging`

  - `remove`
    - Disables Intelligent Paging for ISR.

#### Usage Guidelines

This command initiates the Intelligent Paging for ISR feature for the specified APN Profile, where paging occurs first towards the last known RAT, then towards the other RAT.

The Intelligent Paging for ISR feature is license dependant. Contact your Cisco account representative for more information.
ipv6

Configures the IPv6 pool name to be used by SaMOG if the 'Framed-IPv6-Pool' AVP is unavailable in the Diameter AA-Answer message, or enable SaMOG to send unsolicited router advertisements (RA) to advertise or deprecate an IPv6 prefix for session with the EoGRE access type.

Product
SaMOG

Privilege
Administrator

Command Modes
Exec > Global Configuration > APN Profile Configuration

configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:

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

Syntax Description

ipv6 { address prefix-pool pool_name | unsolicited-router-advt { advertise | deprecate } { interval duration | num-advts num_advts | num-advts num_advts { interval duration } } default ipv6 unsolicited-router-advt

no ipv6 { address prefix-pool pool_name | unsolicited-router-advt { advertise | deprecate } }

default

Configures this command to its default value.

no

If previously configured, removes the IP pool name or disables sending unsolicited router advertisements (RA) to advertise or deprecate an IPv6 prefix.

address prefix-pool pool_name

Specify the IPv6 pool name to be used by SaMOG if the 'Framed-IPv6-Pool' AVP is unavailable in the Diameter AA-Answer message.

pool_name must be an alphanumeric string from 1 to 31 characters.

unsolicited-router-advt { advertise | deprecate }

Configure to send unsolicited router advertisements (RA) to advertise or deprecate an IPv6 prefix for session with the EoGRE access type.
interval duration
Configure the interval between each unsolicited router advertisement.

duration must be an integer from 100 through 16000.
Default: 3000 milliseconds

num-advts num_advts
Configure the number of times unsolicited router advertisement must be sent.

num_advts must be an integer from 1 through 16.
Default: 3

Usage Guidelines
Use this command to:

- Configure the IPv6 pool name to be used by SaMOG if the 'Framed-IPV6-Pool' AVP is unavailable in the Diameter AA-Answer message. SaMOG uses the configured IPv6 prefix in the Gi context with this IPv6 pool name.
- Enable SaMOG to send unsolicited router advertisements (RA) to advertise or deprecate an IPv6 prefix for session with the EoGRE access type.

Examples
The following command configures an IPv6 pool name v6pool:

ipv6 address prefix-pool v6pool
local-offload

Enables or disables the SaMOG Local Breakout (LBO) Enhanced, LBO Basic, or Flow-based LBO features.

**Product**
SaMOG

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration > APN Profile Configuration

```bash
configure > apn-profile profile_name
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

- `local-offload [ flow ]`
  - `no local-offload`
  
    **no**
    Disables Local Breakout for this APN profile.

  **flow**
  Enables flow-based Local Breakout for this APN profile.

  **Important**
  This keyword is available when the Flow-based Local Breakout license is enabled.

**Usage Guidelines**

Use this command to enable or disable the SaMOG LBO Enhanced, LBO basic, or Flow-based LBO features. When enabled, LBO will be allowed for the UE connecting to the specified SSID, through which this APN profile is reached.

**Important**

The SaMOG LBO features are license dependant. Contact your Cisco account representative for more information.
**location-reporting**

Configure location change reporting via ULI IE per APN for an S4-SGSN.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > APN Profile Configuration

```
configure > apn-profile profile_name
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
location-reporting access-type { gprs | umts }
remove location-reporting access-type { gprs | umts }
```

```
remove
```

Disables the location change reporting definition in the APN profile configuration.

```
access-type { gprs | umts }
```

Allows the operator to select location change reporting for the 2G and / or the 3G subscribers. Both access types can be identified in a single command or the command can be issued twice. Either way, two separate entries are created, one for each access type.

**Usage Guidelines**

As with all APN profiles, to enable location change reporting, this APN profile must be associated with a call control profile.

Location change reporting for a Gn-SGSN is enabled with the `location reporting` command in the Call Control Profile configuration mode. That command can be used to configure the location change reporting function for the S4-SGSN, however that configuration would be over-ridden by an APN profile configuration. As well, using this APN profile `location reporting` command gives the operator greater control to apply location change reporting per APN.

**Examples**

Enable location change reporting for 2G subscribers:

```
location-reporting access-type gprs
```
mobility-protocol

This command allows you to configure the default mobility protocol type to be used for setting up a call when the AAA server forwards an IP address directly.

Product: SaMOG

Privilege: Administrator

Command Modes: Exec > Global Configuration > APN Profile Configuration

configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:

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

Syntax Description:

mobility-protocol { gtpv1 | gtpv2 | pmip }

no mobility-protocol

no

Removes the mobility protocol configuration for this APN profile.

Usage Guidelines:

Use this command to configure the default mobility protocol type to be used for setting up a call when the AAA server forwards an IP address directly. If mobility protocol is also configured under the Call Control Profile Configuration Mode, the value configured here will override the configured value in the Call Control profile.

By default, all APN profiles will use the mobility protocol configured under the Call Control Profile Configuration Mode. To configure different mobility protocol values for different APN profiles, use the mobility-protocol command in this configuration mode.

Examples:

The following command configures mobility protocol to GTPv2:

mobility-protocol GTPv2
ntsrt

This command configures QCI and ARP in the apn-profile for Network Triggered Service Restoration (NTSR).

**Product**

S-GW

**Privilege**

Administrator, Security Administrator

**Command Modes**

Exec > Global Configuration > APN Profile Configuration

`configure > apn-profile profile_name`

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

`ntsrt { all | qci number arp-priority-watermark number }`

`no ntsrt all`

`no ntsrt qci number arp-priority-watermark number`

`no`

Removes the specified configuration parameters.

`ntsrt`

Enables the network triggered service restoration configuration.

`all`

Specifies that the NTSR configuration is enabled for all bearers with any qci or arp for MME restoration.

`qci`

Specifies the Quality of Class Identifier for this NTSR configuration. Must be an integer from 1 to 255.

`arp-priority-watermark`

Specifies the ARP's priority level watermark value. Must be an integer from 1 to 15.

**Usage Guidelines**

This command configures qci and arp in the apn-profile for NTSR. The S-GW will decide to retain or release the bearer based on the configured qci/arp, after path failure is detected on ingress side of S-GW. The S-GW can configure a maximum of 2 qci and arp-priority-watermark per apn-profile. The apn-profile can also be configured to retain all bearers from that PDN.
Examples

This example configures the apn-profile to retain all bearers from the PDN.

ntsr all
**overcharge-protection**

Enables overcharge protection for APNs controlled by this APN profile. Each overcharging protection option is a standalone configuration and it does not override the previous option set, if any.

**Product**
- S-GW
- P-GW

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > APN Profile Configuration
```
configure > apn-profile profile_name
```
Entering the above command sequence results in the following prompt:
```
[local]host_name(apn-profile-profile_name)#
```

**Syntax Description**
```
overcharge-protection { abnormal-s1-release | ddn-failure | drop-limit drop_limit_value { packets | bytes } } 
| remove | overcharge-protection { abnormal-s1-release | ddn-failure | drop-limit }
```

`remove`
Removes the specified configuration.

**abnormal-s1-release**
(for future use) If overcharging protection is enabled for abnormal-s1-release, S-GW would send MBR to pause charging at P-GW if Abnormal Release of Radio Link signal occurs from MME.

**Important**
Though the command is available in this release, this scenario is not possible.

**ddn-failure**
If overcharging protection is enabled for ddn-failure message, MBR would be sent to P-GW to pause charging upon receiving DDN failure from MME/S4-SGSN.

**drop-limit drop_limit_value { packets | bytes }**
Send MBR to pause charging at P-GW if specified number of packets/bytes is dropped for a PDN connection.
drop_limit_value is an integer from 1 through 99999.

- **packets**: Configures drop-limit in packets.
- **bytes**: Configures drop-limit in bytes.

**Usage Guidelines**
Use this command to specify P-GW to pause charging on abnormal-s1-release, DDN failure notification, or if the number of packets or bytes dropped exceeds the configured limit.

**Examples**
Use the following command to signal P-GW to pause charging when the number of packets dropped exceeds 1000:

```
overcharge-protection drop-limit 1000 packets
```
**pdp-data-inactivity**

Configures the APN profile regarding PDP data inactivity. This command is specific to the SGSN.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > APN Profile Configuration

```bash
configure > apn-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name{apn-profile-profile_name}#
```

**Syntax Description**

```
pdp-data-inactivity { action { deactivate [ all-pdp | linked-pdp ] | detach-when { all-pdp-inactive | any-pdp-inactive } | timeout minutes minutes } } | default pdp-data-inactivity { action | timeout } no pdp-data-inactivity timeout

default

Reset the APN Profile configuration to the default values for PDP data-inactivity.

no

Disables the timeout feature of the PDP data-inactivity configuration for this APN profile.

**action**

Defines the action to be taken if PDP data-inactivity occurs:

- **deactivate** - defines which PDP context should be deactivated:
  - all-pdp - deactivates all PDP contexts.
  - linked-pdp - deactivates only linked PDP contexts.

- **detach-when** - defines the condition that warrants a detach:
  - all-pdp-inactive - detach when all PDP contexts are inactive.
  - any-pdp-inactive - detach when any PDP context is inactive.
timeout minutes minutes

Specifies the inactivity timeout in minutes. minutes: is an integer from 1 through 1440. Note that even though the timeout is set for minutes, the configuration displays in seconds.

Usage Guidelines

Use this command to define how the SGSN will handle a situation where the PDP is not fully active. Repeat the command, as needed, to configure more than one keyword-controlled function.

Examples

Use the following command to have the SGSN deactivate all PDP contexts associated with the APN when it detects the PDP is inactive:

*pdp-data-inactivity action deactivate all-pdp*

Use the following command to have the SGSN wait 2 minutes after detecting PDP data inactivity:

*pdp-data-inactivity timeout minutes 2*
**pdp-type-ipv4v6-override**

Configure the PDP type to use, per APN, if dual PDP type addressing is not supported by the network and the MS/UE requests the IPv4v6 PDP type.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > APN Profile Configuration

`configure > apn-profile profile_name`

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

`pdp-type-ipv4v6-override { ipv4 | ipv6 }`

`remove pdp-type-ipv4v6-override`

**remove**

Deletes the override configuration and reverts to the default behavior so the SGSN ignores the IPv4v6 request and sends IPv4 to the GGSN.

**ipv4**

Configures IPv4 as the PDP type to send towards the GGSN when overriding the dual PDP type addressing requested by the MS/UE.

**ipv6**

Configures IPv6 as the PDP type to send towards the GGSN when overriding the dual PDP type addressing requested by the MS/UE.

**Usage Guidelines**

This command configures the SGSN to send either IPv4 or IPv6 towards the GGSN when the MS/UE requests PDP type as IPv4v6 but either the SGSN or the RNC is not configured to support dual PDP type.

**Examples**

Use this command to configure the SGSN to always send IPv6, for the PDP type, to the GGSN when overriding a dual PDP type address request from the MS/UE:

```
pdp-type-ipv4v6-override ipv6
```
pgw-address

Configures the IPv4 and/or IPv6 address of the P-GW supporting the APN associated with this APN profile.

**Product**
- ePDG
- MME
- SaMOG
- SGSN

**Privilege**
- Administrator

**Command Modes**
- Exec > Global Configuration > APN Profile Configuration
- `configure > apn-profile profile_name`

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
pgw-address ip_address [ s5-s8-protocol pmip | { IP-ADDRESS ip_address | primary | secondary | weight weight | primary | secondary | } | fqdn fqdn_var | primary | secondary ]
no pgw-address ip_address
```

- `no` Disables the P-GW address configured in this APN profile.

- `ip_address` Specifies the IP address for the P-GW in IPv4 dotted-decimal or IPv6 colon-separated notation.

- `s5-s8-protocol pmip`
  - *MME only.* Configures the S5-S8 protocol for the gateway.

- `primary`
  - Configures the primary PGW for s2b interface.

- `secondary`
  - Configures the secondary PGW for s2b interface.
fqdn
Configures the FQDN to get the PGW IP address for s2b interface.

weight weight
Specifies the weight (preference) assigned to the addressed P-GW for load balancing. weight is an integer from 1 through 100 where 1 is the least preferred and 100 is the most preferred. If no weight is specified, the P-GW address is assigned a default weight of 1.

If a weight is assigned to an address, the weights of the P-GW(s) (that are operational) are totaled, and then a weighted round-robin selection is used to distribute new primary PDP contexts (for MME) or primary CPC requests (for SGSN) or new PDN connections (for ePDG) among the P-GW(s) according to their weights. As with all weighted round-robin algorithms, the distribution does not look at the current distribution, but simply uses the weights to distribute new requests. For example, two P-GWs assigned weights of 70 and 30 would distribute 70% of calls to one, and 30% to the other. The sum of all weights do not need to total 100.

Usage Guidelines
Use this command to define load balancing to be applied during P-GW selection. A maximum of 16 P-GW addresses can be configured for this APN profile.

On the S4-SGSN, use this command to configure a local P-GW address for operators wishing to bypass DNS resolution of APN FQDN.

Examples
The following command configures the P-GW IP address for this APN profile as 10.2.3.4:
pgw-address 10.2.3.4
qos allow-upgrade

Configure this command to allow upgrade of QoS from GGSN. The "Upgrade QoS Supported" flag is now set in "Create PDP Context" and "Update PDP Context" messages sent by SGSN. The SGSN signals the availability of this functionality by use of the "Upgrade QoS Supported" bit within the Common Flags IE. The SGSN sets the "Upgrade QoS Supported" bit within the Common Flags IE to "1" within the "Create PDP Context" and "Update PDP Context" procedures.

Product SGSN

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > APN Profile Configuration

command = apn-profile profile_name

Entering the above command sequence results in the following prompt:

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

Syntax Description qos allow-upgrade access-type { gprs | umts } [ prefer-as-cap-subscription ]

remove qos allow-upgrade access-type { gprs | umts }

remove

Removes the support for QoS upgrade from the configuration for this APN profile.

access-type { gprs | umts }

Allows the operator to choose the access type as either "gprs" or "umts" based on whether it is 2G or 3G network scenario.

prefer-as-cap-subscription

Enable this optional keyword to configure capping of QoS with Subscribed QoS (local/HLR). If this keyword is enabled, SGSN accepts a higher QoS in the Create/Update PDP Context Response than sent in Create/Update PDP Context Request, but negotiates and restricts the value within HLR/local subscribed QoS. If this keyword is disabled, the SGSN accepts the QoS in Create PDP Context Response and Update PDP Context Response as the Negotiated QoS (this QoS may be downgraded by the RNC in case of UMTS access).

Usage Guidelines This command enables the QoS upgrade support feature. On configuring this command, the SGSN sets the "Upgrade QoS Supported" flag within the common flags IE in Tunnel management messages, Create PDP Context Request and Update PDP Context Request messages. The SGSN accepts the QoS from GGSN in
Create PDP Context Response, Update PDP Context Request/Response messages as the Negotiated QoS for the PDP session.

**Examples**

Use the following command to configure QoS upgrade support in a UMTS scenario:  
`qos allow-upgrade access-type umts prefer-as-cap-subscription`
qos apn-ambr

Configures the APN-AMBR (aggregate maximum bit rate) that will be stored in the Home Subscriber Server (HSS).

**Product**
- MME
- SGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > APN Profile Configuration

```
configure > apn-profile profile_name
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**
```
qos apn-ambr max-ul mbr-up max-dl mbr-dwn
remove qos apn-ambr
```

**remove**
Removes the APN-AMBR changes from the configuration for this APN profile.

```
max-ul mbr-up max-dl mbr-dwn
```

Defines the maximum bit rates for uplink (subscriber to network) and downlink (network to subscriber) traffic.

- `mbr-up` is an integer from 0 through 1410065408.
- `mbr-dwn` is an integer from 0 through 1410065408.

**Usage Guidelines**
Use this command to define the MBR that will be enforced by the GGSN or P-GW for both uplink and downlink traffic shaping.

**Examples**
```
qos apn-ambr max-ul 24234222 max-dl 23423423
```
qos class

Configures local values for the traffic class (TC) parameters for the quality of service (QoS) configured for this APN profile.

---

**Important**

To enable any of the values/features configured with this command, the `qos prefer-as-cap` configuration (also in the APN profile configuration mode) must be set to either `local` or `both-hlr-and-local`.

---

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > APN Profile Configuration

`configure > apn-profile profile_name`

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

qos class { background | conversational | interactive | streaming } [ qualif_option ]

remove qos class { background | conversational | interactive | streaming } [ qualif_option ]

remove

Removes previously defined values for the specified option or for an entire class if a qualifying option is not included in the command.

**background**

Selects the background traffic class. This 'best-effort' class manages traffic that is handled as a background function, like email, where time to delivery is not a key factor. The selection of background traffic class can be refined with the addition of one of the following qualifying options:

- all-values
- arp
- mbr-down
- mbr-map-down
- mbr-map-up
• mbr-up
• residual-bit-error-rate
• sdu

All qualifying options are explained below.

**conversational**

Selects the 'real-time' conversational traffic class of service, which has the most stringent time requirements of the four classes and is typically reserved for voice traffic. The section of the conversational traffic class can be refined with the addition of one of the following qualifying options:

• all-values
• arp
• gbr-down
• gbr-up
• mbr-down
• mbr-map-down
• mbr-map-up
• mbr-up
• min-transfer-delay
• residual-bit-error-rate
• sdu

All qualifying options are explained below.

**interactive**

Selects interactive traffic class of service. This class is characterized by a request/response pattern (someone sends data and then waits for a response) which requires the preservation of the data but delivers on a 'best-effort' model. The section of the interactive traffic class can be refined with the addition of one of the following qualifying options:

• all-values
• arp
• mbr-down
• mbr-map-down
• mbr-map-up
• mbr-up
• residual-bit-error-rate
• sdu
• thp
All qualifying options are explained below.

**streaming**
Selects the streaming traffic class of service, which handles one-way, real-time data transmission - such as streaming video or audio. The section of the interactive traffic class can be refined with the addition of one of the following qualifying options:

- **all-values**
- **arp**
- **gbr-down**
- **gbr-up**
- **mbr-down**
- **mbr-map-down**
- **mbr-map-up**
- **mbr-up**
- **min-transfer-delay**
- **residual-bit-error-rate**
- **sdu**

All qualifying options are explained below.

**qualif_option**
Qualifying options are the QoS parameters and they include:

- **all-values** - This option will change the configuration to predefined values for all the relevant QoS parameters for the class. This keyword is not used if other options are to be defined. The predefined values are:

<table>
<thead>
<tr>
<th>QoS Parameter</th>
<th>Predefined Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic Class</td>
<td>Background</td>
</tr>
<tr>
<td>SDU delivery order</td>
<td>No</td>
</tr>
<tr>
<td>Delivery of Erroneous SDUs</td>
<td>No</td>
</tr>
<tr>
<td>Max Bit Rate Uplink</td>
<td>64 kbps</td>
</tr>
<tr>
<td>Max Bit Rate Downlink</td>
<td>64 kbps</td>
</tr>
<tr>
<td>Allocation/Retention Priority</td>
<td>3</td>
</tr>
<tr>
<td>SDU Max Size</td>
<td>1500 octets</td>
</tr>
<tr>
<td>QoS Parameter</td>
<td>Predefined Value</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td>SDU Error Ratio</td>
<td>$3 \times (1 \times 10^{-3})$</td>
</tr>
<tr>
<td>Residual Bit Error Rate</td>
<td>$4 \times (4 \times 10^{-3})$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Traffic Class</th>
<th>Conversational</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDU delivery order</td>
<td>No</td>
</tr>
<tr>
<td>Delivery of Erroneous SDUs</td>
<td>No</td>
</tr>
<tr>
<td>Max Bit Rate Uplink</td>
<td>16 kbps</td>
</tr>
<tr>
<td>Max Bit Rate Downlink</td>
<td>16 kbps</td>
</tr>
<tr>
<td>Allocation/Retention Priority</td>
<td>3</td>
</tr>
<tr>
<td>Guaranteed Bit Rate Uplink</td>
<td>16 kbps</td>
</tr>
<tr>
<td>Guaranteed Bit Rate downlink</td>
<td>16 kbps</td>
</tr>
<tr>
<td>SDU Max Size</td>
<td>1500 octets</td>
</tr>
<tr>
<td>Minimum Transfer Delay</td>
<td>100 milliseconds</td>
</tr>
<tr>
<td>SDU Error Ratio</td>
<td>$1 \times (1 \times 10^{-2})$</td>
</tr>
<tr>
<td>Residual Bit Error Rate</td>
<td>$1 \times (5 \times 10^{-2})$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Traffic Class</th>
<th>Interactive</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDU delivery order</td>
<td>No</td>
</tr>
<tr>
<td>Delivery of Erroneous SDUs</td>
<td>No</td>
</tr>
<tr>
<td>Max Bit Rate Uplink</td>
<td>64 kbps</td>
</tr>
<tr>
<td>Max Bit Rate Downlink</td>
<td>64 kbps</td>
</tr>
<tr>
<td>Traffic Handling Priority</td>
<td>3</td>
</tr>
<tr>
<td>SDU Max Size</td>
<td>1500 octets</td>
</tr>
<tr>
<td>SDU Error Ratio</td>
<td>$3 \times (1 \times 10^{-3})$</td>
</tr>
<tr>
<td>Residual Bit Error Rate</td>
<td>$4 \times (4 \times 10^{-3})$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Traffic Class</th>
<th>Streaming</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDU delivery order</td>
<td>No</td>
</tr>
<tr>
<td>Delivery of Erroneous SDUs</td>
<td>No</td>
</tr>
<tr>
<td>Max Bit Rate Uplink</td>
<td>16 kbps</td>
</tr>
<tr>
<td>Max Bit Rate Downlink</td>
<td>16 kbps</td>
</tr>
<tr>
<td>QoS Parameter</td>
<td>Predefined Value</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Allocation/Retention Priority</td>
<td>3</td>
</tr>
<tr>
<td>Guaranteed Bit Rate Uplink</td>
<td>16 kbps</td>
</tr>
<tr>
<td>Guaranteed Bit Rate downlink</td>
<td>16 kbps</td>
</tr>
<tr>
<td>SDU Max Size</td>
<td>1500 octets</td>
</tr>
<tr>
<td>Minimum Transfer Delay</td>
<td>300 milliseconds</td>
</tr>
<tr>
<td>SDU Error Ratio</td>
<td>7 (1 * 10^-3)</td>
</tr>
<tr>
<td>Residual Bit Error Rate</td>
<td>1 (5 * 10^-2)</td>
</tr>
</tbody>
</table>

- **arp** - Sets the allocation/retention priority. Enter an integer from 1 to 3.
- **gbr-down** - Guaranteed Kbps rate for the downlink direction. Enter an integer from the range 1 to 256000.
- **gbr-up** - Guaranteed Kbps rate for the uplink direction. Enter an integer from 1 to 256000.
- **mbr-down** - Maximum Kbps rate for the downlink direction. Enter an integer from the range 1 to 256000.
- **mbr-map-down from** from_kbps to to_kbps - Map received HLR MBR (from value) to a locally configured downlink MBR value (to value):
  - from_kbps - Enter an integer from 1 to 25600.
  - to_kbps - Enter an integer from 1 to 25600.
- **mbr-map-up from** from_kbps to to_kbps - Map received HLR MBR (from value) to a locally configured uplink MBR value (to value):
  - from_kbps - Enter an integer from 1 to 25600.
  - to_kbps - Enter an integer from 1 to 25600.
- **mbr-up** - Maximum Kbps rate for the uplink direction. Enter an integer from 1 to 256000.
- **min-transfer-delay** - Minimum transfer delay in milliseconds. Enter an integer from 80 to 4000.
- **residual-bit-error-rate** -
  - Background TC residual-bit-error-rate range is from 4*10^-4 to 6*10^-8. Enter on of the following integers, where:
    - 4: represents 4*10^-3
    - 7: represents 10^-5
    - 9: represents 6*10^-8
  - Conversational TC residual-bit-error-rate range is from 5*10^-2 to 10^-6. Enter one of the following integers, where:
    - 1: represents 5*10^-2
Interactive TC residual-bit-error-rate range is from $4 \times 10^{-4}$ to $6 \times 10^{-8}$. Enter one of the following integers, where:

* 4: represents $4 \times 10^{-3}$
* 7: represents $10^{-5}$
* 9: represents $6 \times 10^{-8}$

Streaming TC residual-bit-error-rate range is from $5 \times 10^{-2}$ to $10^{-6}$. Enter one of the following integers, where:

* 1: represents $5 \times 10^{-2}$
* 2: represents $10^{-2}$
* 3: represents $5 \times 10^{-3}$
* 5: represents $10^{-3}$
* 6: represents $10^{-4}$
* 7: represents $10^{-5}$
* 8: represents $10^{-6}$

**sd**u - Signalling data unit keyword, must include one of the following options:

* **delivery-order** - Enter one of the two following options:
  * no - Without delivery order
  * yes - With delivery order

* **erroneous** - Enter one of the two following options:
  * no - Erroneous SDUs will not be delivered
  * no-detect - Erroneous SDUs are not detected ('-')
  * yes - Erroneous SDUs will be delivered

* **error-ratio** - The SDU error-ratio range is from $10^{-3}$ to $10^{-6}$. Enter an integer from 1 to 6, where:
  * 3 - Represents $10^{-3}$
• **-4** Represents \(10^{-4}\)
• **-6** Represents \(10^{-6}\)

- **max-size** - Defines the maximum number of octets (size) of the SDU. Enter an integer from 10 to 1502.

- **thp** - Sets the traffic handling priority. Enter an integer from 1 to 3.

**Usage Guidelines**

This command defines the qualifying options (parameters) for each QoS traffic class defined for this APN profile.

**Important**

Typically this command is only used to define QoS parameters when the APN record does not exist in the subscription record.

Repeat the command as often as needed with different options to define all required QoS criteria. For example, to configure the maximum bit rate (MBR) for the downlink and uplink directions for a traffic class, this command must be used twice, specifying **mbr-down** once and **mbr-up** once.

Advantage for local mapping of MBR: some HLRs cannot be configured with high MBR values. Using the **mbr-map-up** and the **mbr-map-down** parameters allows the SGSN to be configured to treat a specific HLR value as meaning the desired high MBR value. In a case where the HLR does not support HSPA+ bit rates, but the handsets and network do, this feature allows the operator to overcome limitations on the HLR and provide HSPA+ bit rates by overwriting the provisioned HLR-QoS MBR values with SGSN-configured values. When MBR mapping is configured, if QoS is preferred as the HLR value, then the subscription QoS MBR received from the HLR is compared with the "from" value in the table. If it matches, then it is converted to the value specified by the "to" value in the table. QoS negotiation happens based on the converted value.

Advantage for QoS capping with THP and ARP: Controlling THP and ARP via Operator Policy: This functionality can differentiate home vs. roaming subscribers, and prevent visiting subscribers from receiving a high-tiered service. For example, a service provider could offer service differentiation using Ultra/Super/Standard service levels based upon QoS; this could justify charging a corporate customer more to use the Internet APN than would be charged to a consumer. This could be accomplished by controlling the traffic handling priority (THP) over the air interface, i.e. THP 1 = Ultra, THP 2 = Super and THP 3 = Standard.

**Examples**

Use the following command to configure the entire conversational traffic class with predefined QoS options:

```
qos class conversational all-values
```

Now change the background class ARP from 3 to 2:

```
qos class background arp 2
```

Invalidate the THP parameter, by removing all value from the parameter, for the interactive class:

```
remove qos class interactive thp
```
qos dedicated-bearer

Configures the quality of service maximum bit rate (MBR) parameters for the dedicated bearer. This command is specific to the MME.

**Product**
MME

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > APN Profile Configuration
configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:

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

**Syntax Description**
```
qos dedicated-bearer mbr max-ul mbr-up max-dl mbr-dl
remove qos dedicated-bearer
```

- **remove**
  Removes the dedicated bearer maximum bit rate (MBR) changes from the configuration for this APN profile.

  ```
  max-ul mbr-up max-dl mbr-dl
  ```
  Defines the maximum bit rates for uplink and downlink traffic.
  - `mbr-up` is an integer from 0 through 1410065408.
  - `mbr-dl` is an integer from 0 through 1410065408.

**Usage Guidelines**
Use this command to define the MBRs that will be enforced by the P-GW for both uplink and downlink traffic shaping.

**Examples**
```
qos dedicated-bearer mbr max-ul 24234222 max-dl 23423423
```
**qos default-bearer**

Configures the quality of service parameters for the default bearer. This command is specific to the MME.

**Product**

MME

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > APN Profile Configuration

```
configure > apn-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name{apn-profile-profile_name}#
```

**Syntax Description**

```
qos default-bearer { arp arp_value | preemption-capability { may | shall-not } | vulnerability { not-preemptable | preemptable } | qci qci } remove qos default-bearer { arp | qci }
```

**remove**

Removes the default bearer QoS configuration from this APN profile.

**arp**

```
arp arp_value
```

Defines the address retention priority value. *arp_value* is an integer from 1 through 15.

**preemption-capability**

```
preemption-capability { may | shall-not }
```

Specifies the preemption capability flag. Options are:

- **may**: Bearer may be preempted
- **shall-not**: Bearer shall not be preempted

**vulnerability**

```
vulnerability { not-preemptable | preemptable }
```

Specifies the vulnerability flag. Options are:

- **not-preemptable**: Bearer cannot be preempted.
- **preemptable**: Bearer can be preempted.
**qci qci**

Specifies the QoS Class Identifier for the default bearer profile. `qci` is an integer from 0 through 255.

**Usage Guidelines**

Use this command to set the QoS APR and QCI parameters for the default bearer configuration.

**Examples**

```
qos default-bearer arp 2 preemption-capability may
```
qos pgw-upgrade

Configures the action to be taken when the MME receives a QoS upgrade from P-GW for default bearers/Non-Guaranteed Bit Rate (Non-GBR) bearers.

**Product**

MME

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > APN Profile Configuration

`configure > apn-profile profile_name`

Entering the above command sequence results in the following prompt:

```
[local] host_name{apn-profile-profile_name}#
```

**Syntax Description**

```
qos pgw-upgrade non-gbr { accept | reject | locally-cap }
| remove qos pgw-upgrade non-gbr
```

**remove**

Removes the configuration, returning the system to the default setting where the MME accepts the P-GW upgraded QoS values for Non-GBR (default) bearers.

```
non-gbr { accept | reject | locally-cap }
```

For Non-GBR (default) bearers, this keyword configures the action the MME takes when it receives a P-GW upgraded QoS value.

- **accept**: The MME will accept the P-GW upgraded QoS values.
- **reject**: The MME will reject the P-GW upgraded QoS values.
- **locally-cap**: The MME compares QCI, ARP and ARP-PVI provided by P-GW to the locally configured values of those parameters. If the values match, then accepts towards the P-GW and use locally configured values towards the UE/RAN for APN-AMBR and ARP-PCI. If the values do not match, the MME rejects the P-GW upgraded QoS values.

**Usage Guidelines**

Use this command to provide configurability at the APN Profile level for the MME to accept, reject, or locally-cap P-GW upgraded QoS values for default (non-GBR) bearers. This S11 Control is applied whenever QoS parameters are received on S11 interface. The relevant procedures for default bearers are Create Session Response (sent by P-GW during Attach, UE requested PDN connectivity) and Update Bearer Procedures.
(initiated by P-GW resulting from trigger QoS change or other in PCEF/PCRF, or from Modify Bearer Command or Bearer Resource Command sent by MME). \textbf{Note:} This configuration is supported only for Default bearers (i.e Non-GBR bearers) in a roaming scenario.

The MME will set the sum of the APN-AMBR of all active APNs up to the value of the subscribed UE-AMBR, subject to the UE-AMBR restriction.

In the case of an Attach Reject or PDN Connectivity Reject, the ESM failure cause "Operator determined barring" is used and the corresponding MME schema bulk statistic is incremented.

In the case of Update Bearer Request Reject, the EGTP cause "Request rejected" is used and the corresponding EGTP bulk statistic is incremented.

A session disconnect reason mme-qos-pgw-upgrade-reject(589) is incremented when QoS upgrade by P-GW is rejected by the MME during initial attach. The corresponding session disconnect reason statistics are incremented.

Refer to the \texttt{dedicated-bearing} command to configure QoS controls for dedicated bearers (GBR and Non-GBR).

\textbf{Examples}

The following command configures the MME to reject the QoS upgrade from P-GW for non-GBR bearers:

\texttt{qos pgw-upgrade non-gbr reject}
qos prefer-as-cap

Specifies operational preferences for QoS parameters, specifically QoS bit rates. This command is specific to the SGSN in releases prior to 14.0.

**Product**
- MME
- SGSN

**Privilege**
- Security Administrator, Administrator

**Command Modes**
- `Exec > Global Configuration > APN Profile Configuration`

```
configure > apn-profile profile_name
```

Entering the above command sequence results in the following prompt:
```
[local] host_name(apn-profile-profile_name) #
```

**Syntax Description**
```
qos prefer-as-cap { both-hlr-and-local | both-hss-and-local { local-when-subscription-not-available | minimum | subscription-exceed-reject } | hlr-subscription | local }
remove qos prefer-as-cap
```

**Important**
Command and keyword names have changed. `prefer` has become `prefer-as-cap` and `hlr` has become `hlr-subscription`. These changes will not impact configuration generated with earlier releases as the keywords are aliases for the previous names.

**remove**
Removes previous configuration changes and resets the default.

**both-hlr-and-local**
Instructs the SGSN to use, as the capping value during session establishment, the lower of either the locally configured QoS bit rate or the Home Location Register (HLR) subscription.

**both-hss-and-local { local-when-subscription-not-available | minimum | subscription-exceed-reject }**
For the MME only, specifies the QoS cap value to use.

- **local-when-subscription-not-available**: Use the locally configured values if the Home Subscriber Server (HSS) does not provide any values.
• **minimum**: Use the lower of either the locally configured QoS bit rate or the HSS-provided QoS bit rate.

• **subscription-exceed-reject**: If the requested QoS bit rate exceeds the locally configured value, reject the PDN connection.

**hlr-subscription**

Instructs the SGSN to take the QoS bit rates from the HLR configuration and use the HLR rate as the capping value for session establishment.

Default for SGSN.

**local**

Instructs the SGSN to take the QoS bit rate from the local configuration and use it for session establishment.

**Usage Guidelines**

Use this command to instruct the SGSN or MME to take QoS configuration as the bit rate for session establishment.

The MME has no default setting for this command.

**Examples**

The following command specifies use of the bit rate in subscription at the HLR:

```
qos prefer-as-cap hlr-subscription
```

The following command instructs the SGSN to cap the bit rate with the lower rate of the two configurations, HLR or local:

```
qos prefer-as-cap both-hlr-and-local
```
qos rate-limit direction

Configures the actions governing the subscriber traffic flow, if the flow violates or exceeds the configured or negotiated peak or committed data-rates.

This command can be entered multiple times to specify different combinations of traffic direction and class. The SGSN only performs traffic policing if **qos rate-limit direction** is configured.

Additional information on the QoS traffic policing functionality is located in the *System Administration Guide*.

**Product**  
SGSN  
S-GW  
SAEGW

**Privilege**  
Security Administrator, Administrator

**Command Modes**  
Exec > Global Configuration > APN Profile Configuration  
**configure > apn-profile profile_name**

Entering the above command sequence results in the following prompt:  

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

**Syntax Description**

```
remove qos rate-limit direction { downlink | uplink } [ class { background | conversational | interactive traffic_priority | streaming } ]
```

**remove**

Removes the qos rate-limit direction entries from the configuration.

**downlink | uplink**

Apply the limits and actions configured with the other keywords to the selected link:

**downlink** - This is the direction from the GGSN or P-GW to the MS.

**uplink** - This is the direction from the MS to the GGSN or the P-GW.
burst-size { auto-readjust | duration seconds | bytes }

Default: See the table of class default values in the Usage section below.

This keyword specifies the peak burst size allowed. System measurements for this value exclude the GTP and outer packet headers. Supported options include:

- **auto-readjust**: This keyword enables dynamic burst-size calculation using negotiated peak data-rate and negotiated committed data-rate.
- **duration seconds**: Must be an integer from 1 to 30; default is 1. This keyword sets the number of seconds that the dynamic burst-size calculation will last. This allows the traffic to be throttled at the negotiated rates.
- **bytes**: Must be an integer from 1 to 6000000. This value specifies the static burst size for traffic policing. This option is present for backward compatibility.

---

**Important**

Use of dynamic burst size (**auto-readjust**) for traffic policing is recommended, rather than the static burst size.

---

class { background | conversational | interactive traffic_priority | streaming }

The **class** keyword configures the specified traffic policing actions per traffic class, or per traffic priority in the case of interactive traffic class. The following classes are supported:

- **background**: Specifies the traffic action for traffic patterns in which the data transfer is not time-critical (for example, email exchanges).
- **conversational**: Specifies the traffic policing action for traffic patterns in which there is a constant flow of packets in each direction, upstream and downstream.
- **interactive traffic_priority**: Specifies the traffic policing action for traffic patterns in which there is an intermittent flow of packets in each direction, upstream and downstream. 
  
  *traffic_priority* is the 3GPP traffic handling priority and can be an integer 1, 2 or 3.
- **streaming**: Specifies the traffic policing action for traffic patterns in which there is a constant flow of data in one direction, either upstream or downstream.

---

**Important**

This is an SGSN-specific feature. If this keyword is omitted, the same values are used for all classes.

---

exceed-action { drop | lower-ip-precedence | transmit }

Default: See the table of class default values in the Usage section below.

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
gbr-qci [ committed-auto-readjust duration seconds ]
Appplies the traffic policing policy to guaranteed bitrate bearers.

committed-auto-readjust duration seconds: Must be an integer from 1 to 30. This keyword sets the number of seconds that the committed burst-size calculation will last. This allows the traffic to be throttled to the negotiated rates.

Important This is an S-GW-specific feature.

non-gbr-qci [ committed-auto-readjust duration seconds ]
Appplies the traffic policing policy to non-guaranteed bitrate bearers.

committed-auto-readjust duration seconds: Must be an integer from 1 to 30. This keyword sets the number of seconds that the committed burst-size calculation will last. This allows the traffic to be throttled to the negotiated rates.

Important This is an S-GW-specific feature.

violate-action { drop | lower-ip-precedence | transmit }
Default: See the table of class default values in the Usage section below.
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: Drops the packet
• lower-ip-precedence: Transmits the packet after lowering the IP precedence
• transmit: Transmits the packet

+ This symbol indicates that the keywords can be entered multiple times within a single command.

Usage Guidelines
This command configures the APN's quality of service (QoS) traffic policing. Configured actions prevent subscriber flow exceeding or violating configured peak or negotiated peak or committed data rate limits.

Important If either exceed action or violate action is set to lower-ip-precedence, this command may override the configuration of the ip qos-dscp command in the APN profile.

Class: Background
### APN Profile Configuration Mode

#### qos rate-limit direction

<table>
<thead>
<tr>
<th>Downlink Traffic: Disabled</th>
<th>Uplink Traffic: Disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peak Data Rate (in bps): 16000000</td>
<td>Peak Data Rate (in bps): 8640000</td>
</tr>
<tr>
<td>Committed Data Rate (in bps): n/a</td>
<td>Committed Data Rate (in bps): n/a</td>
</tr>
<tr>
<td>Burst Size (in bytes): 65535</td>
<td>Burst Size (in bytes): 65535</td>
</tr>
<tr>
<td>Exceed Action: n/a</td>
<td>Exceed Action: n/a</td>
</tr>
<tr>
<td>Violate Action: drop</td>
<td>Violate Action: drop</td>
</tr>
</tbody>
</table>

**Class: Conversational**

<table>
<thead>
<tr>
<th>Downlink Traffic: Disabled</th>
<th>Uplink Traffic: Disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peak Data Rate (in bps): 16000000</td>
<td>Peak Data Rate (in bps): 8640000</td>
</tr>
<tr>
<td>Committed Data Rate (in bps): 16000000</td>
<td>Committed Data Rate (in bps): 8640000</td>
</tr>
<tr>
<td>Burst Size (in bytes): 65535</td>
<td>Burst Size (in bytes): 65535</td>
</tr>
<tr>
<td>Exceed Action: lower-ip-precedence</td>
<td>Exceed Action: lower-ip-precedence</td>
</tr>
<tr>
<td>Violate Action: drop</td>
<td>Violate Action: drop</td>
</tr>
</tbody>
</table>

**Class: Interactive, Traffic Handling Priority: 1**

<table>
<thead>
<tr>
<th>Downlink Traffic: Disabled</th>
<th>Uplink Traffic: Disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peak Data Rate (in bps): 16000000</td>
<td>Peak Data Rate (in bps): 8640000</td>
</tr>
<tr>
<td>Committed Data Rate (in bps): n/a</td>
<td>Committed Data Rate (in bps): n/a</td>
</tr>
<tr>
<td>Burst Size (in bytes): 65535</td>
<td>Burst Size (in bytes): 65535</td>
</tr>
<tr>
<td>Exceed Action: n/a</td>
<td>Exceed Action: n/a</td>
</tr>
<tr>
<td>Violate Action: drop</td>
<td>Violate Action: drop</td>
</tr>
</tbody>
</table>

**Class: Interactive, Traffic Handling Priority: 2**

<table>
<thead>
<tr>
<th>Downlink Traffic: Disabled</th>
<th>Uplink Traffic: Disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peak Data Rate (in bps): 16000000</td>
<td>Peak Data Rate (in bps): 8640000</td>
</tr>
<tr>
<td>Committed Data Rate (in bps): n/a</td>
<td>Committed Data Rate (in bps): n/a</td>
</tr>
<tr>
<td>Burst Size (in bytes): 65535</td>
<td>Burst Size (in bytes): 65535</td>
</tr>
<tr>
<td>Exceed Action: n/a</td>
<td>Exceed Action: n/a</td>
</tr>
<tr>
<td>Violate Action: drop</td>
<td>Violate Action: drop</td>
</tr>
</tbody>
</table>

**Class: Interactive, Traffic Handling Priority: 3**
Downlink Traffic: Disabled  
Peak Data Rate (in bps): 16000000  
Committed Data Rate (in bps): n/a  
Burst Size (in bytes): 65535  
Exceed Action: n/a  
Violate Action: drop  

Uplink Traffic: Disabled  
Peak Data Rate (in bps): 8640000  
Committed Data Rate (in bps): n/a  
Burst Size (in bytes): 65535  
Exceed Action: n/a  
Violate Action: drop  

Class: Streaming  

Downlink Traffic: Disabled  
Peak Data Rate (in bps): 16000000  
Committed Data Rate (in bps): n/a  
Burst Size (in bytes): 65535  
Exceed Action: n/a  
Violate Action: drop  

Uplink Traffic: Disabled  
Peak Data Rate (in bps): 8640000  
Committed Data Rate (in bps): n/a  
Burst Size (in bytes): 65535  
Exceed Action: n/a  
Violate Action: drop  

Examples

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
```

The following command drops the excess user packets when the subscriber traffic violates both the configured peak and the committed data-rate in the uplink direction. Once either the peak or the committed data-rate for that subscriber goes below the configured/negotiated limit, it transmits them.

```
qos rate-limit direction uplink exceed-action drop
```
ranap allocation-retention-priority-ie

Configures the allocation/retention priority (ARP) IE for this APN profile. This command is specific to the SGSN.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > APN Profile Configuration
configure > apn-profile *profile_name*

Entering the above command sequence results in the following prompt:

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

**Syntax Description**
```
ranap allocation-retention-priority-ie subscription-priority *priority* class { { background | conversational | interactive | streaming } { not-pre-emptable | priority | queuing-not-allowed | shall-not-trigger-pre-emptable } + }
```

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

```
| default | remove | no | ranap allocation-retention-priority-ie | subscription-priority *priority* class { background | conversational | interactive | streaming } |
```

**default**
Resets the configuration to the default values.

**no**
Disables the specified configuration

**remove**
Removes the specified configuration.

**subscription-priority *priority***
This keyword sets the subscription priority. The lowest number has the highest priority.

*priority* must be an integer from 1 to 3.
Configure allocation/retention priority (ARP) for specific QoS traffic classes. Include one or more of the following class options:

- **background**: background class of service
- **conversational**: conversational class of service
- **interactive**: interactive class of service
- **streaming**: streaming class of service

Default values will be included in the configuration for any class configuration not specified.

**qualifying options**

For each of the class options, the configuration must include one or more of the following qualifying options:

- **not-pre-emptable**
- **priority**: smallest number is the highest priority. Value must be an integer from 1 to 15
- **queuing-not-allowed**
- **shall-not-trigger-pre-emptable**

When entering more than one option, we recommend that you do it in the order in which they are listed.

+ This symbol indicates that the keywords can be entered multiple times within a single command.

**Usage Guidelines**

Use this command to configure values for the allocation/retention priority (ARP) IE in the radio access bearer (RAB) assignment request message for RANAP that occurs during RAB setup.

This command can be used multiple times to define multiple priorities, with different combinations of **subscription-priority** and **class**.

If the HLR returns a matching value for the subscribed ARP for the desired traffic class, the SGSN includes the configured qualifying options for the ARP IE in the RANAP message.

If there is no matching configuration, the SGSN includes the following default values for the traffic class within the ARP IE:

**Table 2: Default ARP Values**

<table>
<thead>
<tr>
<th>Subscribed ARP</th>
<th>Traffic Class</th>
<th>RANAP Priority value</th>
<th>RANAP Preemption Capability</th>
<th>RANAP Preemption Vulnerability</th>
<th>RANAP Queuing Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Conversational</td>
<td>1</td>
<td>0 (may-trigger-pre-emption)</td>
<td>0 (not-pre-emptable)</td>
<td>queuing-not-allowed</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>2</td>
<td>0 (may-trigger-pre-emption)</td>
<td>1 (pre-emptable)</td>
<td>queuing-not-allowed</td>
</tr>
</tbody>
</table>
### Examples

The following series of commands define the highest priority for conversational traffic class with priority level 1-10 (Subscribed priority 0-3), PCI of shall-not-trigger-pre-emption, PVI of not-pre-emptable with queuing-not-allowed:

```
ranap allocation-retention-priority-ie subscription-priority 0 priority class conversational
not-pre-emptable priority 1 shall-not-trigger-pre-emptable
ranap allocation-retention-priority-ie subscription-priority 1 priority class conversational
not-pre-emptable priority 4 shall-not-trigger-pre-emptable
ranap allocation-retention-priority-ie subscription-priority 2 priority class conversational
not-pre-emptable priority 7 shall-not-trigger-pre-emptable
ranap allocation-retention-priority-ie subscription-priority 3 priority class conversational
not-pre-emptable priority 10 shall-not-trigger-pre-emptable
```
restrict access-type

Configures the activation restrictions of PDP context on the basis of the access type and QoS class.

**Product**

SGSN

MME

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > APN Profile Configuration

configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:

```
[local] host_name{apn-profile-profile_name}#
```

**Syntax Description**

```
[ no ] restrict access-type { eps | { { gprs | umts } | qos-class { background | conversational | interactive | streaming } } }  
default restrict access-type { eps | gprs | umts }
```

**no**

Remove the restriction rules for PDP context activation configured in this APN profile.

**default**

 Resets the restriction rules for PDP context activation to the default values to allow all access types and with QoS class for GPRS and UMTS.

**eps**

Configures the APN profile to restrict the PDP context activation from EPS (Evolved Packet System) network access.

**gprs**

Configures the APN profile to restrict the PDP context activation from General Packet Radio Service (2.5G) network access.

**umts**

Configures the APN profile to restrict the PDP context activation from Universal Mobile Telecommunications Systems (3G) network access.
**qos-class**

Configures the APN profile to restrict the PDP context activation to a specific QoS traffic class. It is optional and can be configured after selecting the network access type. Possible traffic classes options are:

- **background**: Specifies the QoS class as background service session
- **conversational**: Specifies the QoS class as conversational service session
- **interactive**: Specifies the QoS class as interactive service session
- **streaming**: Specifies the QoS class as streaming service session

**Usage Guidelines**

Use this command to configure the restriction rules in an APN profile for activation of PDP context on the basis of the access type. It also provides the facility to restrict type of traffic QoS class.

**Important**

From release 19.0 onwards this command is also supported for MME. In earlier releases this command was supported only on SGSN.

This command is used to configure the APN not supported in particular RAT and PLMN combinations. If this command is enabled, new PDP activations to an APN with which this APN profile is associated are rejected. During handovers PDPs/PDNs are deactivated if the APN name matches with this APN profile.

If the operator does not include the optional QoS-Class keyword option, then complete APN restriction is enabled. And QoS related restrictions have no impact, as QoS restriction is subset of a complete APN restriction.

**Examples**

The following command configures the APN profile to restrict all traffic from a GPRS network service having a QoS class of interactive:

```
restrict access-type grps qos-class interactive
```
sm t3396

The `sm` command includes a new keyword to set the SM T3396 back-off timer for an APN Profile.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > APN Profile Configuration

`configure > apn-profile profile_name`

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
sm t3396 min minimum_minutes max maximum_minutes cause code
remove sm t3396
```

**remove**

Including this filter with the command removes the SM back-off timer definition from the APN Profile configuration.

**min minimum_minutes**

Enter an integer from 1 to 15 to identify the minimum number of minutes the timer should run; default is 15 minutes.

**max maximum_minutes**

Enter an integer from 1 to 30 to identify the maximum number of minutes the timer should run; default is 30 minutes.

**cause code**

Enter an integer from 1 to 255 to identify the appropriate rejection cause code. The default is 26. During congestion, the configured value is ignored and 26 is sent.

**Usage Guidelines**

- Under congestion, the SGSN can assign the T3396 back-off timers to the UEs and request the UEs not to access the network for a given (timer value) period of time.
• If a message is rejected due to congestion, then the T3396 value will be included in the reject message with cause code 26. The SM back-off timer value sent will be chosen randomly from within the configured T3396 timer value range.

• If T3396 timer value is configured in an APN Profile then it will override the back-off timer values defined for either the SGSN Service or GPRS Service configurations.

Examples

Use a command similar to the following to define a T3396 with a timeout range of 2 to 15 minutes.

`sm t3396 min 2 max 15`
**timeout bearer-inactivity**

Supports a bearer inactivity timeout for GBR and non-GBR S-GW bearer type sessions.

**Product**

- S-GW
- SAEGW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration > APN Profile Configuration

```plaintext
configure > apn-profile profile_name
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```plaintext
[ remove ] timeout bearer-inactivity [ gbr | non-gbr ] dur_seconds volume-threshold { total bytes | uplink bytes | downlink bytes } | exclude-default-bearer
```

- **remove**
  Removes the timeout bearer-inactivity setting.

- **timeout**
  Specifies that a session time out value will be configured for this APN profile.

- **bearer-inactivity**
  Specifies that a session time out value will be configured for this APN profile.

- **gbr dur_seconds**
  Specifies that the system will check for low activity on a GBR bearer. `dur_seconds` specifies the bearer inactivity timer in seconds. Valid entries are from 900 to 2592000 seconds (15 minutes to 720 hours).

- **non-gbr dur_seconds**
  Specifies that the system will check for low activity on a non-GBR bearer. `dur_seconds` specifies the bearer inactivity timer in seconds. Valid entries are from 900 to 2592000 seconds (15 minutes to 720 hours).
volume-threshold
Specifies that a threshold value of the data traffic for a bearer will be used for the inactivity timeout value.

total bytes
Specifies that the total of both uplink and downlink data will be used as a volume threshold. bytes must be a value from 1 to 4294967295.

uplink bytes
Specifies that an uplink data volume threshold will be used. bytes must be a value from 1 to 4294967295.

downlink bytes
Specifies that a downlink data volume threshold will be used. bytes must be a value from 1 to 4294967295.

exclude-default-bearer
Specifies that inactivity handling for the default bearer will be excluded.

Usage Guidelines
Use this command to support a bearer inactivity timeout for GBR and non-GBR S-GW bearer type sessions per Qos Class Identifier (QCI). This enables the deletion of bearers experiencing less data traffic than the configured threshold value. This allows for more efficient use of system resources. This feature is supported only for Pure S calls on the SAE-GW.

Examples
The following example configures a 5 minute dedicated bearer timeout setting for GBR bearers on a downlink volume threshold of 100000 bytes.

timeout bearer-inactivity gbr 300 downlink 100000
timeout idle

Configures the subscriber's time-to-live (TTL) settings for the EPDG service.

**Product**
ePDG

**Privilege**
System Administrator, Administrator

**Command Modes**
Exec > Global Configuration > Context Configuration > APN Profile Config

```
configure > apn-profile apn_profile_name
```

The following prompt is displayed in the APN Profile Config mode:

```
[local] host_name(apn-profile-profname1)#
```

**Syntax Description**

```
timeout idle sec { micro-checkpoint-deemed-idle [ dur ] | micro-checkpoint-periodicity dur } 
no timeout idle 
default timeout idle

no
```

Disables idle timeout configuration along with the idle seconds micro-checkpoint duration or deemed idle duration configuration.

```
default
```

Configures the default value for subscriber’s timeout settings. The idle timeout default value is 0. The default value of micro-checkpoint-deemed-idle would be 0 seconds and that for micro-checkpoint-periodicity is 10 seconds.

```
idle sec
```

Designates the maximum duration a session can remain idle, in seconds, before system automatically terminates the session. Must be followed by number of seconds between 0 and 2147483647. Zero indicates function is disabled.

```
micro-checkpoint-deemed-idedle dur
```

Configures micro-checkpoint duration when UE is deemed idle for this Subscriber. Default is "0" (disabled).

dur is an integer between 10 and 1000.
micro-checkpoint-periodicity\textit{dur}

Configures the micro-checkpoint-periodicity for this Subscriber. Default is "10". \textit{dur} is the an integer between 10 and 10000.

**Syntax Description**

Use this command to configure the subscriber's time-to-live (TTL) settings for the EPDG service.

**Examples**

The following command configures the idle timeout to \textit{10} and micro-checkpoint-periodicity to \textit{50} for the subscriber:

\texttt{timeout idle 10 micro-checkpoint-periodicity 50}
**twan**

Configures the APN profile with the default gateway address and mask to be sent in the DHCP offer and PBA messages. This command is specific to SaMOG.

**Product**
SaMOG

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration > APN Profile Configuration

```
configure > apn-profile profile_name
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
| no | twan default-gateway ipv4/ipv6_address/mask
```

*no*

Removes the default gateway configuration from this APN profile.

```
ipv4/ipv6_address/mask
```

Specifies the IP address of the default gateway sent in the DHCP offer and PBA messages for a 3G session. *ipv4/ipv6_address* must be an IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation. *mask* must be an integer value from 1 to 32 for IPv4 addresses, and 1 to 128 for IPv6 addresses (CIDR notation).

**Usage Guidelines**

Use this command to configure the APN profile with the default gateway address and mask to be sent in the DHCP offer and PBA messages. This configuration is required for GTPv1 support only. For 3G subscribers, if the configured default gateway is unavailable, or does not match with the subnet of the allocated IP from P-GW or GGSN, the call will be dropped.

A maximum of 16 IP addresses and subnet masks can be configured (in separate lines) for each APN profile.

**Examples**

The following command configures the APN profile with the default gateway address and mask of 194.122.12.20/12:

```
twan default-gateway 194.122.12.20/12
```
virtual-mac

Configures or validates the virtual MAC address for this APN profile to use as the default gateway's MAC address for the user equipment (UE).

Product

SaMOG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > APN Profile Configuration
configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:

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

Syntax Description

virtual-mac { mac_address| violation drop }
no virtual-mac { violation drop }

no

 Removes the virtual MAC configuration from this APN profile.

mac_address

Specifies the media-specific access control layer address. mac_address must be specified as a 6-byte hexadecimal number with each byte separated by a colon or hyphen, for example, "AA:12:bb:34:f5:0E" or "AA-12-bb-34-f5-0E".

violation drop

Specifies SaMOG to validate if the destination MAC address in the packet received over the EoGRE tunnel matches with the configured virtual MAC, broadcast, or multicast address.

Usage Guidelines

Use this command to configure or validate the virtual MAC address for this APN profile to use as the default gateway's MAC address for the user equipment (UE).

By default, virtual MAC is not configured. In the event where no virtual MAC is configured, SaMOG creates a virtual MAC by adding fe:ff to the start of the bind address of the CGW service.
Dynamic change in the virtual MAC address will only affect new sessions. Older sessions will continue to use the old virtual MAC address until the session exists.

**Examples**

The following command configures a virtual mac with the IP address of AB:12:22:34:f5:0E for this APN profile:

```
virtual-mac AB:12:22:34:f5:0E
```
virtual-mac