



## P-GW Service Configuration Mode Commands

The P-GW (PDN Gateway) Service Configuration Mode is used to create and manage the relationship between specified services used for either GTP or PMIP network traffic.

### Command Modes

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

**configure** > **context** *context\_name* > **pgw-service** *service\_name*

Entering the above command sequence results in the following prompt:

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



### Important

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

- [associate](#), [page 3](#)
- [authorize-with-hss](#), [page 5](#)
- [dns-client](#), [page 7](#)
- [egtp](#), [page 8](#)
- [end](#), [page 11](#)
- [exit](#), [page 12](#)
- [fqdn](#), [page 13](#)
- [gtpc handle-collision upc nrupc](#), [page 15](#)
- [gx-li](#), [page 16](#)
- [map-initial-setup-auth-fail-to-gtp-cause-user-auth-fail](#), [page 17](#)
- [message-timestamp-drift](#), [page 18](#)
- [newcall](#), [page 20](#)
- [pcscf-restoration](#), [page 22](#)

- [plmn id, page 23](#)
- [session-delete-delay, page 25](#)
- [setup-timeout, page 26](#)

# associate

Associates the P-GW service with specific pre-configured services and/or policies configured in the same context.

## Product

P-GW  
SAEGW  
S-GW

## Privilege

Administrator

## Command Modes

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

**configure** > **context** *context\_name* > **pgw-service** *service\_name*

Entering the above command sequence results in the following prompt:

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

## Syntax Description

**associate** { **egtp-service** *name* [ **lma-service** *name* ] | **gtpc-load-control-profile** *name* | **gtpc-overload-control-profile** *name* | **ggsn-service** *name* | **lma-service** *name* [ **egtp-service** *name* ] | **peer-map** *map\_name* ] | **qci-qos-mapping** *name* }  
**no associate** { **egtp-service** | **lma-service** | **peer-map** | **qci-qos-mapping** }

**no**

Removes the selected association from this service.

**egtp-service** *name* [ **lma-service** *name* ] | **lma-service** *name* [ **egtp-service** *name* ]

**egtp-service** *name* [ **lma-service** *name* ]: Specifies that the P-GW service is to be associated with an existing eGTP service within this context.

*name* must be an alphanumeric string of 1 through 63 characters and be an existing eGTP service.

Configure an associated LMA service name to support handoffs between PMIPv6 and GTP. *name* must be an alphanumeric string of 1 through 63 characters and be an existing LMA service.

**lma-service** *name* [ **egtp-service** *name* ]: Specifies that the P-GW service is to be associated with an existing LMA service within this context.

*name* must be an alphanumeric string of 1 through 63 characters and be an existing LMA service.

Configure an associated eGTP service name to support handoffs between PMIPv6 and GTP. *name* must be an alphanumeric string of 1 through 63 characters and be an existing eGTP service.

**gtpc-load-control-profile *name***

Specifies that a GTPC Load Control Profile is to be associated with an existing P-GW service in this context. *name* must be an alphanumeric string from 1 to 64 characters in length.

**gtpc-overload-control-profile *name***

Specifies that a GTPC Overload Control Profile is to be associated with an existing P-GW service in this context.

*name* must be an alphanumeric string from 1 to 64 characters in length.

**ggsn-service *name***

Specifies that the P-GW service is to be associated with an existing GGSN service within this context.

*name* must be an alphanumeric string of 1 through 63 characters and be an existing GGSN service.

**peer-map *map\_name***

Specifies that the P-GW service is to be associated with an existing peer map within this context.

*map\_name* must be an alphanumeric string of 1 through 63 characters and be an existing peer map.

Refer to the *LTE Policy Configuration Mode Commands* chapter for more information on peer map creation.

**qci-qos-mapping *name***

Specifies that the P-GW service is to be associated with an existing QCI-QoS mapping configuration within this context.

*name* must be an alphanumeric string of 1 through 63 characters and be an existing QCI-QoS mapping configuration.

QCI-Qos mapping is typically configured in a AAA context. Refer to the *QCI-QoS Mapping Configuration Mode Commands* chapter for more information.

**Important**

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

**Usage Guidelines**

Use this command to associate the P-GW service with other pre-configured services and/or policies configured in the same context.

**Examples**

The following command associates this service with an eGTP service called *egtp1*:

```
associate egtp-service egtp1
```

## authorize-with-hss

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

### Product

P-GW  
SAEGW

### Privilege

Administrator

### Command Modes

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

**configure** > **context** *context\_name* > **pgw-service** *service\_name*

Entering the above command sequence results in the following prompt:

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

### Syntax Description

**authorize-with-hss** [ **egtp** [ **s2b** ] [ **s5-s8** ] [ **report-ipv6-addr** ] | **lma** [ **s6b-aaa-group** *aaa-group-name* | **report-ipv6-addr** ] | **report-ipv6-addr** ]  
{ **default** | **no** } **authorize-with-hss**

#### default

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

#### no

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

#### egtp

Enables S6b authorization for eGTP only.

#### s2b

Enables S6b authorization for eGTP S2b.

#### s5-s8

Enables S6b authorization for eGTP S5S8.

**lma**

Enables S6b authorization for LMA only.

**report-ipv6-addr**

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

**Usage Guidelines**

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

# dns-client

Specifies the DNS client context to use for sending DNS queries.

## Product

P-GW  
SAEGW

## Privilege

Administrator

## Command Modes

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

**configure** > **context** *context\_name* > **pgw-service** *service\_name*

Entering the above command sequence results in the following prompt:

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

## Syntax Description

**dns-client context** *name*  
{ **default** | **no** } **dns-client context**

### default

Returns the command to the default setting of targeting the DNS client in the context where the P-GW service resides.

### no

Disables DNS queries.

### context *name*

Specifies the name of the context where the DNS client is used for the resolution of PCSCF-FQDN received from S6b interface.

*name* must be an existing context expressed as an alphanumeric string of 1 through 79 characters.

## Usage Guidelines

Use this command to specify the context where the DNS client resides to perform P-CSCF-FQDN resolution from the S6b interface.

## Examples

The following command identifies the *egress1* context as the context where the DNS client resides:

```
dns-client context egress1
```

# egtp

Configures handling of eGTP related procedures.

## Product

P-GW  
SAEGW

## Privilege

Administrator

## Command Modes

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

**configure** > **context** *context\_name* > **pgw-service** *service\_name*

Entering the above command sequence results in the following prompt:

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

## Syntax Description

```
egtp { bitrates-rounded-down-kbps | cause-code temp-fail timeout sec retry retries |
ngnp-modify-bearer-rsp-with-apn-ambr | modify-bearer-cmd-negotiate-qos | overcharge-protection [
drop-all | transmit-all ] | sgw-restoration session-hold timeout seconds| suppress-ubr no-bitrate-change
}
default egtp { cause-code temp-fail | modify-bearer-cmd-negotiate-qos |
ngnp-modify-bearer-rsp-with-apn-ambr | overcharge-protection | sgw-restoration session-hold }
no egtp { bitrates-rounded-down-kbps | cause-code temp-fail | ngnp-modify-bearer-rsp-with-apn-ambr
| modify-bearer-cmd-negotiate-qos | overcharge-protection | sgw-restoration session-hold| suppress-ubr
no-bitrate-change }
```

### default

Resets the command to the default setting.

### no

Disables the configuration statement.

### bitrates-rounded-down-kbps

Bit rate granularity provided by different interfaces was not originally aligned in 3GPP specifications. For example, the PCRF provided bits per second on the Gx and the GTP utilized kilobits per second. Due to the conversion of bps to kbps, there were scenarios where the rounding off could have resulted in the incorrect allocation of MBR/GBR values.

When this keyword is disabled, a bitrate value sent on GTP interface will be rounded up if the conversion from bps (received from Gx) to kbps results in a fractional value. However, the enforcement of bitrate value (AMBR, MBR, GBR) values will remain the same. Once the value (in kbps) that is sent towards the Access



side, it needs to be rounded up. Also, **show subscribers pgw-only full all** will show the APN-AMBR in terms of bps.

When enabled, the previous behavior of rounded-down kpbs bitrate (AMBR, MBR, BGR) values being sent towards the Access side is enforced. In addition, **show subscribers pgw-only full all** displays in terms of kpbs.

By default, this command is configured to use rounded-up bitrate values.

#### **cause-code temp-fail timeout sec retry retries**

Enables eGTP Cause Code Handling when the P-GW receives a temporary failure response from peer (cause code 110). By default, this option is disabled.

When enabled, all transactions that were moved to pending queue because of temporary cause failure would be re-attempted after the temporary failure timer expires. After timer expiry, the P-GW informs PCRF about the transient failure. PCRF sends new Re-Auth-Request (RAR) and Create Bearer Request (CBR)/Modify Bearer Request (MBR)/Update Bearer Request (UBR) would succeed.

**timeout sec**: Specifies the time to wait (in seconds) before re-attempting the CBR/MBR/UBR.

*sec* must be an integer from 1 to 100.

**retry retries**: Specifies the maximum number of retries. The P-GW discards CBR/MBR/UBR after the maximum number of retries are exceeded.

*retries* must be an integer from 1 to 4.

#### **gnnp-modify-bearer-rsp-with-apn-ambr**

Sends Modify Bearer Response with APN-AMBR only for GnGp Handoff. By default, this option is disabled.

#### **modify-bearer-cmd-negotiate-qos**

This configuration only impacts the PGW QoS negotiation behavior when PCRF is unreachable or event trigger is not registered while handling Modify Bearer Command. By default, this configuration is disabled.

When enabled, P-GW will always enforce old QoS values authorized by the PCRF. When disabled, the P-GW will always accept new QoS values (APN-AMBR/Def-EPS-Bearer-QoS) received in Modify Bearer Command.

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

Configures overcharging protection by temporarily not charging during loss of radio coverage. By default, this configuration is disabled.

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

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

#### **sgw-restoration session-hold timeout seconds**

Enables S-GW Restoration functionality and configure session hold timeout on a P-GW service. By default, S-GW Restoration is disabled.

*seconds* must be an integer from 1 to 3600.

Default: 0 (disabled).

On S-GW failure indication, P-GW shall check if S-GW Restoration feature is enabled or not. If enabled, P-GW shall maintain all the affected sessions for session-hold timeout. After session-hold timeout, P-GW shall clear all the sessions which are not recovered yet.

#### **suppress-ubr no-bitrate-change**

Enables the P-GW to suppress the Update Bearer Request (UBR) message UBR if the bit rate is the same after the round-off.

As the bit rate is expressed in bps on Gx and kbps on GTP, the P-GW does a round-off to convert a Gx request into a GTP request. When the P-GW receives a RAR from the PCRF with minimal bit rate changes (in bps), a UBR is sent, even if the same QoS (in kbps) is already set for the bearer. The UBR suppression feature enables the P-GW to suppress such a UBR where there is no update for any of the bearer parameters.

When the UBR has multiple bearer contexts, the bearer context for which the bit rate change is less than 1 kbps after round-off is suppressed. If other parameters, such as QCI, ARP, and TFT, that might trigger an UBR are changed and there is no change in bit rates after round-off, then UBR is not suppressed. Suppression of UBR is applicable for UBR triggered by CCA-I, RAR, and Modify Bearer Command.

Default: disabled. This means that the UBRReq should be triggered even if the Gx and GTP bit-rates in kbps are same after round-off.

If the **no** option is used, it will disable this feature. That is, the UBRReq should be triggered even if the Gx and GTP bit-rates in kbps are same after round-off.

There is no separate **default** keyword for this feature. Use the **no** option to revert to the default behavior.



#### **Important**

The UBR Suppression Feature is a licensed-controlled feature. Contact your Cisco account or service representative for detailed licensing requirements.

#### **Usage Guidelines**

Use this command to configure the behavior of the P-GW/SAEGW for eGTP procedures.

#### **Examples**

The following command sets the temporary failure timer to 30 seconds and 2 retries:

**egtp cause-code temp-fail timeout 30 retry 2**

The following command configures the P-GW to accept new QoS values from the modify bearer command while the PCRF is not reachable:

**egtp modify-bearer-cmd-negotiate-qos**

The following command enables S-GW restoration functionality and configures session hold timeout on a P-GW service:

**sgw-restoration session-hold timeout seconds**

# 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.

# fqdn

Configures a Fully Qualified Domain Name for this P-GW service used in messages between the P-GW and a 3GPP AAA server over the S6b interface.

## Product

P-GW  
SAEGW

## Privilege

Administrator

## Command Modes

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

**configure** > **context** *context\_name* > **pgw-service** *service\_name*

Entering the above command sequence results in the following prompt:

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

## Syntax Description

**fqdn** **host** *domain\_name* **realm** *realm\_name*  
{ **default** | **no** } **fqdn**

### default

Returns the command to the default setting of "null".

### no

Removes the configured FQDN from this service configuration.

### host *domain\_name*

Specifies the domain name of the P-GW service.

*domain\_name* must be an alphanumeric string of 1 through 255 characters.

### realm *realm\_name*

Specifies the realm name of the P-GW service.

*realm\_name* must be an alphanumeric string of 1 through 255 characters.

## Usage Guidelines

Use this command to identify the P-GW service using an FQDN required when sending messages over the S6b interface to a 3GPP AAA server.

**Important**

In order to properly interact with other nodes in the network, the FQDN should be less than or equal to 96 alphanumeric characters.

**Topology Matching (eHRPD only)**

You may specify which P-GW you wish an HSGW interface to connect with by enabling topology matching within the FQDNs for both the HSGW service and P-GW service. Topology matching selects geographically closer nodes and reduces backhaul traffic for a specified interface.

The following optional keywords enable or disable topology matching when added to the beginning of an FQDN:

- **topon.interface\_name.**

Beginning an FQDN with **topon** initiates topology matching with available HSGWs in the network. Once this feature is enabled, the rest of the FQDN is processed from right to left until a matching regional designator is found on a corresponding HSGW FQDN.

- **topoff.interface\_name.**

By default, topology matching is disabled. If you enable topology matching for any interfaces within a node, however, all interfaces not using this feature should be designated with **topoff**.

**Examples**

The following command configures the FQDN for this P-GW service as *123abc.all.com* with a realm name of *all.com*:

```
fqdn host 123abc.all.com realm all.com
```

The following command configures this P-GW service with an FQDN that enables topology matching:

```
fqdn host topon.interface_name.pgww01.bos.ma.node.epc .mnc<value>.mcc<value>.3gppnetwork.org  
realm node.epc.mnc.mcc.3gppnetwork.org
```

**Important**

The associated HSGW service must have a corresponding FQDN similar to the following:

```
topon.interface_name.hsgw01.bos.ma.node.epc.mncvalue.mccvalue.3gppnetwork.org
```

# gtpc handle-collision upc nrupc

This command helps in enabling or disabling collision handling between SGSN initiated UPC and NRUPC request.

## Product

P-GW

## Privilege

Security Administrator, Administrator

## Command Modes

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

**configure** > **context** *context\_name* > **pgw-service** *service\_name*

Entering the above command sequence results in the following prompt:

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

## Syntax Description

[ **no** | **default** ] **gtpc handle-collision upc nrupc**

### **no**

Disables collision handling between SGSN initiated UPC and NRUPC request.

### **default**

Sets default collision handling behavior between SGSN initiated UPC and NRUPC request. By default, collision handling is enabled.

### **handle-collision upc nrupc**

Enables/Disables collision handling between SGSN initiated UPC and network requested UPC. By default, collision handling is enabled.

## Usage Guidelines

This command is used to enable or disable collision handling between SGSN initiated UPC and NRUPC request.

## Examples

The following example disables collision handling between SGSN initiated UPC and NRUPC request.

```
no gtpc handle-collision upc nrupc
```

## gx-li

Refer to the *Lawful Intercept Configuration Guide* for a description of this command.



# map-initial-setup-auth-fail-to-gtp-cause-user-auth-fail

Maps Gx cause code (5xxx) to access side GTP cause code Auth-failure(92) in Create Session Response message.

## Product

P-GW  
SAEGW

## Privilege

P-GW  
SAEGW

## Command Modes

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

**configure** > **context** *context\_name* > **pgw-service** *service\_name*

Entering the above command sequence results in the following prompt:

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

## Syntax Description

[ default | no ] **map-initial-setup-auth-fail-to-gtp-cause-user-auth-fail**

### default

Maps Gx cause code (5xxx) to access side GTP cause code No-Resource(73) in Create Session Response message.

### no

Maps Gx cause code (5xxx) to access side GTP cause code No-Resource(73) in Create Session Response message.

## Usage Guidelines

When Create Session Request message arrives at P-GW, CCR-I is sent to PCRF and PCRF rejects calls with 5xxx cause code in CCA-I. In this case, Create Session Response is sent with failure indicated by GTP cause code. Use this command to control which GTP cause code is sent, "No Resources Available" or "User Authentication Failed", in Create Session Response message for this scenario. By default, "No Resources Available" is sent for this case; however, enabling this command sends "User Authentication Failed" cause code in Create Session Response.

## Examples

The following command maps Gx cause code (5xxx) to access side GTP cause code Auth-failure(92) in Create Session Response message:

**map-initial-setup-auth-fail-to-gtp-cause-user-auth-fail**

# message-timestamp-drift

Allows drift time configuration to take care of NTP drift issues.

## Product

P-GW  
SAEGW

## Privilege

Administrator

## Command Modes

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

**configure** > **context** *context\_name* > **pgw-service** *service\_name*

Entering the above command sequence results in the following prompt:

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

## Syntax Description

**message-timestamp-drift** *time\_in\_seconds*  
{ **default** | **no** } **message-timestamp-drift**

### default

Sets drift time to 180 seconds.

If P-GW detects drift less than 180 seconds, it will check for condition "MWT + ReceivedTimeStamp (time from MME) > CurrentTimeStampAtPGW", and based on that P-GW will reject the call. If this condition is not met, it will transparently forward MWT and timestamp to AAA/Gx/Gy interfaces.

### no

Disables message timestamp drift. MWT and received timestamp will not be passed on to all AAA/Gx/Gy interfaces.

### message-timestamp-drift *time\_in\_seconds*

Configures the drift time from the message timestamp, in seconds, up to which P-GW will consider processing the message timestamp and max-wait-time (MWT) IEs.

If the create-time from MME is off from the currenttime by configured-drift-duration, then this could lead to a high NTP drift and session uniqueness falls back to using currenttime toward Diameter servers.

If the timestamp received in CSReq is significantly off (more than configured drift), then P-GW will not take action based on MWT and received timestamp and will transparently pass it to all AAA/Gx/Gy interfaces.

When received drift is less than configured limit, P-GW will reject the call if "MWT + ReceivedTimeStamp > CurrentTimeStampAtPGW" condition is met. Otherwise, P-GW will forward the timestamp and MWT to AAA/Gx/Gy interfaces.

*time\_in\_seconds* must be an integer from 0 to 1000.

Default: 180

### Usage Guidelines

When the MME is reselected by the UE or when the MME reselects a different P-GW during timeout scenarios, it is possible that the old PDN connection request is still being processed in the network and the session created by the new PDN connection request is overwritten by the stale procedure.

IEs TimeStamp and MWT (MaxWaitTime) have been added in CSReq and forwarded on S6b/Gx/Gy interfaces in order to maintain session uniqueness at P-GW.



### Important

Drift time configuration under P-GW service shall be used by the associated LMA service.

### Example Scenario

In the following scenario, stale session won't be present on P-GW.

The P-GW is still processing the session creation but the S-GW times out due to timer configurations and notifies the MME with Create Session Failure (Cause #100: Remote Peer Not Responding). MME reselects an alternate P-GW in this case, but the original P-GW still continues to process the session. In certain scenarios, the original P-GW can overwrite the Gx session on the PCRF that is created by the newly selected P-GW. In this case, the new P-GW session is the valid session and original P-GW session is invalid as far as the UE, MME, and S-GW are concerned. The same can occur with the AAA session as well based on timing. This results in PCRF having invalid session information and the user plane works fine anchored on the second P-GW, but the Rx and Gx signaling fails as this terminates via original P-GW.

This results in VoLTE calls failing after SIP signaling between UE and P-CSCF.

To solve the problem, TimeStamp and MWT IE have been incorporated to be transmitted from MME and shared across the network nodes.

### Examples

The following command sets drift time to 200 seconds.

**message-timestamp-drift 200**

# newcall

Configures the P-GW to accept or reject requests for a static IP address if the address is already in use by another session.

## Product

P-GW  
SAEGW  
SaMOG

## Privilege

Administrator

## Command Modes

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

**configure** > **context** *context\_name* > **pgw-service** *service\_name*

Entering the above command sequence results in the following prompt:

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

## Syntax Description

**newcall** { **duplicate-subscriber-requested-address** | **duplicate-subscriber-requested-v6-address** } { **accept** | **reject** }

**no newcall** { **duplicate-subscriber-requested-address** | **duplicate-subscriber-requested-v6-address** }

**no**

Returns the command to the default setting of "reject".

**duplicate-subscriber-requested-address**

Configures how duplicate sessions with same IPv4 address request are handled.

**duplicate-subscriber-requested-v6-address**

Configures how duplicate sessions with same IPv6 address request are handled.

**accept** | **reject**

Default: **reject**

**accept**: Specifies that the old session with the requested address will be ended to accept the new session with the same address.

**reject**: Specifies that the new session requesting the same address will be rejected.

### Usage Guidelines

Use this command to configure the behavior of the P-GW service when receiving requests for static IP or IPv6 address already in use by other sessions.



#### Important

This command is only applicable to sessions using services supporting duplicate address abort. These services include HA, GGSN, and P-GW.

### Examples

The following command allows for the acceptance of requests for static IP addresses already in use by other sessions:

**newcall duplicate-subscriber-requested-address accept**

# pcscf-restoration

Configures the mechanism to support P-CSCF restoration when a failure is detected.

## Product

P-GW  
SAEGW

## Privilege

Administrator, Security Administrator

## Command Modes

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

**configure** > **context** *context\_name* > **pgw-service** *service\_name*

Entering the above command sequence results in the following prompt:

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

## Syntax Description

**pcscf-restoration { hss-solution | custom-hss-solution }**  
**default pcscf-restoration**

### **hss-solution**

Enables the Release 12-based HSS solution for P-CSCF restoration.

### **custom-hss-solution**

Enables private extension-based HSS solution for P-CSCF restoration.

This is the default setting.

### **default**

Returns pcscf-restoration to the default setting (**custom-hss-solution**).

## Usage Guidelines

Use this command to enable/disable the standards-based mechanism for P-CSCF failure detection. This command enables operators to ensure a failed P-CSCF address is not provided to the IMS client. Prior to StarOS release 18.2, P-CSCF restoration was supported by using the Private Extn IE. In StarOS releases 18.2 and later, the failure detection mechanism can be configured as standards-based. By default this feature is disabled; in which case the Private Extn mechanism will be used for P-CSCF restoration.

## Examples

This example configures P-CSCF restoration to **custom-hss-solution**:

```
pcscf-restoration custom-hss-solution
```

# plmn id

Configures Public Land Mobile Network (PLMN) identifiers used to determine if a mobile station is visiting, roaming, or belongs to a network. Up to 512 PLMN IDs can be configured for each P-GW service.

## Product

P-GW  
SAEGW

## Privilege

Administrator

## Command Modes

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

**configure** > **context** *context\_name* > **pgw-service** *service\_name*

Entering the above command sequence results in the following prompt:

[*context\_name*]*host\_name* (config-pgw-service) #

## Syntax Description

**plmn id** *mcc mcc\_value* [ **mnc** *mnc\_value* ] [ **primary** ]  
**no plmn id** *mcc mcc\_value* [ **mnc** *mnc\_value* ]

**no**

Removes a previously configured PLMN identifier for the P-GW service.

**mcc** *mcc\_value*

Specifies the mobile country code (MCC) portion of the PLMN identifier.

*mcc\_value* is the PLMN MCC identifier and must be an integer from 100 through 999.

**mnc** *mnc\_value*

Specifies the mobile network code (MNC) portion of the PLMN identifier.

*mnc\_value* is the PLMN MNC identifier and can be configured to a 2- or 3-digit integer from 00 through 999.

**primary**

When multiple PLMN IDs are configured, the **primary** keyword can be used to designate one of the PLMN IDs to be used for the AAA attribute.

**Usage Guidelines**

The PLMN identifier is used to aid the P-GW service in the determination of whether or not a mobile station is visiting, roaming, or home. Multiple P-GW services can be configured with the same PLMN identifier. Up to 512 PLMN IDs can be configured for each P-GW Service.

**Important**

The number of supported PLMN IDs was increased from 5 to 512 in StarOS Release 17.1. In addition, the MNC portion of the PLMN ID became optional.

If the MNC portion of a PLMN ID is not specified, home PLMN qualification will be done based solely on the MCC value and the MNC portion will be ignored for these particular MCCs.

**Examples**

The following command configures the PLMN identifier with an MCC of 462 and MNC of 02:

```
plmn id mcc 462 mnc 02
```



# session-delete-delay

Configures a delay in terminating a session.

## Product

P-GW  
SAEGW

## Privilege

Administrator

## Command Modes

Exec > Global Configuration > Context Configuration > P-GW Service Configuration  
**configure > context** *context\_name* > **pgw-service** *service\_name*  
Entering the above command sequence results in the following prompt:  
*[context\_name]host\_name* (config-pgw-service) #

## Syntax Description

**session-delete-delay timeout** [ *msec* ]  
{ **default** | **no** } **session-delete-delay timeout**

### default

Resets the command to the default setting of 10000 milliseconds.

### no

Disables the feature.

### timeout *msec*

Default: 10000

Specifies the time to retain the session (in milliseconds) before terminating it.

*msec* must be an integer from 1000 to 60000.

## Usage Guidelines

Use this command to set a delay to provide session continuity in break-before-make scenarios.

## Examples

The following command sets the session delete delay to the default setting of 10,000 milliseconds:  
**session-delete-delay timeout**

# setup-timeout

Configures the maximum amount of time the P-GW service takes for creating a session.

## Product

P-GW

## Privilege

Security Administrator, Administrator

## Command Modes

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

**configure** > **context** *context\_name* > **pgw-service** *service\_name*

Entering the above command sequence results in the following prompt:

*[context\_name]host\_name(config-pgw-service)#*

## Syntax Description

**setup-timeout** *setup\_time*  
**default setup-timeout**

### default

Configures the default guard timer value for session creation.

### setup-time

Default: 60

Specifies the maximum amount of time taken by P-GW for service creation.

*setup\_time* is measured in seconds and can be configured to an integer from 1 through 120.

## Usage Guidelines

Use this command to limit the amount of time allowed for creating a session. If a "Create Session Request" is received and the setup-timeout is configured, the timer starts with the configured value. If the setup timeout is not configured, the timer starts with the default value of 60 seconds.

## Examples

The following command allows a maximum of 120 seconds for creating a session:

**setup-timeout 120**