ERICSSON

Policy Control Configuration

OPERATION DIRECTIONS

70/1543-AXB 250 10/4-V3 Uen GH

Contents

1 Introduction

This document describes the configuration of the Gx+ Policy and Charging Control (PCC) feature for Service-Aware Charging and Control (SACC) in the EPG for GSM, WCDMA, LTE, trusted non-3GPP network, and untrusted non-3GPP network.

1.1 Scope

This document covers the following issues:

— How to enable the Gx+ PCC feature.

— How to configure the Gx+ PCC feature, including charging rule provisioning over the Gx+ interface and locally configured policies.

— How to configure parameters related to PCC sessions.

— How to configure the handling of unauthorized payload.

For an overview of Gx+ PCC, see Policy Control. For an overview of SACC, see SACC Overview. For an overview of the Gx+ Interface, see Gx+ Interface Description.

1.2 Target Groups

This document is intended for personnel configuring the EPG. The document is written with the assumption that the reader has basic knowledge of data communication and telecommunication.

2 Prerequisites

Before configuring the Gx+ PCC feature, ensure that the following prerequisites are met:

— The Gx+ PCC license must be activated. Optional licensed features in the EPG are disabled by default. To employ these features in the GGSN or PGW, licenses must be purchased from Ericsson. For information on how to purchase licenses and enable licensed features, see Software License Management or contact the local Ericsson support.

— An Access Point Name (APN) must be configured. Refer to APN Configuration for more information.

— SACC must be enabled for the APN with the associated user category, rule space, and service set. Refer to SACC Configuration for more information.

— If Gx+ PCC over the Gx+ interface is to be used, a Diameter Application System (DAS) with application identifier (ID) **pcc** or **10415:16777238** (3GPP:PCC) must be configured in the GGSN and PGW. Refer to Diameter Configuration for more information.

3 Configuring Gx+ PCC

The following sections describe configurable parameters related to the Gx+ PCC feature.

3.1 Enabling Policy Control

By default, a rule space is only used to determine the charging parameters for different services. To enable access control, QoS control, and other policy control functions, include the following statement:

```
Ericsson(config)# epg pgw rule-space <rule-space-name>
   enable-access-control-rules
```

Policy control can be enabled or disabled in runtime. The change takes effect immediately.

3.2 Configuring ACGs

To add an ACR or a consecutive range of ACRs separated by a - to an ACG for a rule space, include the following statement:

```
Ericsson(config)# epg pgw rule-space <rule-space-name
> access-control-group <acg-id>
   access-control-rule (<acr-id> | <acr-id>-<acr-id>)
```

The maximum number of ACGs that can be configured per rule space is 1000.

ACGs can be added, removed, or modified in runtime. The change takes effect immediately.

To configure the relative precedence for an ACG, include the following statement:

```
Ericsson(config)# epg pgw rule-space <rule-space-name
> access-control-group <acg-id>
   precedence <value>
```

The precedence value must be an integer between 0 and 2^{32}-1.

3.3 Configuring Aliases for ACRs and ACGs

By default, the EPG accepts only numerical PCC rule names and PCC rule base names. A PCC rule maps to exactly one ACR, and a PCC rule base maps to exactly one ACG.

Optionally, the EPG can be configured to accept textual PCC rule names and PCC rule base names. A textual PCC rule name can be mapped to one or several ACRs, and a textual PCC rule base name can be mapped to one or several ACGs.

To configure a textual PCC rule name as the ACR alias for a rule space, include the following statement:

```
Ericsson(config)# epg pgw rule-space <rule-space-name
> access-control-rule <acr-id>
   alias <rule-name>
```

Note: An alias cannot be configured for a range of ACRs.

To configure a textual PCC rule base name as the ACG alias for a rule space, include the following statement:

```
Ericsson(config)# epg pgw rule-space <rule-space-name
> access-control-group <acg-id>
   alias <rule-base-name>
```

An alias is configured using a maximum 63 American Standard Code for Information Interchange (ASCII) characters. If an alias contains any characters other than the following ones, the PCC rule name or the PCC rule base name must be enclosed in double quotation mark ("). An alias cannot be numerical.

— Uppercase characters (A–Z)

— Lowercase characters (a–z)

— Base 10 digits (0–9)

— Hyphen (-)

— Underscore (_)

An alias can be added, removed, or modified in runtime. The change takes effect at the next installation or removal of the named PCC rule or PCC rule base.

3.4 Configuring Always Allowed ACRs

To add an ACR or a consecutive range of ACRs separated by a hyphen (-) as a permanently allowed service for a rule space, include the following statement:

```
Ericsson(config)# epg pgw rule-space <rule-space-name>
   always-allowed-access-control-rule (<acr-id> |
<acr-id>-<acr-id>)
```

Note: If an ACR is included among the always allowed ACRs, including the ACR in the Local Policy Table (LPT) has no effect, and the ACR remains always allowed.

3.5 Configuring Always Denied ACRs

To add an ACR or a consecutive range of ACRs separated by a hyphen (-) as an explicitly denied service for a rule space, include the following statement:

```
Ericsson(config)# epg pgw rule-space <rule-space-name>
    always-denied-access-control-rule (<acr-id> |
<acr-id>-<acr-id>)
```

Always denied ACRs can be added or removed in runtime. The change takes effect immediately.

3.6 Configuring Local Policies

Locally configured policies provide access control locally in the EPG when no PCRF is used. Provisioning of predefined ACRs and ACGs is performed automatically based on configuration of a Local Policy Table (LPT) and status of the user session. The LPT can be used as the primary mechanism for access control, or as a fallback mechanism in case access control over Gx fails.

Note: Access control must be enabled for the rule space. For more information, see Section 3.1 on page 2.

3.6.1 Configuring an LPT

An LPT contains rules for provisioning of authorized or unauthorized ACRs or ACGs, optionally based on time of day, roaming class, and QoS type for user sessions.

To configure an LPT to provision an ACR for a rule space, include the following statement:

```
Ericsson(config)# epg pgw rule-space <rule-space-nam
e> local-policy-control
   (all-time  | activation-time <time>)
      (default-roaming-class  | roaming-class <id>)
         (default-quality-of-service  | quality-of-service <qos-type>)
            access-control-rule <acr-id>
               authorization-code <code>
```

To configure an LPT to provision an ACG for a rule space, include the following statement:

```
Ericsson(config)# epg pgw rule-space <rule-space-nam
e> local-policy-control
   (all-time | activation-time <time>)
      (default-roaming-class | roaming-class <id>)
         (default-quality-of-service | quality-of-service <qos-type>)
            access-control-group <acg-id>
               authorization-code <code>
```

The LPT can be modified in runtime. For an active user session, the change takes effect at next update.

Up to 12 activation times can be configured in the format `hh:mm`. The activation time range is `00:00` to 23:59, with a resolution of one minute. The time difference between two activation times must be at least one hour. If no activation times are configured, it is mandatory to configure a set of data called `all-time` which is always valid, independently of time.

For each activation time or for the `all-time` data set, up to 24 roaming classes can be defined. It is also mandatory to configure a set of data called `default-roaming-class`. The default roaming class is used if no entry exists for the roaming class of the user session.

For each roaming class or for the `default-roaming-class`, up to six Quality of Service (QoS) types can be defined:

- `background`
- `conversational`
- `streaming`
- `interactive–1`
- `interactive–2`
- `interactive–3`

It is also mandatory to configure a set of data called `default-quality-of-service`. The default QoS is used if no entry exists for the QoS of the bearer.

For each defined QoS type or for the `default-quality-of-service`, a list of ACRs or ACGs can be configured. For each of these ACRs or ACGs, the following authorization states can be defined:

- `authorized`
- `denied-calendar-time`
- `denied-roaming`
- `denied-quality-of-service`
- `denied-blacklisted`

- denied-terminal
- denied-user—defined-reason-1
- denied-user—defined-reason-2
- denied-user—defined-reason-3
- denied-user—defined-reason-4
- denied-user—defined-reason-5
- denied-unknown

Note: ACRs and ACGs not defined for the current activation time are considered unsubscribed, regardless of their previous authorization state.

3.7 Enabling Network Location

The EPG can be configured to support Network Location (NetLoc) if the following conditions are satisfied:

- IMS-Based Telephony - MMTel is activated.
- NetLoc is enabled for a Gx profile.

To activate IMS-Based Telephony - MMTel, include the following statement:

```
Ericsson(config)# epg pgw feature-activation
   ims-based-telephony-mmtel
```

To enable NetLoc for a Gx profile, include the following statement:

```
Ericsson(config)# epg pgw apn <apn-name> service-based-charging
policy-control dynamic gx-profile <profile-id>
   netloc
```

3.7.1 Enabling NetLoc for Untrusted WLAN

To enable NetLoc for a Gx profile for untrusted WLAN, include the following statement:

```
Ericsson(config)# epg pgw apn <apn-name> service-based-charging
policy-control dynamic gx-profile <profile-id>
   netlocuwan
```

3.8 Enabling PCRF-Based P-CSCF Restoration

To enable PCRF-based P-CSCF restoration for an APN, include the following statement:

```
Ericsson(config)# epg pgw apn <apn-name> service-based-charging
policy-control dynamic gx-profile <profile-id>
   p-cscf-restoration-enhancement
```

3.9 Enabling Presence Reporting Area

The EPG can be configured to support Presence Reporting Area (PRA).

3.9.1 Activating Presence Reporting Area

To activate the PRA, include the following statement:

```
Ericsson(config)# epg node feature-activation
   presence-reporting-area
```

3.9.2 Deactivating Presence Reporting Area

To deactivate the PRA, include the following statement:

```
Ericsson(config)# no epg node feature-activation presence-reporting-area
```

4 Enabling the Gx+ Interface

To enable the Gx+ interface in the GGSN or PGW, do the following:

— Configure a dynamic Gx profile, see Section 4.1 on page 7.

— Optionally, configure the 3GPP Gx PCC release to be used, see Section 4.2 on page 8.

— Associate the dynamic Gx profile with a user category, see Section 4.3 on page 8.

4.1 Configuring a Dynamic Gx Profile

Associating a DAS with the dynamic Gx profile is mandatory. To associate a PCC Gx DAS with the dynamic Gx profile, a DAS with application identifier (ID) **`pcc`** or **`10415:16777238`** (3GPP:PCC) must be configured in the GGSN and PGW, see Diameter Configuration.

To associate a PCC Gx DAS with the dynamic Gx profile, a DAS with application identifier (ID) **`pcc`** or **`10415:16777238`** (3GPP:PCC) must be previously configured in the GGSN and PGW, see Diameter Configuration.

Configure a dynamic Gx profile and associate a DAS with it by including the following statement:

```
Ericsson(config)# epg pgw apn <apn-name> service-based-charging
policy-control dynamic gx-profile <profile-id>
   diameter-application-system <das-id>
```

A dynamic Gx profile can be configured in runtime. The maximum number of dynamic Gx profiles that can be configured per APN is 32.

4.2 Configuring 3GPP Gx PCC Release

For each Gx policy control profile, it is possible to configure which PCC release to use. If PCC release 7 or 8 is configured, that release is used; if release 9 is configured, the release used is negotiated with the PCRF at session initialization. For more information about negotiation of supported features, see Gx+ Interface Description.

Note: Configuring PCC release 7 disables negotiation of supported features.

PCC release 7 is not valid for PGW-enabled APNs.

Configure the PCC release used for a Gx profile by including the `pcc-release` statement. It is not possible to perform this change during runtime. If `pcc-release` is not configured, the release used is negotiated with the PCRF.

```
Ericsson(config)# epg pgw apn <apn-name> service-based-charging
policy-control dynamic gx-profile <profile-id>
   pcc-release (7 | 8 | 9)
```

To set this parameter, a PCC Gx DAS must be associated with the Gx policy control profile, as described in Section 4.1 on page 7.

4.3 Associating a Dynamic Gx Profile with a User Category

Associate a dynamic Gx profile with the default user category by including the following statement:

```
Ericsson(config)# epg pgw apn <apn-name> user-category default
   policy-control-dynamic-gx-profile <profile-id>
```

Associate a dynamic Gx profile with a specific user category by including the following statement:

```
Ericsson(config)# epg pgw apn <apn-name> user-categor
y category <user-category-id>
   policy-control-dynamic-gx-profile <profile-id>
```

For instructions on configuring a user category, refer to SACC Configuration.

5 Configuring Gx+ PCC Sessions

The following sections describe configurable parameters related to PCC sessions.

5.1 Disable Proprietary Gx+ Extensions

It is possible to disable all proprietary Gx+ extensions for Gx and only use 3GPP Gx standard.

Disable Gx+ capability negotiation by including the following statement:

```
Ericsson(config)# epg pgw apn <apn-name> service-based-charging
policy-control dynamic gx-profile <profile-id>
   disable-gx-extensions
```

5.2 Enabling Rule Space Negotiation

Enable rule space negotiation over the Gx+ interface by including the following statement:

```
Ericsson(config)# epg pgw apn <apn-name> service-based-charging
policy-control dynamic gx-profile <profile-id>
   rule-space-negotiation
```

5.3 Configuring RAT Type to HRPD over Gx

Configure RAT type to HRPD in Gx interface for eHRPD access by including the following statement:

```
Ericsson(config)# epg pgw apn <apn-name> service-based-charging
policy-control dynamic gx-profile <profile-id>
   rat-type-for-ehrpd (hrpd | ehrpd)
```

Note: The default value is `ehrpd`.

5.4 Configuring Subscription IDs

Configure different subscription identifiers that are included in `Credit-Control-Request` (CCR) messages sent to the PCRF according to different Rat- Types by including the following statement:

```
Ericsson(config)# epg pgw apn <apn-name> service-based-charging
policy-control dynamic gx-profile <profile-id>
   subscription-id (msisdn | nai | imsi)
    rat-type (eutran|wlan|ehrpd|hrpd|geran|utran|gan|hspa|nb-iot)
      subscription-id (msisdn | nai | imsi)
```

When subscription-id under the specific rat-type is configured, the subscription-id which is configured directly under the Gx profile for this rat-type is overwritten.

The following subscription IDs can be used over the Gx+ interface:

— msisdn

— nai

— imsi

Note: If subscription-id is not configured under this rat-type, the default value is msisdn.

The following RAT types can be used over the Gx+ interface:

— eutran

— wlan

— ehrpd

— hrpd

— geran

— utran

— gan

— hspa

— nb-iot

5.5 Configuring the User-Equipment-Info AVP in CCR Messages

The EPG can be configured to include the User-Equipment-Info AVP in a CCR Update message to the PCRF during the handover between LTE and untrusted Wi-Fi. To include the AVP, include the following statement:

```
Ericsson(config)# epg pgw apn <apn-name> service-based-charging
policy-control dynamic gx-profile <profile-id>)
   user-equipment-info-in-ccru
```

To configure the PGW not to include the User-Equipment-Info AVP in a CCR message sent to the PCRF for CDMA access, include the following statement:

```
Ericsson(config)# epg pgw apn <apn-name> service-based-charging
policy-control dynamic gx-profile <profile-id>
   no-cdma-user-equipment-info
```

5.6 Configuring the Called-Station-Id AVP Within the PS-Information AVP

To configure which APN name to include in the `Called-Station-Id` AVP, include the following statement:

```
Ericsson(config)# epg pgw apn <apn-name> service-based-charging
policy-control dynamic gx-profile <profile-id>
   select-apn (used | logical | requested)
```

The `select-apn` configuration has three options. Page 11 describes how the selected option determines which APN name is included in the `Called-Station-Id` AVP.

Table 1 The APN Name in Called-Station-Id AVP

Option	**The APN Name in `Called-Station-Id` AVP**
used	Same as the configured APN name for the selected APN. The GGSN and PGW apply the used option by default.
logical	Same as the configured APN name for the requested APN(1).
requested	Same as the requested APN name in the GTP message, if the APN was changed by Radius Assisted Selection of APN (RAAS) or the PCRF-Assisted APN Selection. Same as the configured APN name for the requested APN(1), if the APN was not changed by RAAS or the PCRF-Assisted APN Selection.

(1) The requested APN means the APN that was received over the Gn/Gp, S5/S8, GTP-based S2a, GTP-based S2b, or PMIPv6-based S2a interface.

5.7 Configuring Inclusion of the Called-Station-Id AVP in CCR Messages

The EPG can be configured to send the APN selected for the Gi or SGi interface to the PCRF.

To configure the EPG to include the `Called-Station-Id` AVP in `CCR-U` and `CCR-T` messages sent to the PCRF, include the following statement:

```
Ericsson(config)# epg pgw apn <apn-name> service-based-charging
policy-control dynamic gx-profile <profile-id>
   always-include-called-station-id
```

Note: By default, the `Called-Station-Id` AVP is only included in the `CCR-I` message sent to the PCRF.

5.8 Configuring User-Equipment-Info-Type AVP

The EPG supports the value settings for the `User-Equipment-Info-Type` listed in Table 2 according to 3GPP TS 29.212.

Table 2 Supported User-Equipment-Info-Type AVP Value

User-Equipment-Info-Type	Value
IMEISV(1)	0
MAC(2)	1
ESN(3)	4
MEID(3)	5

(1) This type is supported for all access.
(2) This type is supported for untrusted Wi-Fi access only. For untrusted Wi-Fi access, whether to use IMEISV or MAC is decided by configuration.
(3) This type is supported for CDMA access only. For CDMA access, refer to PMIPv6-Based S2a Interface Description for which type is used.

To configure the values of User-Equipment-Info-Type for untrusted Wi-Fi access, include the following statement:

```
Ericsson(config)# epg pgw apn <apn-name> service-based-charging
policy-control dynamic gx-profile <profile-id>
   u-wlan-user-equipment-info (imeisv | mac)
```

Note: The default value is `imeisv`.

5.9 Configuring Always Inclusion

This section describes the configuration of PGW to always include the following AVPs:

— `3GPP-User-Location-Info` AVP

— `3GPP-SGSN-MCC-MNC` AVP

— `3GPP-MS-TimeZone` AVP

— `Subscription-Id` AVP

5.9.1 Configuring 3GPP-User-Location-Info AVP

To include `3GPP-User-Location-Info` AVP in all `CCR` messages, include the following statement:

```
Ericsson(config)# epg pgw apn <apn-name> service-based-charging
policy-control dynamic gx-profile <profile-id>
   always-include-user-location-info
```

Note: Configuring 3GPP-User-Location-Info AVP is only applicable for 3GPP access.

5.9.2 Configuring 3GPP-SGSN-MCC-MNC AVP

To include 3GPP-SGSN-MCC-MNC AVP in all CCR messages, include the following statement:

```
Ericsson(config)# epg pgw apn <apn-name> service-based-charging
policy-control dynamic gx-profile <profile-id>
   always-include-plmn
```

5.9.3 Configuring 3GPP-MS-TimeZone AVP

To include 3GPP-MS-TimeZone AVP in all CCR messages, include the following statement:

```
Ericsson(config)# epg pgw apn <apn-name> service-based-charging
policy-control dynamic gx-profile <profile-id>
   always-include-ms-timezone
```

Note: Configuring 3GPP-MS-TimeZone AVP is only applicable for 3GPP access.

5.9.4 Configuring Subscription-Id AVP

To include the Subscription-Id AVP in all CCR messages, include the following statement:

```
Ericsson(config)# epg pgw apn <apn-name> service-based-charging
policy-control dynamic gx-profile <profile-id>
   always-include-subscription-id
```

The subscription IDs are included only in the CCR Initial messages if the always-include-subscription-id statement is not configured.

5.9.5 Configuring RAT-Type AVP

To include RAT-Type AVP in all CCR messages, include the following statement:

```
Ericsson(config)# epg pgw apn <apn-name> service-based-charging
policy-control dynamic gx-profile <profile-id>
   always-include-rat-type
```

Note: The EPG supports including the RAT-Type AVP in all CCR messages for Gx PCC 8 and later releases.

5.10 Configuring IP-CAN-Type for CDMA

To configure IP-CAN-Type to 3GPP2 when it is CDMA access, that is eHRPD and HRPD, include the following statement:

```
Ericsson(config)# epg pgw apn <apn-name> service-based-charging
policy-control dynamic gx-profile <profile-id>
   ip-can-type-for-cdma (non-3gpp-eps | 3gpp2)
```

If IP-CAN-Type is not configured, the default value is non-3gpp-eps.

5.11 Configuring User-Equipment-Info-Value AVP

The default encoding of User-Equipment-Info-Value AVP is according to 3GPP Release 9, Unicode Transformation Format-8 (UTF-8).

The following statement makes it possible to configure the use of 3GPP release 6 (Binary-Coded Decimal) encoding of the User-Equipment-Info-Value AVP:

```
Ericsson(config)# epg pgw apn <apn-name> service-based-charging
policy-control dynamic gx-profile <profile-id>
   pcc-imei-encoding 3gpp-rel6
```

5.12 Excluding the 3GPP2-BSID AVP in CCR Messages

To configure the PGW not to include the 3GPP2-BSID AVP in a CCR message sent to the PCRF, include the following statement:

```
Ericsson(config)# epg pgw apn <apn-name> service-based-charging
policy-control dynamic gx-profile <profile-id>
   no-cdma-bsid
```

5.13 Enabling CSG Reporting over Gx+

To enable CSG Reporting over Gx+, include the following statement:

```
Ericsson(config)# epg pgw apn <apn-name> service-based-charging
policy-control dynamic gx-profile <profile-id>
   csg-reporting
```

For more information on CSG, refer to Session Management.

5.14 Requiring Explicit Subscription of QoS Change Event Triggers

By default, the PGW always activates the QOS_CHANGE and DEFAULT_EPS_BEARER_QOS_CHANGE event triggers.

To configure the PGW to only activate the QOS_CHANGE and DEFAULT_EPS_BEARER_QOS_CHANGE event triggers if the PCRF subscribes to the event triggers, include the following statement:

```
Ericsson(config)# epg pgw apn <apn-name> service-based-charging
policy-control dynamic gx-profile <profile-id>)
   qos-change-provisioning-required
```

5.15 Disabling APN-AMBR Mediation

The PGW can be configured not to perform APN-AMBR mediation upon receiving an SGSN initiated QoS update by including the following statement:

```
Ericsson(config)# epg pgw apn <apn-name> service-based-charging
policy-control dynamic gx-profile <profile-id>
   disable-apn-ambr-mediation
```

Note: It is not possible to disable APN-AMBR mediation when dedicated bearers are enabled, as described in APN Configuration.

5.16 Allowing Dynamic PCC Rules with Missing Bit Rates

By default, the EPG rejects the installation of dynamic PCC rules that do not include all associated bit rates, with the rule failure code `UNSUCCESSFUL_QOS_VALIDATION`. The EPG can be configured to allow the installation of dynamic PCC rules that do not specify all associated bit rates; any missing bit rate is set to `0` kbps.

To enable support for dynamic PCC rules with missing bit rates, use the following command:

```
Ericsson(config)# epg pgw apn <apn-name> service-based-charging
policy-control dynamic gx-profile <profile-id>)
   allow-rules-with-missing-bitrates
```

This only applies when installing new PCC rules. If an update is missing one or more bit rates, the currently used values remain unchanged.

This only applies to dynamic PCC rules that specify a QCI. If no QCI is specified (in which case the rule is installed on the default bearer), the absence of bit rates means that no bit rate policing is done.

5.17 Configuring Usage Monitoring over Gx

Usage Monitoring over Gx is an optional licensed feature that is disabled by default. For information on how to manage licensed features, see Section 2 on page 1.

The Usage Monitoring over Gx feature requires that both the GGSN and the PCRF support Gx Release 9.

Note: Do not configure `pcc-release (7 | 8)` for the Gx profile. For more information, see Section 4.2 on page 8.

5.17.1 Activating Usage Monitoring over Gx

The following configurations activate Usage Monitoring over Gx.

Activate the Usage Monitoring over Gx feature by issuing the following command:
```
Ericsson(config)# epg pgw feature-activation
   usage-monitoring
```
The following example shows how usage monitoring can be configured:

```
epg pgw feature-activation usage-monitoring
epg pgw apn apn_1
 service-based-charging control-context 3gpp
 service-based-charging policy-control dynamic gx-profile gx_profile_1
  diameter-application-system       das_1
 !
epg pgw diameter diameter-application-system das_1
 application-id    pcc
!
```

Example 1 Example Configuration for Usage Monitoring over Gx

5.17.2 Configuring Usage Monitoring at All Interim Updates

Usage monitoring over Gx can also report usage at all interim updates by including the extended-usage-monitoring statement.

Enable usage reporting at all interim updates by including the following statement:
```
Ericsson(config)# epg pgw apn <apn-name> service-based-charging
policy-control dynamic gx-profile <profile-id>
   extended-usage-monitoring
```

5.17.3 Associating an ACR with a Monitoring Key

To configure the mapping between a monitoring key and an ACR or a consecutive range of ACRs separated by -, include the following statement:
```
Ericsson(config)# epg pgw rule-space <rule-space-nam
e> monitoring-key map <mk-id>
   access-control-rule (<acr-id> | <acr-id>-<acr-id>)
```

A monitoring key can be mapped to several ACRs, but an ACR can only be mapped to one monitoring key.

5.17.4 Associating an ACG with a Monitoring Key

To configure the mapping between a monitoring key and an ACG, or a consecutive range of ACGs separated by -, include the following statement:
```
Ericsson(config)# epg pgw rule-space <rule-space-nam
e> monitoring-key map <mk-id>
```

```
   access-control-group (<acg-id> | <acg-id>-<acg-id>)
```

A monitoring key can be mapped to several ACGs, but an ACG can only be mapped to one monitoring key.

5.17.5 Configuring Default Monitoring Key

Default monitoring can be configured for packet flows associated with ACRs or ACGs that are not mapped to any monitoring key. The default monitoring can be either of the following:

— Disabled. Monitoring is disabled by default. This is the default if nothing is configured.

— Use ACR. The ACR-ID is used as monitoring key identifier.

— Default monitoring key identifier.

To configure the default monitoring, include the following statement:

```
Ericsson(config)# epg pgw rule-space <rule-space-name
> monitoring-key default
   (disabled | use-access-control-rule | default-mo
nitoring-key <mk-id>)
```

Note: Default monitoring is not applicable for packet flows associated with DCRs.

5.17.6 Configuring an Alias for a Monitoring Key

By default, the EPG accepts only numerical monitoring key identifiers. To configure a textual monitoring key name as the monitoring key alias for a rule space, include the following statement:

```
Ericsson(config)# epg pgw rule-space <rule-space-na
me> alias <mk-name>
   monitoring-key <mk-id>
```

An alias is configured using a maximum 63 American Standard Code for Information Interchange (ASCII) characters. If an alias contains any characters other than the following ones, the PCC rule name or the PCC rule base name must be enclosed in double quotation mark ("). An alias cannot be numerical.

— Uppercase characters (A–Z)

— Lowercase characters (a–z)

— Base 10 digits (0–9)

— Hyphen (-)

— Underscore (_)

A monitoring key name can be mapped to exactly one monitoring key identifier.

5.18 Configuring Application Detection and Control

Application Detection and Control (ADC) is an optional licensed feature that is disabled by default. For information on how to manage licensed features, see Section 2 on page 1.

5.18.1 Activating Application Detection and Control

To activate the ADC feature, include the following statement:

```
Ericsson(config)# epg pgw feature-activation
   application-detection-and-control
```

5.18.2 Associating an SDF with an Application

To configure the mapping between an APP and an SDF or a consecutive range of SDFs separated by -, include the following statement:

```
Ericsson(config)# epg pgw rule-space <rule-space-name> applic
ation-detection application <application-id>
   service-data-flow (<sdf-id> | <sdf-id>-<sdf-id>)
```

An APP can be mapped to several SDFs, but an SDF can only be mapped to one APP.

5.18.3 Configuring Uplink Filters for an Application at Dedicated Bearer Establishment

To configure one or more uplink filter components for an APP, to be used at dedicated bearer establishment, include the following statement:

```
Ericsson(config)# epg pgw rule-space <rule-space-name> applicati
on-detection application <application-id> uplink-filter
   precedence <value>
   filter <id>
      remote-address <ip-address-prefix>
      remote-port (<port> | <port>-<port>)
      local-port (<port> | <port>-<port>)
      protocol-number <number>
      dscp <value>
```

The remote address notation is a dot-decimal IPv4 number or a colon-hexadecimal IPv6 number followed by the network prefix bit-length, separated by a slash (/) character. Optionally, the explicit "any" address can be specified with "0.0.0.0/0" or "::/0".

The supported DSCP values are af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs1, cs2, cs3, cs4, cs5, cs6, cs7, be, and ef. For more information on DSCP, see Quality of Service on the GGSN and PGW.

5.19 Associating an ACR with a Service Chain

To configure the mapping between an uplink Service Chain (SC) and an ACR, include the following statement:

```
Ericsson(config)# epg pgw rule-space <rule-space-name> acce
ss-control-rule <acr-id> service-chain
   uplink <sc-id>
```

To configure the mapping between a downlink SC and an ACR, include the following statement:

```
Ericsson(config)# epg pgw rule-space <rule-space-name> acce
ss-control-rule <acr-id> service-chain
   downlink <sc-id>
```

5.20 Configuring the Handling of Empty Bearers

Enable the rejection and disconnection of bearers without authorized services by including the following statement:

```
Ericsson(config)# epg pgw apn <apn-name> service-based-charging
policy-control dynamic gx-profile <profile-id>
   deny-empty-context
```

5.21 Configuring Online Charging Control

To configure online charging control as the default charging method for a user session, include the following statement:

```
Ericsson(config)# epg pgw apn <apn-name> service-based-charging
policy-control dynamic gx-profile <profile-id> charging-control
   online (enable | disable)
```

Note: Associate a user category associated with a charging-control based dynamic `gx-profile` with a `ro-profile` as well.

5.22 Enabling Immediate Credit Control

The EPG can be configured to perform a credit request to the Online Charging System (OCS) immediately at the activation of dynamic charging rules by including the following statement:

```
Ericsson(config)# epg pgw apn <apn-name> service-based-charging
policy-control dynamic gx-profile <profile-id>
```

```
   immediate-credit-control
```

5.23 Configuring Packet Marking Based on PISC

To configure the mapping between a packet marking value and an ACR or a consecutive range of ACRs separated by -, include the following statement:

```
Ericsson(config)# epg pgw rule-space <rule-space-name> pack
et-marking map <packet-marking-value>
   access-control-rule (<acr-id> | <acr-id>-<acr-id)
```

The allowed range of the packet marking value is 0–255 (0x00–0xff).

5.24 Configuring Inclusion of the 3GPP-Charging-Characteristics AVP in CCR Messages

The EPG can be configured to send the selected Charging Characteristics to the PCRF.

Note: Inclusion of CC in CCR messages cannot be enabled if proprietary Gx+ extensions are disabled as described in Section 5.1 on page 9.

To configure the EPG to include the selected CC in CCR-I messages sent to the PCRF, include the following statement:

```
Ericsson(config)# epg pgw apn <apn-name> service-base
d-charging policy-control dynamic gx-profile <profile
-id> charging-characteristics
   initial
```

Note: If the CC is provided by the OCS, no CC is included in the CCR-I message to the PCRF, instead, the CC is sent in the next CCR-U message.

To configure the EPG to include the selected CC in CCR-U messages sent to the PCRF always, include the following statement:

```
Ericsson(config)# epg pgw apn <apn-name> service-base
d-charging policy-control dynamic gx-profile <profile
-id> charging-characteristics
   update
```

5.25 Configuring Charging Rule Revalidation

The following properties of charging rule revalidation can be configured in the EPG:

— max-rate: the rate at which charging rule revalidation is performed.

— `margin`: the time period reserved for revalidation of newly created or updated sessions after revalidation starts.

— `max-deviation`: the maximum ahead of time by which the PGW is allowed to start the charging rule revalidation.

To configure charging rule revalidation in the EPG, include the following statement:

```
Ericsson(config)# epg pgw policy-control revalidation
   max-rate <value>
   margin <value>
   max-deviation <value>
```

The `max-rate` indicates the percentage of the maximum request rate configured on the DAS. The value range is 1–80 percent. The default value is 10. If the maximum request rate on the DAS is not configured, the rate of the charging rule revalidation is 5000 sessions per second per PSC instance.

The supported range of values for `margin` is 1–60 seconds. If a value for `margin` is not configured, no safety margin is used. By default, the `margin` is not configured in the EPG.

The supported range of values for `max-deviation` is 1–60 minutes. If a value for `max-deviation` is not configured, no maximum deviation is used. By default, the `maxDeviation` is not configured.

Note: The new configuration takes effect when a session is created or the revalidation time of a session is updated.

5.26 Configuring Sending of Bearer Usage on WLAN

The `Bearer-Usage` AVP is not included in `CCR-I` messages sent to the PCRF on the Gx+ interface for WLAN access. To configure the EPG to include the `Bearer-Usage` AVP in `CCR-I` messages also for WLAN access, use the following command:

```
Ericsson(config)# epg pgw apn <apn-name> service-based-charging
policy-control dynamic gx-profile <profile-id>
   include-bearer-usage-on-wlan
```

5.27 Configuring APN Name Extension for VPNs

The EPG can be configured to prepend the domain of a user to the APN that is normally sent in the `Called-Station-Id` AVP. This APN extension allows identification of different groups of users based on their domains. The domain is extracted from the username in the `PAP` or `CHAP` packets contained in the `PCO` IE. A single colon (`:`) is used to delimit the domain from the APN. For example, if the APN is `internet.com` and the username is `jane@example.com`, the `Called-Station-Id` sent to the PCRF is `example.com:internet.com`.

If the domain name contains byte values outside the printable ASCII range (32–127), the EPG converts the entire domain name to hexadecimal format before including the domain name in the Called-Station-Id AVP.

If no domain is available, only the delimiter is prepended. The domain is not available if any of the following applies:

— The PCO IE is missing.

— The PCO IE does not contain a PAP/CHAP packet.

— The username does not contain a @ character.

To configure APN Name Extension for VPNs, use the following command:

```
Ericsson(config)# epg pgw apn <apn-name> service-based-charging
policy-control dynamic gx-profile <profile-id>
   extend-apn-with-domain
```

The change takes effect immediately for all CCR-I messages.

5.28 Configuring the Late Request Handling AVPs

To configure a Gx profile to include the Origination-Time-Stamp and Maximum-Wait-Time AVPs, include the following statement:

```
Ericsson(config)# epg pgw apn apn-name> service-based-charging
policy-control dynamic gx-profile <profile-id>
   late-request-handling
```

5.29 Configuring Custom Attribute Decoding

The GGSN and PGW can be configured to decode vendor specific AVPs, referred to as custom attributes, received at the command level in a successful CCA-Initial message from the PCRF. A custom attribute is assigned a logical name in the GGSN and PGW configuration and identified on the Gx interface by it's AVP code and vendor identifier. A decoded AVP value can be used for user session identification, categorization, etc.

To configure the AVP code of a custom attribute, include the following statement:

```
Ericsson(config)# epg pgw apn <name> service-based-charging
policy-control dynamic gx-profile <name> cca-avp custom-attribute
<attribute-name> code <value>
```

To configure the AVP vendor identifier of a custom attribute, include the following statement:

```
Ericsson(config)# epg pgw apn <name> service-based-charging
policy-control dynamic gx-profile <name> cca-avp custom-attribute
<attribute-name> vendor-id <value>
```

To configure the AVP type of a custom attribute, include the following statement:

```
Ericsson(config)# epg pgw apn <name> service-based-charging
policy-control dynamic gx-profile <name> cca-avp custom-attribute
<attribute-name> type (octet-string)
```

5.30 Suppressing the Sending of Update Bearer Request after Receiving Modify Bearer Request during Handovers

In handovers to Gn access, the PGW applies the authorized QoS. For scenarios where the PCC session modification is performed after the PGW receives a `Modify Bearer Request` message, the PGW sends the authorized QoS to the serving node in an `Update Bearer Request` message after sending a `Modify Bearer Response` message if the negotiated QoS is different from the authorized QoS. If the HSS controls the QoS based on the RAT type of the session, a `Modify Bearer Command` message from the HSS can cause a collision with this `Update Bearer Request` message.

To suppress the sending of an `Update Bearer Request` message after sending a `Modify Bearer Response` message during handovers, include the following statement:

```
Ericsson(config)# epg pgw apn <apn-name> service-based-charging
policy-control dynamic gx-profile <profile-id>
   suppress-update-at-handover
```

The configuration takes effect immediately on the current session.

6 Configuring Failure Handling

The following section describes how to configure failure handling for Gx+ PCC Sessions and PCC rules. For complete failure handling, do the following:

— Configure failure handling profile and include failure actions and conditions.

— Associate the failure handling profiles with a Gx profile.

6.1 Configuring Failure Handling Profiles

A failure handling profile defines configurable failure handling options related to policy control. One or more failure handling profiles can be configured.

To configure a failure handling profile, include the following statement:

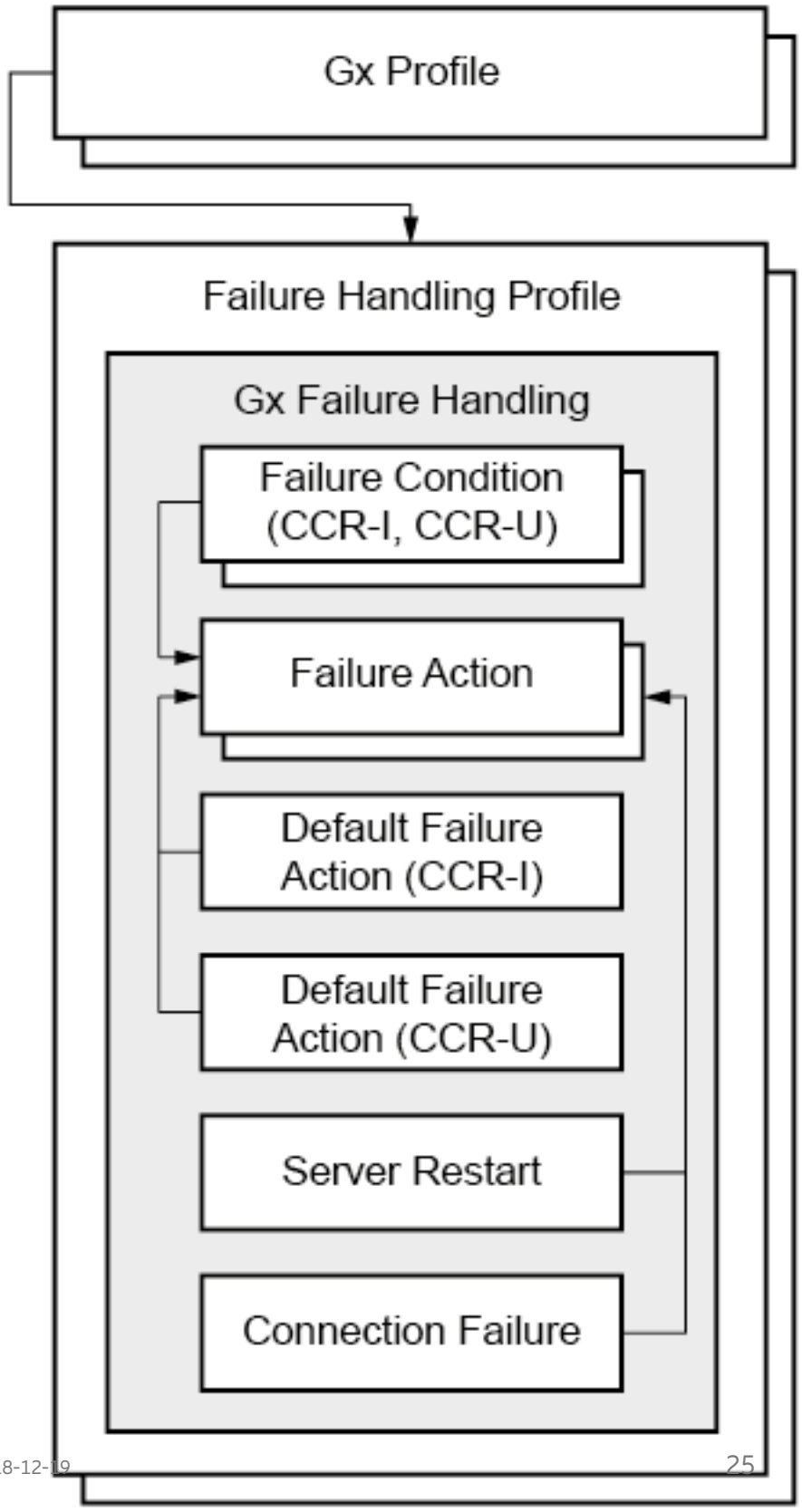
```
Ericsson(config)# epg pgw policy-control
   failure-handling-profile <profile-name>
```

6.1.1 Configure Gx+ PCC Failure Handling

This section describes how to configure Gx failure handling conditions and actions related to Gx+ PCC request session and node level failures. Example 2 shows an example failure handling profile.

Figure 1 shows the failure handling profile configuration structure.

Configuration Structure for Gx Failure Handling



6.1.1.1 Configure Default Action for Request Level Failures

The default failure action for failed Gx+ PCC requests is to terminate the user session. The default action can be changed by associating a user defined failure action.

For information on how to configure failure actions, see Section 6.1.1.5 on page 29.

6.1.1.1.1 Configure Default Failure Action for CCR Initial Messages

To associate a failure action to use as the default CCR-I message failure action, include the following statement:

```
Ericsson(config)# epg pgw policy-control failure-handling-profile
<profile-name> gx-failure-handling
   default-ccr-initial-failure-action <failure-action-name>
```

6.1.1.1.2 Configure Default Failure Action for CCR Update Messages

To associate a failure action to use as the default CCR-U message failure action, include the following statement:

```
Ericsson(config)# epg pgw policy-control failure-handling-profile
<profile-name> gx-failure-handling
   default-ccr-update-failure-action <failure-action-name>
```

6.1.1.2 Configure a Connection Failure Action

To associate a failure action to use as the connection failure action, include the following statement:

```
Ericsson(config)# epg pgw policy-control failure-handling-profile
<profile-name> gx-failure-handling
   connection-failure-action <failure-action-name>
```

6.1.1.3 Configure a Server Restart Action

To associate a failure action to use as the server restart action, include the following statement:

```
Ericsson(config)# epg pgw policy-control failure-handling-profile
<profile-name> gx-failure-handling
   server-restart-action <failure-action-name>
```

6.1.1.4 Configure a Failure Condition

A failure condition specifies the request failures that trigger an associated failure-action during a Gx+ PCC session failure. To configure a request failure condition, perform the following steps:

— Configure the failure condition name.

— Configure the failure condition priority.

— Configure an association to a failure action.

— Configure the failure condition message type and one or more message failure types.

  • Configure timeout as a possible message failure type.

  • Configure routing failure as a possible message failure type.

  • Configure Diameter result codes as a possible message failure type.

  • Configure experimental Diameter result codes as a possible message failure type.

6.1.1.4.1 Configure Name

To configure the name of a failure condition, include the following statement:

```
Ericsson(config)# epg pgw policy-control failure-handling-profile
<profile-name> gx-failure-handling
   request-failure-condition <request-failure-condition-name>
```

6.1.1.4.2 Configure Priority

The failure condition priority specifies the importance of a failure condition in relation to other failure conditions. To configure the priority of a request failure condition, include the following statement:

```
Ericsson(config)# epg pgw policy-control failure-handling-profile
<profile-name> gx-failure-handling request-failure-condition
<request-failure-condition-name>
   priority <value>
```

The value range of `priority` is 1-128.

Note: A lower value means higher priority.

6.1.1.4.3 Configure Failure Action Association

The failure action association specifies what action to take when a failure condition is matched.

For information on how to configure a failure action, refer to Section 6.1.1.5 on page 29.

To associate a failure action with a failure condition, include the following statement:

```
Ericsson(config)# epg pgw policy-control failure-handling-profile
<profile-name> gx-failure-handling request-failure-condition
<request-failure-condition-name>
   failure-action <failure-action-name>
```

6.1.1.4.4 Configure Message Type

The message type specifies the Gx message for which the configured failure types are matched against. To configure the message type, include the following statement:

```
Ericsson(config)# epg pgw policy-control failure-handling-profile
<profile-name> gx-failure-handling request-failure-condition
<request-failure-condition-name>
   message-type (ccr-initial | ccr-update)
```

6.1.1.4.5 Configure Message Failure Type Timeout

Message timeout occurs if a response to a request is not received within the configured request timeout for a DAS, or when the GGSN or PGW fails to send the message because it timed out according to the internal traffic shaper. To configure message timeout as a failure condition, include the following statement:

```
Ericsson(config)# epg pgw policy-control failure-handling-profile
<profile-name> gx-failure-handling request-failure-c
ondition <request-failure-condition-name> message-ty
pe (ccr-initial | ccr-update)
   timeout
```

6.1.1.4.6 Configure Message Failure Type Connection Failure

Connection failure occurs if a message cannot be sent because a route cannot be found. For example, if all peers in a DAS are unavailable. To configure message connection failure as a failure condition, include the following statement:

```
Ericsson(config)# epg pgw policy-control failure-handling-profile
<profile-name> gx-failure-handling request-failure-c
ondition <request-failure-condition-name> message-ty
pe (ccr-initial | ccr-update)
   connection-failure
```

6.1.1.4.7 Configure Message Failure Type Result Codes

Diameter result codes indicate success or failure of Diameter messages. To configure which result codes are failure conditions include the following statement:

```
Ericsson(config)# epg pgw policy-control failure-handling-profile
<profile-name> gx-failure-handling request-failure-c
```

```
ondition <request-failure-condition-name> message-ty
pe (ccr-initial | ccr-update)
   result-code (<result-code> | <result-code>-<result-code>)
```

Result codes can be configured as single result codes, or by configuring a range of result codes.

Note: The following result code is ignored if configured:

— (2001) DIAMETER SUCCESS

6.1.1.4.8 Configure Message Failure Type Experimental Result Codes

Experimental result codes indicate vendor specific failures towards the GGSN or PGW. To configure which experimental result codes are failure conditions, include the following statement:

```
Ericsson(config)# epg pgw policy-control failure-handling-profile
<profile-name> gx-failure-handling request-failure-c
ondition <request-failure-condition-name> message-ty
pe (ccr-initial | ccr-update)
   experimental-result-code (<vendor-id:result-code> |
<vendor-id>:<result-code>-<result-code>)
```

Result codes can be configured as single result codes, or by configuring a range of result codes.

Note: The EPG supports the following keywords for IANA vendor IDs:

— **ericsson** = **193**

— **3gpp** = **10415**

— **3gpp2** = **5535**

The following experimental result code is ignored if configured:

— (10415:4144), 3GPP:DIAMETER PENDING TRANSACTION

6.1.1.5 Configure a Failure Action

A failure action specifies what action the PGW or GGSN takes when a failure condition is fulfilled. To configure a failure action, include the following statement:

```
Ericsson(config)# epg pgw policy-control failure-handling-profile
<profile-name> gx-failure-handling
   failure-action <failure-action-name>
```

6.1.1.5.1 Configure Continue Failure Action

The `continue` failure action allows the user session to continue, with additional commands that allow for the PGW to apply behaviors to the Gx+ PCC session

and select PCC rules. Table 3 shows the permitted command combinations with applied behaviors.

Table 3 Permitted Command Combinations with Applied Behaviors

Failure Action	Behavior Applied to the Gx+ PCC Session	Behavior Applied to the PCC Rules and Authorized QoS
`continue`	The Gx+ PCC session is terminated, no `CCR-T` is sent.	PCC rules installed by the PCRF are kept. Authorized QoS is kept and enforced.
`continue retain`(1)	The Gx+ PCC session is kept. The next time an event trigger is matched, a `CCR-U` is sent, and a `CCR-T` is sent when the session is terminated.	PCC rules installed by the PCRF are kept. Authorized QoS is kept and enforced.
`continue reestablish`	The Gx+ PCC session is terminated, no `CCR-T` is sent. The GGSN or PGW attempts to re-establish the connection to the PCRF by creating a new Gx+ PCC session.	PCC rules installed by the PCRF are kept. Authorized QoS is kept and enforced. When a new Gx+ PCC session is established, the PCC rules and QoS that were kept are removed and the new PCC rules and QoS provided by the PCRF are installed.

Failure Action	Behavior Applied to the Gx+ PCC Session	Behavior Applied to the PCC Rules and Authorized QoS
`continue local-policy-control`	The Gx+ PCC session is terminated, no `CCR-T` is sent.	PCC rules installed by the PCRF are removed, new PCC rules are installed based on LPT. Authorized QoS is removed and any QoS requested by the serving node is accepted.
`continue local-policy-control reestablish`	The Gx+ PCC session is terminated, no `CCR-T` is sent. The GGSN or PGW attempts to re-establish the connection to the PCRF by creating a new Gx+ PCC session.	PCC rules installed by the PCRF are removed, new PCC rules are installed based on LPT. Authorized QoS is removed and any QoS requested by the serving node is accepted. When a new Gx+ PCC session is established, the PCC rules that were installed by LPT are removed and the new PCC rules and QoS provided by the PCRF are installed.

(1) The Retain failure action is only valid for CCR-U failure messages.

Configure Continue

Delete the Gx+ PCC session and retain the installed rules.

To configure the `continue` failure action, include the following statement:

```
Ericsson(config)# epg pgw policy-control failure-handl
ing-profile <profile-name> gx-failure-handling failure
-action <failure-action-name>
   continue
```

Configure Retain

Retain the Gx+ PCC session and retain the installed PCC rules.

Note: The `retain` failure action cannot be configured for CCR-I failure messages.

To configure the `retain` failure action, include the following statement:

```
Ericsson(config)# epg pgw policy-control failure-handling-
profile <profile-name> gx-failure-handling failure-action
<failure-action-name> continue
   retain
```

Configure Reestablish

Reestablish the Gx+ PCC session and retain the installed PCC rules.

To configure the `reestablish` failure action, include the following statement:

```
Ericsson(config)# epg pgw policy-control failure-handling-
profile <profile-name> gx-failure-handling failure-action
<failure-action-name> continue
   reestablish
```

Configure Local Policy Control

Delete the Gx+ PCC session and use the LPT.

To configure the Local Policy Control failure action, include the following statement:

```
Ericsson(config)# epg pgw policy-control failure-handling-
profile <profile-name> gx-failure-handling failure-action
<failure-action-name> continue
   local-policy-control
```

Configure Local Policy Control and Reestablish

Reestablish the Gx+ PCC session and use the LPT.

To configure the Local Policy Control and Reestablish failure action, include the following statement:

```
Ericsson(config)# epg pgw policy-control failure-handling-
profile <profile-name> gx-failure-handling failure-action
<failure-action-name> continue
   local-policy-control
   reestablish
```

6.1.1.5.2 Configure Terminate Failure Action

The Terminate failure action leads to the GGSN or PGW rejecting or deleting user sessions.

Configure Terminate

To configure the Terminate failure action, include the following statement:

```
Ericsson(config)# epg pgw policy-control failure-handl
ing-profile <profile-name> gx-failure-handling failure
-action <failure-action-name>
   terminate
```

Configure Termination of the Related Gx+ PCC Session

To configure the GGSN or PGW to terminate the Gx+ PCC session related to the user session, include the following statement:

```
Ericsson(config)# epg pgw policy-control failure-handl
ing-profile <profile-name> gx-failure-handling failure
-action <failure-action-name>
   terminate
      send-ccr-termination
```

Configure Termination Using GTP Cause Code Reactivation Requested

To configure the GGSN or PGW to terminate the user session using the cause code Reactivation Requested included in the IP-CAN deletion request message, include the following command:

```
Ericsson(config)# epg pgw policy-control failure-handl
ing-profile <profile-name> gx-failure-handling failure
-action <failure-action-name>
   terminate
      send-reactivation-requested
```

Configure GTPv1 Cause Code for IP-CAN Termination

To configure the GTPv1 cause code to be included when rejecting the IP-CAN session creation or the IP-CAN session modification, include the following statement:

```
Ericsson(config)# epg pgw policy-control failure-handl
ing-profile <profile-name> gx-failure-handling failure
-action <failure-action-name>
   terminate
      gtpv1cause <gtpv1cause-code-number>
```

Configure GTPv2 Cause Code for IP-CAN Termination

To configure the GTPv2 cause code to be included when rejecting the IP-CAN session creation or the IP-CAN session modification, include the following statement:

```
Ericsson(config)# epg pgw policy-control failure-handl
ing-profile <profile-name> gx-failure-handling failure
-action <failure-action-name>
   terminate
```

```
gtpv2cause <gtpv2cause-code-number>
```

6.1.1.6 Example of a Gx+ PCC Failure Handling Profile

Example 2 shows a failure handling profile. The example configuration results in the following behaviors:

- `CCR-I` message failure: Time-out, 3002-3004, or 4002 leads to use of LPT with Reestablish failure action.
- `CCR-U` message failure: 5002 leads to termination of the user session, termination of Gx+ PCC session, and GTP cause code `Reactivation Requested`.
- Other `CCR-U` message failures configured to use the default failure action lead to termination of user session, termination of Gx+ PCC session, and GTP cause code `System Failure` (204/72).
- Other `CCR-I` message failures use hardcoded default failure action.
- PCRF restart leads to continuation of all existing user sessions affected by the restart together with use of installed PCC rules and Gx+ PCC session reestablishment

```
epg pgw policy-control failure-handling-profile failure-handling-profile1
 gx-failure-handling default-ccr-update-failure-action failure-action3
 gx-failure-handling server-restart-action failure-action4
 gx-failure-handling request-failure-condition request-failure-condition1
  priority       1
  failure-action failure-action1
  message-type ccr-initial
   timeout
   result-code [ 3002-3004 4002 ]
  !
 !
 gx-failure-handling request-failure-condition request-failure-condition2
  priority       2
  failure-action failure-action2
  message-type ccr-update
   result-code [ 5002 ]
  !
 !
 gx-failure-handling failure-action failure-action1
  continue reestablish
  continue local-policy-control
 !
 gx-failure-handling failure-action failure-action2
  terminate send-ccr-termination
  terminate send-reactivation-requested
 !
 gx-failure-handling failure-action failure-action3
  terminate send-ccr-termination
  terminate gtpv1-cause 204
  terminate gtpv2-cause 72
 !
 gx-failure-handling failure-action failure-action4
  continue reestablish
 !
!
```

Example 2 A Failure Handling Profile

6.1.2 Configure PCC Rule Failure Handling

This section describes how to configure PCC rule failure handling conditions and actions related to failures during PCC rule procedures. An example of a failure handling profile is shown in Example 3.

To configure PCC rule failure handling, start by issuing the following statement:

```
Ericsson(config)# epg pgw policy-control failure-handl
ing-profile <profile-name>
    pcc-rule-failure-handling
```

6.1.2.1 Configure Default Installation Failure Action

The default failure action for PCC rule installations is to send a charging rule report with the `Rule-Failure-Code` AVP set to `RESOURCE_ALLOCATION_FAILURE`. The default action can be changed by associating a user-defined failure action. For information on how to configure failure actions, see Section 6.1.2.4 on page 38.

To associate a failure action to use as the default PCC rule installation failure action, issue the following statement:

```
Ericsson(config)# epg pgw policy-control failure-handling-profile
<profile-name> pcc-rule-failure-handling
   default-installation-failure-action <failure-action-name>
```

6.1.2.2 Configure Default Modification Failure Action

The default failure action for PCC rule modifications is to remove the PCC rule, and send a charging rule report with the `Rule-Failure-Code` AVP set to `RESOURCE_ALLOCATION_FAILURE`. The default action can be changed by associating a user-defined failure action. For information on how to configure failure actions, see Section 6.1.2.4 on page 38.

To associate a failure action to use as the default PCC rule modification failure action, issue the following statement:

```
Ericsson(config)# epg pgw policy-control failure-handling-profile
<profile-name> pcc-rule-failure-handling
   default-modification-failure-action <failure-action-name>
```

6.1.2.3 Configure an Installation or Modification Failure Condition

A failure condition specifies the serving node, RAN, or NAS request failures that trigger an associated failure-action during a PCC rule failure. To configure a failure condition, perform the following steps:

— Configure the failure condition name

— Configure the failure condition priority.

— Configure an association to a failure action.

— Configure the failure operation type and one or more message failure types:

- Configure GTPv1 cause codes.
- Configure GTPv2 cause codes.
- Configure GTPv2 RAN cause codes.
- Configure GTPv2 NAS cause codes.

If more than one of GTPv2 cause, GTPv2 RAN cause, and GTPv2 NAS cause are provided in the same failure condition, at least one of them must be contained in a received message for the condition to be fulfilled.

6.1.2.3.1 Configure Failure Condition Name

To configure the name of a failure condition for PCC rule operations, include the following statement:

```
Ericsson(config)# epg pgw policy-control failure-handling-profile
<profile-name> pcc-rule-failure-handling
   request-failure-condition <failure-condition-name>
```

6.1.2.3.2 Configure Priority

The failure condition priority specifies the evaluation precedence of a failure condition in relation to other failure conditions. To configure the priority of a PCC rule failure condition, include the following statement:

```
Ericsson(config)# epg pgw policy-control failure-handling-profile
<profile-name> pcc-rule-failure-handling request-failure
-condition <failure-condition-name>
   priority [1-64]
```

Note: A lower value means higher priority.

6.1.2.3.3 Configure Failure Action Association

The failure action association specifies what action to take when a failure condition is matched. For information on how to configure a failure action, see Section 6.1.2.4 on page 38. To associate a failure action with a failure condition, include the following statement:

```
Ericsson(config)# epg pgw policy-control failure-handling-profile
<profile-name> pcc-rule-failure-handling request-failure
-condition <failure-condition-name>
   failure-action <failure-action-name>
```

6.1.2.3.4 Configure Operation Type

The operation type specifies the PCC rule operation for which the failure condition applies. To configure the PCC rule operation type, include the following statement:

```
Ericsson(config)# epg pgw policy-control failure-handling-profile
<profile-name> pcc-rule-failure-handling request-failure
-condition <failure-condition-name>
   operation-type (installation | modification)
```

6.1.2.3.5 Configure GTPv1 Failure Cause Codes

GTPv1 cause codes indicate success or failure of GTPv1 messages. To configure which cause codes are failure conditions include the following statement:

```
Ericsson(config)# epg pgw policy-control failure-hand
ling-profile <profile-name> pcc-rule-failure-handling
request-failure-condition <failure-condition-name> operation-type
(installation | modification)
   gtpv1cause (cause-code | cause-code-cause-code)
```

Note: Configuration of the following cause codes is ignored: 192, 240.

6.1.2.3.6 Configure GTPv2 Failure Cause Codes

GTPv2 cause codes indicate success or failure of GTPv2 messages. To configure which cause codes are failure conditions include the following statement:

```
Ericsson(config)# epg pgw policy-control failure-hand
ling-profile <profile-name> pcc-rule-failure-handling
request-failure-condition <failure-condition-name> operation-type
(installation | modification)
   gtpv2cause (cause-code | cause-code-cause-code)
```

Note: Configuration of the following cause codes is ignored: 64, 107.

6.1.2.3.7 Configure GTPv2 RAN Failure Cause Codes

GTPv2 RAN cause codes indicate success or failure of GTPv2 messages. Configured RAN cause values match if the Protocol type is set to 1 (S1ApCause) and Cause type is set to 0 (Radio Network Layer) in the `RAN/NAS Cause` IE. To configure which cause codes are failure conditions include the following statement:

```
Ericsson(config)# epg pgw policy-control failure-hand
ling-profile <profile-name> pcc-rule-failure-handling
request-failure-condition <failure-condition-name> operation-type
(installation | modification)
   gtpv2ran-cause (cause-code | cause-code-cause-code)
```

6.1.2.3.8 Configure GTPv2 NAS Failure Cause Codes

GTPv2 NAS cause codes indicate success or failure of GTPv2 messages. Configured NAS cause values match if the Protocol type is set to 2 (EMM Cause) or 3 (ESM Cause) in the `RAN/NAS Cause` IE. To configure which cause codes are failure conditions include the following statement:

```
Ericsson(config)# epg pgw policy-control failure-hand
ling-profile <profile-name> pcc-rule-failure-handling
request-failure-condition <failure-condition-name> operation-type
(installation | modification)
   gtpv2nas-cause (cause-code | cause-code-cause-code)
```

6.1.2.4 Configure a Failure Action

A failure action specifies what action the PGW or GGSN takes when a failure condition is fulfilled. To configure a failure action, include the following statement:

```
Ericsson(config)# epg pgw policy-control failure-handling-profile
<profile-name> pcc-rule-failure-handling
   failure-action <failure-action-name>
```

6.1.2.4.1 Configure Keep

The keep failure action indicates that the PGW keeps the previous version of the PCC rule, if possible. To configure the keep failure action, include the following statement:

```
Ericsson(config)# epg pgw policy-control failure-hand
ling-profile <profile-name> pcc-rule-failure-handling
failure-action <failure-action-name>
   keep
```

6.1.2.4.2 Configure Remove

The remove failure action indicates that the PGW removes the PCC rule. To configure the remove failure action, include the following statement:

```
Ericsson(config)# epg pgw policy-control failure-hand
ling-profile <profile-name> pcc-rule-failure-handling
failure-action <failure-action-name>
   remove
```

6.1.2.4.3 Configuring Rule Failure Code

To configure a `Rule-Failure-Code` to be sent to the PCRF, include the following statement:

```
Ericsson(config)# epg pgw policy-control failure-hand
ling-profile <profile-name> pcc-rule-failure-handling
failure-action <failure-action-name>
   rule-failure-code code
```

6.1.2.5 Example of a Failure handling profile

Example 3 shows a failure handling profile.

Example case for a PCC rule installation failure:

— If a GTPv2 cause code in the range 64–95 is received as the result of a PCC rule installation, the priority 1 PCC rule failure condition is matched, and `Rule-Failure-Code` 32 is sent.

— Else, if a GTPv2 cause code in the range 64–128 or a GTPv2 NAS cause code in the range 1–128 is received as the result of a PCC rule installation, the priority 2 PCC rule failure condition is matched, and `Rule-Failure-Code` 33 is sent.

— For PCC rule installation failures that do not match any specified failure conditions, the default `Rule-Failure-Code` `RESOURCE_ALLOCATION_FAILURE` is sent.

Example case for a PCC rule modification failure:

— If a GTPv2 cause code in the range 64–95 or a GTPv2 RAN cause code in the range 1–64 is received as the result of a PCC rule modification, the

priority 1 PCC rule failure condition is matched, the unmodified rule is kept and `Rule-Failure-Code` 32 is sent.

— Else, if a GTPv2 cause code in the range 64–128 is received as the result of a PCC rule modification, the priority 2 PCC rule failure condition is matched, the unmodified rule is kept and `Rule-Failure-Code` 33 is sent.

— For PCC rule modification failures that do not match any specified failure condition, the default modification failure action is used, the unmodified rule is kept and `Rule-Failure-Code` 34 is sent.

```
epg pgw policy-control failure-handling-profile failure-handling-profile-profil
 pcc-rule-failure-handling default-modification-failure-action failure-action-3
 pcc-rule-failure-handling failure-action failure-action-1
  keep
  rule-failure-code 32
 !
 pcc-rule-failure-handling failure-action failure-action-2
  keep
  rule-failure-code 33
 !
 pcc-rule-failure-handling failure-action failure-action-3
  keep
  rule-failure-code 34
 !
 pcc-rule-failure-handling request-failure-condition failure-condition-1
  priority       1
  failure-action failure-action-1
  operation-type installation
   gtpv2-cause [ 64-95 ]
  !
  operation-type modification
   gtpv2-cause     [ 64-95 ]
   gtpv2-ran-cause [ 1-64 ]
  !
 !
 pcc-rule-failure-handling request-failure-condition failure-condition-2
  priority       2
  failure-action failure-action-2
  operation-type installation
   gtpv2-cause     [ 64-128 ]
   gtpv2-nas-cause [ 1-128 ]
  !
  operation-type modification
   gtpv2-cause [ 64-128 ]
  !
 !
!
```

Example 3 A Failure Handling Profile

6.2 Associating a Failure Handling Profile with a Gx Profile

To associate a failure handling profile to use with a Gx profile, include the following statement:

```
Ericsson(config)# epg pgw apn <apn-name> service-based-charging
policy-control dynamic gx-profile <gx-profile-id>
   failure-handling-profile <profile-name>
```

To configure a failure handling profile, see Section 6.1 on page 23.

Reference List

Standards

[1] 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface, 3GPP TS 29.060