ERICSSON

Charging Methods Configuration

OPERATION DIRECTIONS

60/1543-AXB 250 10/4-V3 Uen BK

Contents

1	**Introduction**	**1**
1.1	Scope	1
1.2	Target Groups	1
2	**Overview**	**1**
3	**Configure Volume-Based Charging**	**2**
3.1	Configure Volume Measurement	2
3.1.1	Configure Application Layer Volume Measurement	2
3.1.2	Exclude Retransmitted Packets from Measured Volume	4
3.1.3	Exclude Fragmented Packet IP Headers from Measured Volume	5
3.2	Configure Volume Reporting	5
3.2.1	Configure Bearer Level Volume Reporting	5
3.2.2	Configure RG Level Volume Reporting	5
3.2.3	Configure SI Level Volume Reporting	5
3.2.4	Configure URI Level Volume Reporting	5
3.2.5	Configure IP Flow Level Volume Reporting	6
3.2.6	Configure Transaction Level Volume Reporting	6
4	**Configure Time-Based Charging**	**7**
4.1	Configure Time Measurement	7
4.1.1	Configure an RG Cluster	7
4.1.2	Configure the Time Measurement Method	7
4.1.3	Configure Time Measurement Resolution	8
4.1.4	Configure Time Measurement Inactivity	8
4.1.5	Configure Time Envelope Measurement and Reporting	9
4.2	Configure Time Reporting	9
4.2.1	Configure RG Level Time Reporting	9
5	**Configure Event-Based Charging**	**9**
5.1	Configure Event Tracking	10
5.1.1	Activate Event Tracking for a Rule Classifying FTP Traffic	10
5.1.2	Activate Event Tracking for a Rule Classifying HTTP or WSP Traffic	10
5.1.3	Activate Event Tracking for a Rule Classifying MMS Traffic	11
5.1.4	Activate Event Tracking for a Rule Classifying POP3 Traffic	12
5.1.5	Activate Event Tracking for a Rule Classifying RTSP Traffic	12
5.1.6	Activate Event Tracking for a Rule Classifying SIP Traffic	12
5.1.7	Activate Event Tracking for a Rule Classifying SMTP Traffic	12
5.2	Configure Event Reporting	13
5.2.1	Configure RG Level Event Reporting	13

5.2.2 Configure URI Level Event Reporting 13

1 Introduction

This document provides instructions for configuring the service aware charging methods, referred to as charging methods, available for the Service-Aware Charging and Control (SACC) solution in the EPG for GSM, WCDMA, LTE systems, and trusted non-3GPP networks, such as CDMA2000.

1.1 Scope

This document covers the following issues:

— Detailed instructions for configuring volume-based charging

— Detailed instructions for configuring time-based charging

— Detailed instructions for configuring event-based charging

For an overview of the SACC solution, refer to SACC Overview.

For detailed information on the charging methods, refer to Charging Methods.

For detailed information on configuring the reporting levels, refer to Offline Charging Configuration.

1.2 Target Groups

This document is intended for personnel performing the configuration of the EPG.

2 Overview

The following sections provide detailed instructions for configuring the following charging methods:

— Volume-based charging

— Time-based charging

— Event-based charging

For detailed information on the charging methods, refer to Charging Methods.

3 Configure Volume-Based Charging

Volume, that is, usage in number of forwarded bytes, can be measured and reported on bearer level, Rating Group (RG) level, Service Identifier (SI) level, or Uniform Resource Identifier (URI) level.

3.1 Configure Volume Measurement

For detailed information on the available volume measurement characteristics, refer to Charging Methods.

The following subsections provide detailed instructions for configuring optional volume measurement characteristics.

3.1.1 Configure Application Layer Volume Measurement

Note: Volume measurement on the application layer is resource-consuming and can have an impact on the capacity and performance of the EPG.

By default, volume is measured on the network layer, that is, including the bytes used for network and transport layer protocol headers.

The following subsections provide detailed instructions for configuring application level volume measurement for the supported protocols.

3.1.1.1 Configure Application Layer Volume Measurement for a Rule Classifying FTP Traffic

To enable volume measurement on the application layer for a term in a deep inspection rule classifying File Transfer Protocol (FTP) traffic, include the following statement:

```
Ericsson(config)# epg pgw service-identification ftp-rule
<rule-name> term <term-id> then
   aggregated-volume application
```

3.1.1.2 Configure Application Layer Volume Measurement for a Rule Classifying HTTP or WSP Traffic

To enable volume measurement on the application layer for a term in a deep inspection rule classifying Hypertext Transfer Protocol (HTTP) or Wireless Session Protocol (WSP) traffic, include the following statement:

```
Ericsson(config)# epg pgw service-identification http-wsp-rule
<rule-name> term <term-id> then
   aggregated-volume application
```

3.1.1.3 Configure Application Layer Volume Measurement for a Rule Classifying MMS Traffic

To enable volume measurement on the application layer for a term in a deep inspection rule classifying Multimedia Messaging Service (MMS) traffic, include the following statement:

```
Ericsson(config)# epg pgw service-identification http-wsp-rule
<rule-name> term <term-id> then
   aggregated-volume application
```

3.1.1.4 Configure Application Layer Volume Measurement for a Rule Classifying IMAP Traffic

To enable volume measurement on the application layer for a term in a deep inspection rule classifying Internet Message Access Protocol (IMAP) traffic, include the following statement:

```
Ericsson(config)# epg pgw service-identification imap-rule
<rule-name> term <term-id> then
   aggregated-volume application
```

3.1.1.5 Configure Application Layer Volume Measurement for a Rule Classifying POP3 Traffic

To enable volume measurement on the application layer for a term in a deep inspection rule classifying Post Office Protocol 3 (POP3) traffic, include the following statement:

```
Ericsson(config)# epg pgw service-identification pop3-rule
<rule-name> term <term-id> then
   aggregated-volume application
```

3.1.1.6 Configure Application Layer Volume Measurement for a Rule Classifying RTSP Traffic

To enable volume measurement on the application layer for a term in a deep inspection rule classifying Real Time Streaming Protocol (RTSP) traffic, include the following statement:

```
Ericsson(config)# epg pgw service-identification rtsp-rule
<rule-name> term <term-id> then
   aggregated-volume application
```

3.1.1.7 Configure Application Layer Volume Measurement for a Rule Classifying SIP Traffic

To enable volume measurement on the application layer for a term in a deep inspection rule classifying Session Initiation Protocol (SIP) traffic, include the following statement:

```
Ericsson(config)# epg pgw service-identification sip-rule
<rule-name> term <term-id> then
   aggregated-volume application
```

3.1.1.8 Configure Application Layer Volume Measurement for a Rule Classifying SMTP Traffic

To enable volume measurement on the application layer for a term in a deep inspection rule classifying Simple Mail Transfer Protocol (SMTP) traffic, include the following statement:

```
Ericsson(config)# epg pgw service-identification smtp-rule
<rule-name> term <term-id> then
   aggregated-volume application
```

3.1.1.9 Configure Application Layer Volume Measurement for a Rule Classifying TFTP Traffic

To enable volume measurement on the application layer for a term in a deep inspection rule classifying Trivial File Transfer Protocol (TFTP) traffic, include the following statement:

```
Ericsson(config)# epg pgw service-identification tftp-rule
<rule-name> term <term-id> then
   aggregated-volume application
```

3.1.2 Exclude Retransmitted Packets from Measured Volume

Note: Excluding retransmitted packets from the measured volume is resource-consuming and can have an impact on the capacity and performance of the EPG.

To exclude retransmitted TCP packets from the measured volume, include the following statement:

```
Ericsson(config)# epg pgw service-set service-set-name service-identification t
   no-volume-reporting
```

To exclude duplicated TCP ACK packets (except disordered duplicated TCP ACK) from the measured volume, include the following statement:

```
Ericsson(config)# epg pgw service-set service-set-name service-identification t
   no-volume-reporting
```

3.1.3 Exclude Fragmented Packet IP Headers from Measured Volume

To exclude IP headers of fragmented packets from the measured volume, include the following statement:

```
Ericsson(config)# epg pgw service-set <service-set-name> serv
ice-identification signaling-classification
   ip-fragment-header-no-reporting
```

3.2 Configure Volume Reporting

For detailed information on the available volume reporting levels, refer to Charging Methods.

The following subsections provide instructions for configuring the reporting levels available for volume reporting.

3.2.1 Configure Bearer Level Volume Reporting

Volume is by default reported on bearer level by the GGSN and SGW, and optionally by the PGW.

For detailed information on configuring bearer level volume reporting for the PGW, refer to Offline Charging Configuration.

3.2.2 Configure RG Level Volume Reporting

Volume is by default reported on RG level if SACC is applied.

For detailed information on configuring RG level volume reporting, refer to Offline Charging Configuration.

3.2.3 Configure SI Level Volume Reporting

Volume can be reported on SI level by configuring SI level reporting on global level or per SI on rule space level.

For detailed information on configuring offline SI level volume reporting, refer to Offline Charging Configuration.

For detailed information on configuring online SI level volume reporting, refer to Credit Control Configuration.

3.2.4 Configure URI Level Volume Reporting

Note: URI tracking and URI level volume reporting are resource-consuming and can have an impact on the capacity and performance of the EPG.

To enable volume reporting on URI level, URI tracking must be configured for the applicable Packet Inspection and Service Classification (PISC) rules and URI level reporting with the attributes `volume` and `identifier` must be configured as record extension attributes.

For detailed information on configuring URI tracking, refer to Offline Charging Configuration.

For detailed information on configuring URI level volume reporting, refer to Offline Charging Configuration.

3.2.5 Configure IP Flow Level Volume Reporting

By activating IP flow level volume reporting for offline charging, additional information is reported per IP flow identified by the 5-tuple. For detailed information, refer to Charging Methods.

The maximum number of IP flows to be reported in a CDR can be configured. For detailed information on configuring IP flow level volume reporting, refer to Offline Charging Configuration.

To report a URL domain for IP flow level volume reporting, make sure that the following conditions are met:

— A header rule must be configured with the highest priority to capture all HTTP traffic, refer to PISC Configuration.

— A DPI rule must be associated with this header rule, refer to PISC Configuration. This DPI rule is configured not to match any condition.

By meeting these conditions, the EPG performs HTTP level analysis and packet data extraction without classifying packets into a service.

3.2.6 Configure Transaction Level Volume Reporting

Volume can be reported per RG or SI for each transaction identified by specific classification rules.

For detailed information on configuring transaction level volume reporting for Rf-based offline charging, refer to Offline Charging Configuration.

4 Configure Time-Based Charging

Time-based charging is an optional licensed feature in the EPG available for the SACC solution, and is disabled by default. To enable time-based charging in the EPG, a license must be purchased from Ericsson.

For information on purchasing licenses and enabling licensed features, refer to Software License Management or contact your local Ericsson support.

Time, that is, usage in number of seconds, can be measured and reported on RG level. Optionally, time and volume can be measured and reported in envelopes of absolute time. Time measurement and reporting is disabled by default.

4.1 Configure Time Measurement

The following subsections provide detailed instructions for configuring RG clusters, and the available time measurement methods and parameters.

4.1.1 Configure an RG Cluster

To add an RG or a consecutive range of RGs separated by `-` to an RG cluster, include the following statement:

```
Ericsson(config)# epg pgw rule-space <rule-space-name> time-b
ased-charging rating-group-cluster <cluster-id>
   rating-group (<rating-group-id> | <rating-group-
id>-<rating-group-id>)
```

The cluster ID must be a number from 1 through 4095. Up to 256 RGs can be associated with a cluster.

4.1.2 Configure the Time Measurement Method

Duration is the default time measurement method. This method is used for service-context 3GPP Gy (3Gy) and Ericsson Gy (EGy).

The `inactivity` statement corresponds to the consecutive active periods - inactivity not included time measurement method and the `inactivity-included` statement corresponds to the consecutive active periods - inactivity included time measurement method. Both of these time measurement methods and the active periods time measurement method are used only for service-context EGy.

To configure the time measurement method for an RG cluster, include the following statement:

```
Ericsson(config)# epg pgw rule-space <rule-space-name> time-bas
ed-charging rating-group-cluster <cluster-id> measurement
   method (inactivity | inactivity-included | durat
ion | active-periods)
```

To configure the time measurement method for RGs not belonging to an RG cluster, include the following statement:

```
Ericsson(config)# epg pgw rule-space <rule-space-name
> time-based-charging measurement
   method (inactivity | inactivity-included | durat
ion | active-periods)
```

4.1.3 Configure Time Measurement Resolution

To configure the time measurement resolution for an RG cluster, include the following statement:

```
Ericsson(config)# epg pgw rule-space <rule-space-name> time-bas
ed-charging rating-group-cluster <cluster-id> measurement
   resolution <seconds>
```

To configure the time measurement resolution for RGs not belonging to an RG cluster, include the following statement:

```
Ericsson(config)# epg pgw rule-space <rule-space-name
> time-based-charging measurement
   resolution <seconds>
```

The default time measurement resolution is 1 second. The value range is 1–86,400 seconds.

4.1.4 Configure Time Measurement Inactivity

To configure the time measurement inactivity for an RG cluster, include the following statement:

```
Ericsson(config)# epg pgw rule-space <rule-space-name> time-bas
ed-charging rating-group-cluster <cluster-id> measurement
   inactivity <seconds>
```

To configure the time measurement inactivity for RGs not belonging to an RG cluster, include the following statement:

```
Ericsson(config)# epg pgw rule-space <rule-space-name
> time-based-charging measurement
   inactivity <seconds>
```

The default value is 60 seconds. The range is 1–86,400 seconds.

4.1.5 Configure Time Envelope Measurement and Reporting

To configure time envelope measurement and reporting for an RG cluster, include the following statement:

```
Ericsson(config)# epg pgw rule-space <rule-space-name> time-bas
ed-charging rating-group-cluster <cluster-id> measurement
   reporting (no-reporting | timestamp | timestamp-and-volume)
```

To configure time envelope measurement and reporting for RGs not belonging to an RG cluster, include the following statement:

```
Ericsson(config)# epg pgw rule-space <rule-space-name
> time-based-charging measurement
   reporting (no-reporting | timestamp | timestamp-and-volume)
```

4.2 Configure Time Reporting

For detailed information on the available time reporting levels, refer to Charging Methods.

The following subsection provides information on configuring the reporting level used for time reporting.

4.2.1 Configure RG Level Time Reporting

To enable time reporting on RG level, time measurement must be enabled.

For detailed information on configuring RG level reporting, refer to Offline Charging Configuration.

5 Configure Event-Based Charging

Event-based charging is an optional licensed feature in the EPG available for the SACC solution, and is disabled by default. To enable event-based charging in the EPG, a license must be purchased from Ericsson.

For information on purchasing licenses and enabling licensed features, refer to Software License Management or contact your local Ericsson support.

Events, that is, usage measured in service-specific units, can be tracked and reported on RG level or URI level. Event measurement and reporting is disabled by default.

5.1 Configure Event Tracking

Note: Event tracking is resource-consuming and can have an impact on the capacity and performance of the EPG.

The following subsections describe how to activate event tracking for each type of deep inspection rule supporting event-based charging.

5.1.1 Activate Event Tracking for a Rule Classifying FTP Traffic

To activate event tracking for a term in a deep inspection rule classifying File Transfer Protocol (FTP) traffic, include the following statement:

```
Ericsson(config)# epg pgw service-identification ftp-rule
<rule-name> term <term-id> then
   activate-event-tracking
```

5.1.2 Activate Event Tracking for a Rule Classifying HTTP or WSP Traffic

Events can be configured to trigger at the start of a transaction, at the completion of a transaction, when receiving HTTP responses, or any combination.

To activate event tracking for a term in a deep inspection rule classifying Hypertext Transfer Protocol (HTTP) traffic, include the following statement:

```
Ericsson(config)# epg pgw service-identification http-wsp-rule
<rule-name> term <term-id> then activate-event-tracking
   track (complete | start | response)
```

If event tracking is configured as `response`, response codes must be configured for HTTP as a match condition in the same HTTP-WSP rule. For more information on how to configure packet matching based on HTTP response codes, refer to PISC Configuration.

To activate event tracking for a term in a deep inspection rule classifying Wireless Session Protocol (WSP) traffic, include the following statement:

```
Ericsson(config)# epg pgw service-identification http-wsp-rule
<rule-name> term <term-id> then activate-event-tracking
   track (complete | response | start)
```

To activate the event tracking for any combination of `complete`, `start`, and `response`, the corresponding options can be included in a single step or separate steps.

For example, either of the following configurations can be used to activate event tracking for the combination of `start` and `response`:

— A single step:

```
Ericsson(config)# epg pgw service-identification http-wsp-rule
<rule-name> term <term-id> then activate-event-tracking
   track [ start response ]
```

— Separate steps:

1
```
Ericsson(config)# epg pgw service-identification http-wsp-r
ule <rule-name> term <term-id> then activate-event-tracking
   track start
```

2
```
Ericsson(config)# epg pgw service-identification http-wsp-r
ule <rule-name> term <term-id> then activate-event-tracking
   track response
```

Note: When changing the existing configuration of activating event tracking, make sure to use the `show-config` command to show which options have been configured so that the configuration change works as expected. For example, if `start` needs to be replaced by `response`, use the `show-config` command to check if `start` has been configured. If configured, issue `no track start` to remove `start` and then configure `track response`.

To classify trailing HTTP packets into the appropriate header rule instead of the deep inspection rule where event tracking is activated, include the following statement:

```
Ericsson(config)# epg pgw service-identification trailing-http-packets
   classified-to-header-rule
```

5.1.3 Activate Event Tracking for a Rule Classifying MMS Traffic

To activate event tracking for a term in a deep inspection rule classifying Multimedia Messaging System (MMS) traffic, include the following statement:

```
Ericsson(config)# epg pgw service-identification http-wsp-rule
<rule-name> term <term-id> then
   activate-event-tracking
```

Note: Event tracking cannot be activated for a term that is configured to match MMS notification messages, forward messages, acknowledge messages, or read-report messages.

To classify trailing MMS packets into the appropriate header rule instead of the deep inspection rule where event tracking is activated, include the following statement:

```
Ericsson(config)# epg pgw service-identification trailing-mms-packets
   classified-to-header-rule
```

5.1.4 Activate Event Tracking for a Rule Classifying POP3 Traffic

To activate event tracking for a term in a deep inspection rule classifying Post Office Protocol version 3 (POP3) traffic, include the following statement:

```
Ericsson(config)# epg pgw service-identification pop3-rule
<rule-name> term <term-id> then
   activate-event-tracking
```

5.1.5 Activate Event Tracking for a Rule Classifying RTSP Traffic

To activate event tracking for a term in a deep inspection rule classifying Real Time Streaming Protocol (RTSP) traffic, include the following statement:

```
Ericsson(config)# epg pgw service-identification rtsp-rule
<rule-name> term <term-id> then
   activate-event-tracking
```

5.1.6 Activate Event Tracking for a Rule Classifying SIP Traffic

To activate event tracking for a term in a deep inspection rule classifying Session Initiation Protocol (SIP) traffic, include the following statement:

```
Ericsson(config)# epg pgw service-identification sip-rule
<rule-name> term <term-id> then
   activate-event-tracking
```

Note: It is not possible to activate event tracking for a term that is configured to match traffic based on the contents of Via headers or response code.

5.1.7 Activate Event Tracking for a Rule Classifying SMTP Traffic

To activate event tracking for a term in a deep inspection rule classifying Simple Mail Transfer Protocol (SMTP) traffic, include the following statement:

```
Ericsson(config)# epg pgw service-identification smtp-rule
<rule-name> term <term-id> then
   activate-event-tracking
```

To classify trailing SMTP packets into the appropriate header rule instead of the deep inspection rule where event tracking is activated, include the following statement:

```
Ericsson(config)# epg pgw service-identification trailing-smtp-packets
   classified-to-header-rule
```

Note:

- SMTP event tracking is not compatible with SMTP content enrichment.
- Event tracking cannot be used in rules where the operation Mail is configured explicitly as a match condition.

5.2 Configure Event Reporting

For detailed information on the available event reporting levels, refer to Charging Methods.

The following subsection provides information on configuring the reporting level used for event reporting.

5.2.1 Configure RG Level Event Reporting

To enable event reporting on RG level, event tracking must be configured for the applicable PISC rules.

For detailed information on configuring RG level reporting, refer to Offline Charging Configuration.

5.2.2 Configure URI Level Event Reporting

Note: URI tracking and URI level event reporting are resource-consuming and can have an impact on the capacity and performance of the EPG.

To enable event reporting on URI level, event tracking must be configured for the applicable PISC rules and URI level reporting with the attribute `count` or `timestamp` must be configured as record extension attributes.

For detailed information on configuring URI tracking, refer to Offline Charging Configuration.

For detailed information on configuring URI level reporting, refer to Offline Charging Configuration.