

Application Detection and Control (Gx)

Ericsson Service-Aware Policy Controller

FACILITY DESCRIPTION

Copyright

© Ericsson España, S.A. 2017. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

All trademarks mentioned herein are the property of their respective owners. These are shown in the document Trademark Information.

Abstract

This document describes the Application Detection and Control function provided by the SAPC.



Contents

1	Application Detection and Control Introduction	1
1.1	Document Purpose and Scope	1
1.2	Concepts	1
2	ADC Function	3
2.1	ADC Overview	3
2.2	Service Access Control	5
2.3	ADC Redirection Control	5
2.4	ADC Mute Notification Control	6
2.5	Application Detection Reporting	6
3	ADC Network Deployments	9
4	ADC Traffic Cases	11
4.1	QoS Control Based on Application Traffic Detection	11
4.2	ADC Redirection Control	15
4.3	ADC Mute Notification	16
4.4	ADC Error Handling	18
	Reference List	21





1 Application Detection and Control Introduction

1.1 Document Purpose and Scope

This document describes the Application Detection and Control (ADC) function provided by the SAPC.

1.2 Concepts

Application detection filter

Logic used to detect packets generated by an application based on extended inspection of these packets, such as header or payload information, and dynamics of packet flows. The logic is entirely internal to a PCEF enhanced with ADC.

Application identifier

An identifier, referring to a specific application detection filter.

PCC Rule

The set of information enabling the detection of application traffic and providing parameters for Policy and Charging Control (PCC).

Policy

The set of rules that implies a decision about a resource and that triggers certain behavior in the network.

Rule

It contains a condition formula that is evaluated to permit or deny the authorization to a resource or to return an output attribute.

Service Data Flow

An aggregate set of IP flows.

Service Data Flow Filter

A set of filter parameters used to identify one or more of the IP flows constituting a service data flow. At least the following means for the IP flow identification are supported: source and destination IP address+port, protocol.





2 ADC Function

2.1 ADC Overview

The SAPC supporting ADC function instructs the PCEF to detect and report application start and stop events. Based on this report, the SAPC makes policy decisions and sends enforcement actions to the PCEF.

This function enables the operator to have real-time control over the services of the users. The operator can take the following immediate actions based on application status:

- Change of service authorization
- QoS modification
- Bandwidth management
- Service charging control
- User notifications

This function also supports redirecting the detected applications to another destination, or muting notifications to the SAPC for specific applications.

- For details on application redirection, see Section 2.3 on page 5.
- For details on mute notification, see Section 2.4 on page 5.

This functionality is provided through the Gx interface. The SAPC can enable PCEFs for ADC support. The PCEF detects the application traffic using static or preconfigured PCC rules enhanced with ADC.

- A static PCC rule enhanced with ADC is a PCC rule locally configured in the PCEF and dynamically activated or deactivated by the SAPC. Its Traffic Detection Function (TDF) application identifier (used to reference an application detection filter, which is predefined in the PCEF), redirection, and mute notification information are locally configured in the PCEF.
- A preconfigured PCC rule enhanced with ADC is a PCC rule predefined in the SAPC. Apart from rest of data of a PCC rule, it includes TDF application identifier, redirection and mute notification information configured in the SAPC, but does not include Service Data Flow Filters.

Figure 1 illustrates an example of QoS upgrade based on application detection. The SAPC makes QoS decisions depending on application events reported by the PCEF.

Use Case Example

Application Detection and Control

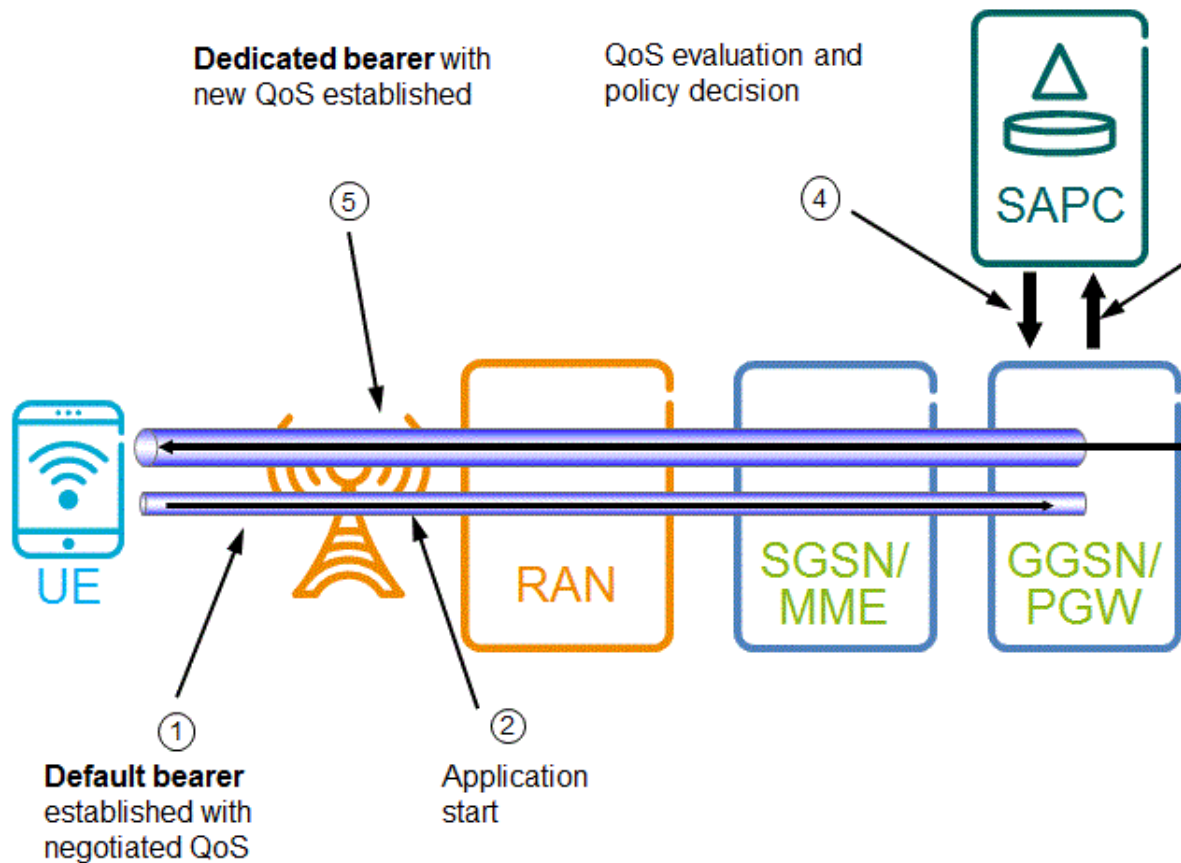


Figure 1 QoS upgrade based on Application Detection start

- 1 The default bearer is established with negotiated QoS.
- 2 The UE starts the application traffic.
- 3 The GGSN (PGW) detects and reports an application start event together with the flow information to the SAPC.
- 4 The SAPC evaluates the QoS and sends new QoS to the GGSN (PGW).
- 5 The dedicated bearer with new QoS is established.
- 6 The End-to-End application traffic is established.



2.2 Service Access Control

The SAPC authorizes PCC rules enhanced with ADC together with other PCC rules by evaluating Access and Charging Control, as described in [Access and Charging Control \(Gx\)](#), including:

- Service Selection
- Service Authorization
- Service Qualification

2.3 ADC Redirection Control

The SAPC can instruct the PCEF to redirect the uplink traffic of specific applications to another destination based on conditions such as Time of Day (ToD). The SAPC can also disable the redirection of these applications.

The SAPC sends redirection information for preconfigured PCC rules enhanced with ADC including type and address of a redirection server and an indication to enable or disable redirection. The type of server address can be IPv4 address, IPv6 address, URL, or SIP URI.

If the redirection server address is not provided by the SAPC, the server address preconfigured in the PCEF for this PCC rule is used instead.

The SAPC selects the redirection profile for a PCC rule enhanced with ADC by evaluating ADC Redirection policies according to the following precedence allocation:

- 1 Subject policy locator.
- 2 Subject group policy locator. All the active subscriber groups are considered.

Therefore configure Dynamic Group Selection policies to evaluate only the desired subscriber group policies.

- 3 Global policy locator.

In case there are conflicts among the rules within a policy, the result for the policy depends on the rule combining algorithm configured. See [Solving Policies Conflicts](#) section in [Subscription and Policy Management](#) for further information.

If there are no configured policies or the policies are not fulfilled, the SAPC obtains the ADC Redirection information provisioned statically for the service.

If ADC Redirection cannot be selected either dynamically or statically, the SAPC does not request to redirect the traffic.



2.4 ADC Mute Notification Control

The SAPC can instruct the PCEF to mute application notifications associated with preconfigured PCC rules enhanced with ADC. It can be used if the enforcement action to be applied for the application is access control or bandwidth limitation to save event notifications.

ADC Mute Notification can only be set at PCC rule installation and it cannot be updated during the lifetime of the PCC rule.

The SAPC selects the mute status for PCC rules enhanced with ADC by evaluating ADC Mute Notification policies according to the following precedence allocation:

- 1 Subject policy locator.
- 2 Subject group policy locator. All the active subscriber groups are considered.

Therefore configure Dynamic Group Selection policies to evaluate only the desired subscriber group policies.

- 3 Global policy locator.

In case there are conflicts among the rules within a policy, the result for the policy depends on the rule combining algorithm configured. See Solving Policies Conflicts section in [Subscription and Policy Management](#) for further information.

If there are no configured policies or the policies are not fulfilled, the SAPC obtains the mute status provisioned statically for the service.

If ADC Mute Notification cannot be selected either dynamically or statically, the SAPC does not request the PCEF to mute the application notifications.

2.5 Application Detection Reporting

The PCEF enhanced with ADC performs the application reporting if the following conditions are met:

- The SAPC subscribes to application start and application stop event triggers, which indicate the start and stop of the application traffic.
- The SAPC activates a static PCC rule with ADC configured in the PCEF, or the SAPC installs a preconfigured PCC rule with ADC to the PCEF.
- The PCC rule enhanced with ADC has not ADC Mute Notification information enabled.

The PCEF reports the application status at application level or service data flow level, by sending the application start and stop events and application detection information to the SAPC.



- If the reporting is at application level, the application detection information only includes a TDF application identifier used to reference the corresponding application.
- If the reporting is at service data flow level, besides the TDF application identifier, the application detection information includes flow information along with the TDF application instance identifier. Each application may have several service data flows, and each TDF application instance identifier maps to an individual flow or a group of flows.

During the lifetime of a PCC rule enhanced with ADC, the SAPC expects that the application start and stop events are reported at the same level (application level or service data flow level). The SAPC uses the TDF application identifier and TDF application instance identifiers received in the start and stop notifications reported by the PCEF to keep track of application traffic status. The SAPC does not handle flow information for PCC rules enhanced with ADC. It is the PCEF which knows about the flow information corresponding to the application or service traffic reported.

Note: The PCEF reports application status to the SAPC, even if the application traffic is discarded in the PCEF.





3 ADC Network Deployments

The SAPC can provide Application and Detection Control in the following network deployments:

- Ericsson EPG and Non-Ericsson PCEF supporting ADC feature.
- Multiple PCEFs deployments.

Note: In a multiple Gx scenario where an IP-CAN session is controlled by several PCEFs, ADC support can be configured for more than one PCEF. But each PCEF reports application status and performs enforcement independently: for applications detected by one PCEF, the SAPC does not reauthorize the IP-CAN session on the other PCEFs.





4 ADC Traffic Cases

This chapter explains the interface (Gx) involved in the Application Detection and Control function and the traffic interactions between the network functions involved. For a detailed description of the Gx interface, see the corresponding interface description.

The preconditions to all ADC traffic cases are as follows:

- Same preconditions as Access and Charging Control described in *Access and Charging Control (Gx)* apply to ADC function.
- ADC control is enabled for the connected PCEF.
- ADC license is active, otherwise the SAPC does not download any PCC rule enhanced with ADC or accept any traffic detection information received from the PCEF regarding these PCC rules enhanced with ADC.
- Related ADC event-triggers are configured in the SAPC.

4.1 QoS Control Based on Application Traffic Detection

This traffic case shows an example of QoS control based on application traffic detection for PCC rules enhanced with ADC in an EPS deployment.

In this example, the QoS profile of the default bearer is upgraded/downgraded when PCEF detects and reports the application traffic start/stop of a previously installed PCC rule enhanced with ADC.

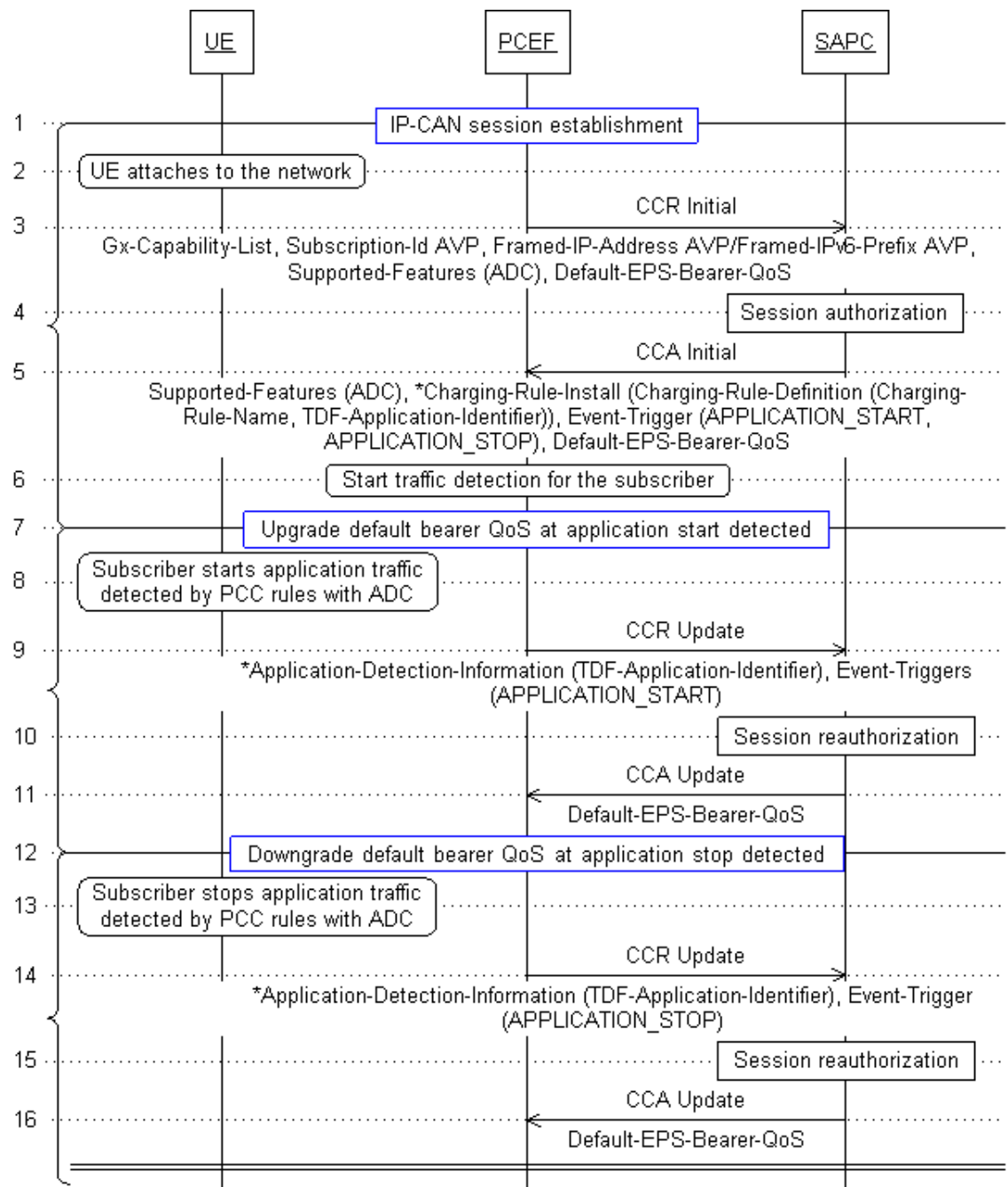


Figure 2 QoS Control based on Application Traffic Detection

IP-CAN session establishment

- 2. The UE attaches to the network, and the PCEF receives a notification about this situation.



- 3. The PCEF sends a CCR-Initial to the SAPC with the ADC bit set in the Supported-Features AVP, notifying that it supports ADC.
- 4. The SAPC performs session authorization including evaluation of Access and Charging Control, ADC Redirection Control, and ADC Mute Notification Control.

The SAPC decides to install preconfigured PCC rules enhanced with ADC and to activate static PCC rules with ADC to the PCEF.

Note: For the PCC rule precedence calculation, the SAPC does not increment the dynamic part of the precedence of the PCC rules enhanced with ADC as flow information is implicit in the TDF application identifier of the PCC rule with ADC.

For more information regarding precedence calculation, refer to *Access and Charging Control (Gx)*.

- 5. The SAPC answers with a CCA-Initial message to the PCEF including the following AVPs:

- Supported-Features AVP with the ADC bit (6) set.

Note: If the ADC bit is not received in the Supported-Features AVP, the ADC license is not active or ADC support is not configured for the PCEF, the SAPC answers back with the ADC bit unset, meaning ADC function is not enabled for the session.

- Charging-Rule-Install AVP including the Charging-Rule-Name or Charging-Rule-Base-Name AVPs for static PCC rules enhanced with ADC, and the Charging-Rule-Definition AVP with the following additional AVPs for preconfigured PCC rules enhanced with ADC:

- The TDF-Application-Identifier AVP that identifies the application for traffic detection.

Note: If TDF-Application-Identifier AVP is included, then no Flow-Information AVP shall be included under the same Charging-Rule-Definition AVP.

For static PCC rules, the TDF-Application-Identifier AVP is never downloaded to the PCEF.

- The Redirect-Information AVP if any ADC Redirection profile is statically or dynamically provisioned for the service.
- The Mute-Notification AVP if ADC Mute Notification “muted” value is statically or dynamically provisioned for the service.
- The Event-Triggers AVP including the APPLICATION_START and APPLICATION_STOP events.



- The Default-EPS-Bearer-QoS AVP with the QoS to apply to the default bearer.
- 6. The PCEF applies the downloaded QoS parameters to the default bearer and starts detecting traffic.

Upgrade default bearer QoS at application start detected

- 8. The subscriber starts application traffic that is to be detected by the PCC rule enhanced with ADC.
- 9. The PCEF reports the application traffic start event by sending a CCR-Update message with:
 - The Event-Triggers AVP including the APPLICATION_START event.
 - The Application-Detection-Information AVP including the TDF-Application-Identifier AVP.

Note: When the service data flow descriptions are deducible, Application-Detection-Information AVP includes also the Flow-Information AVP for the detected application.

If the Flow-Information AVP is included, the TDF-Application-Instance-Identifier AVP is also included. In any other case, the SAPC returns an error as described in Section 4.4.2 on page 19.

- 10. The SAPC reauthorizes the session and as result the QoS for the default bearer is upgraded.
- 11. The SAPC answers with a CCA-Update message to the PCEF, with the Default-EPS-Bearer-QoS AVP containing the upgraded QCI or ARP.

Downgrade default bearer QoS at application stop detected

- 13. The subscriber stops the application traffic detected by the PCC rule enhanced with ADC.
- 14. The PCEF reports the application stop event using a CCR-Update with:
 - The Event-Triggers AVP including the APPLICATION_STOP event.
 - The Application-Detection-Information AVP including the TDF-Application-Identifier AVP.

Note: If an application start event was received with the TDF-Application-Instance-Identifier AVP, the corresponding stop event should also include the TDF-Application-Instance-Identifier AVP. In any other case, the SAPC returns an error as described in Section 4.4.2 on page 19.



- 15. The SAPC reevaluates the data to be applied to the subscriber and as result the QoS for the default bearer is downgraded.
- 16. The SAPC answers with a CCA-Update message to the PCEF, with the Default-EPS-Bearer-QoS AVP with the downgraded QCI or ARP.

4.2 ADC Redirection Control

This traffic case shows an example of ADC Redirection Control based on a ToD condition where the SAPC controls time.

In this example ADC Redirection Control is dynamically selected only during a specific range of time. The SAPC triggers the reauthorization of the session when ADC Redirection is to be applied.

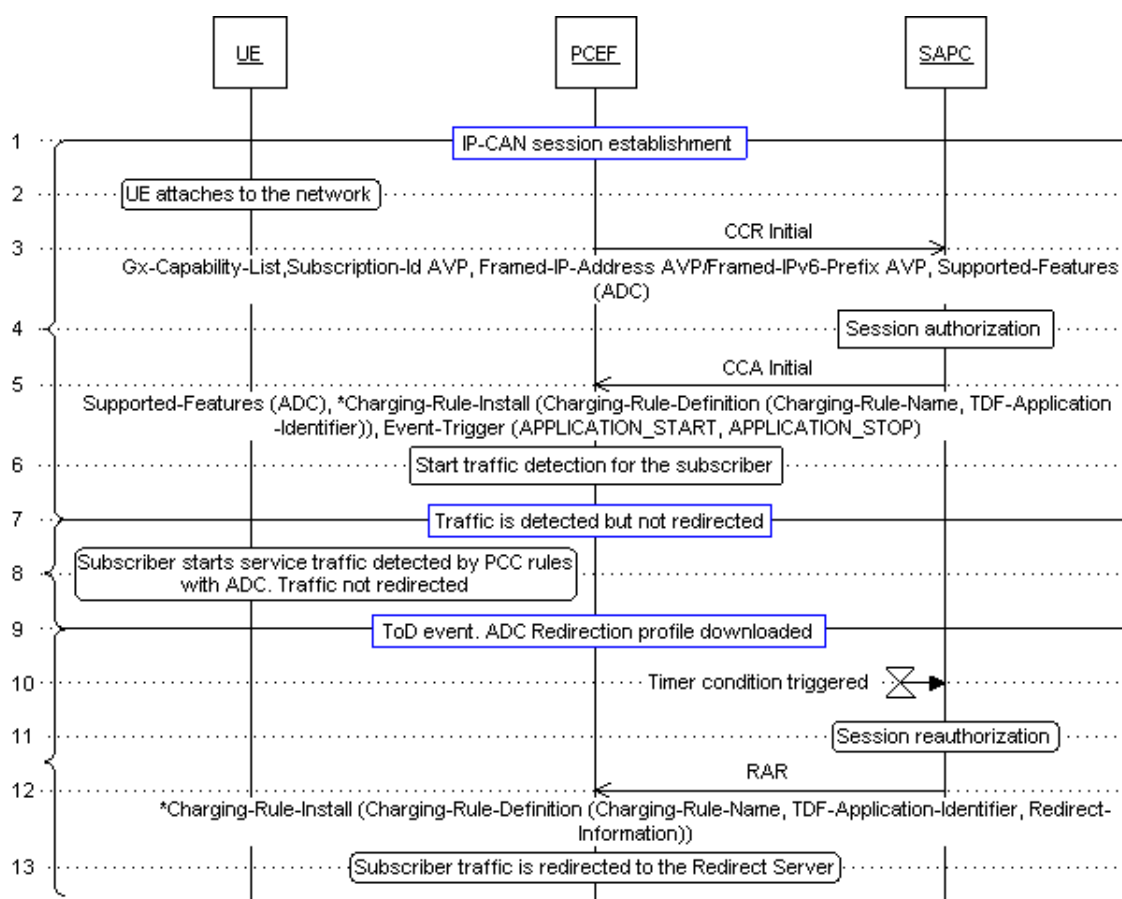


Figure 3 ADC Redirection Control based on ToD conditions

IP-CAN session establishment

- 1-6. The steps are the same to steps 1–6 in Section 4.1 on page 11 except step 5:



In this case, the Charging-Rule-Definition AVP does not include the Redirect-Information AVP, as the time of day condition for ADC Redirection is not fulfilled at ADC Redirection policy evaluation.

Traffic is detected but not redirected

- 8. The subscriber starts service traffic that is detected by the PCC rules enhanced with ADC.

The application traffic is not redirected, because ADC Redirection profile is not applicable at that time of day, but PCEF may report application traffic start and application traffic stop independently of application traffic being redirected or not.

ToD event. ADC Redirect profile downloaded

- 10. The time at which the ToD event is to be triggered arrives.
- 11. The SAPC reauthorizes the session and determines to apply an ADC Redirection profile to the previously installed PCC rule enhanced with ADC.
- 12. The SAPC sends a RAR message to the PCEF with the Charging-Rule-Definition AVP containing the applicable Charging-Rule-Name, TDF-Application-Identifier, and Redirect-Information AVP including:
 - Redirect-Support AVP set to REDIRECTION_ENABLED value.
 - Redirect-Address-Type AVP.
 - Redirect-Server-Address AVP.

Note: When the Redirect-Server-Address AVP is not sent, the Redirect-Server-Address value configured in the PCEF is used. In case the Redirect-Server-Address value is neither configured in the PCEF, the PCEF reports an error to the SAPC. For further details, see Section 4.4.1 on page 18.

Subscriber traffic is redirected to the Redirect Server

- 13. From now on, the service traffic of PCC rule enhanced with ADC is redirected to the destination server where information about the accessed service may be offered.

4.3 ADC Mute Notification

This traffic case shows how ADC Mute Notification Control can be used when it is not needed to report traffic start/stop towards the SAPC, for example if it is only needed to perform bandwidth enforcement for the application.



In this example, the preconfigured PCC rule enhanced with ADC is downloaded with MUTE_REQUIRED value, so the PCEF does not report any service traffic start or stop for the PCC rule enhanced with ADC.

Note: ADC Mute Notification value is persistent during the life of the PCC rule enhanced with ADC, so Mute-Notification AVP is only sent in first PCC rule installation.

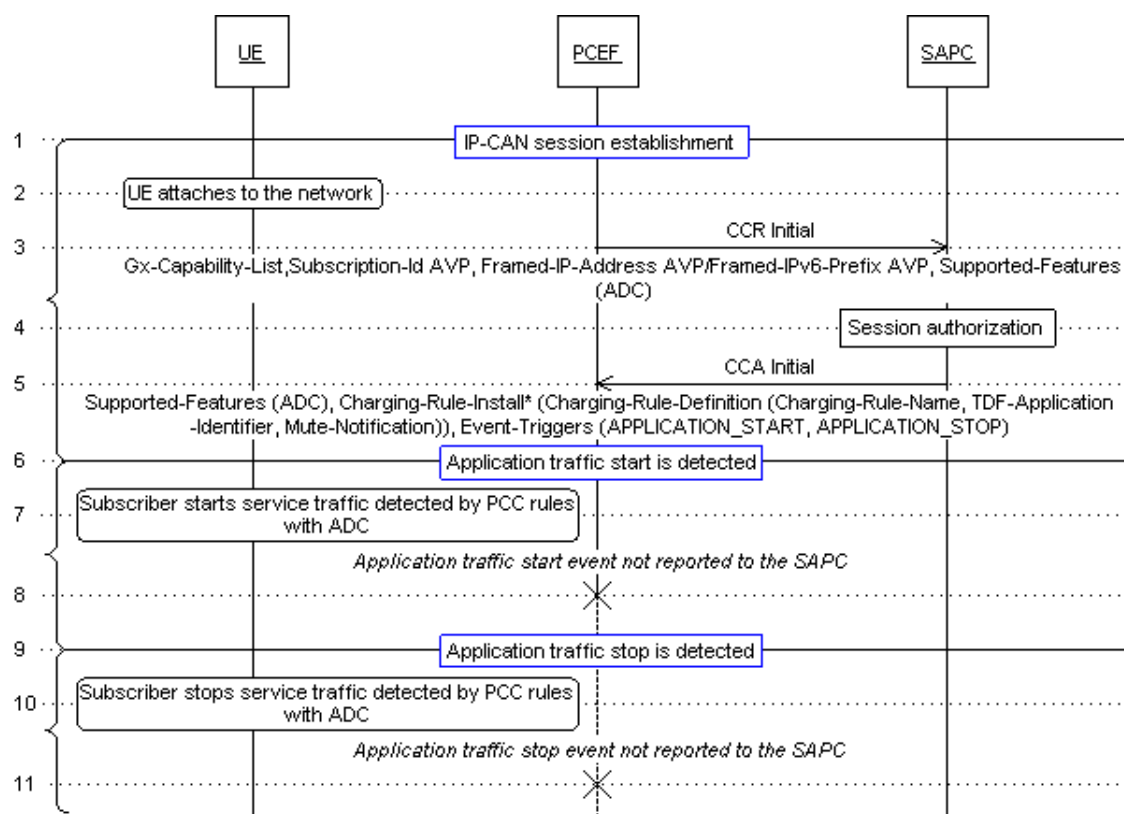


Figure 4 ADC Mute Notification Control

IP-CAN session establishment

- 1-5. The steps are the same to steps 1–5 in Section 4.1 on page 11 except step 5:

The Charging-Rule-Definition AVP includes the Mute-Notification AVP with MUTE_REQUIRED value as ADC Mute Notification profile is static or dynamic configured with “muted” value for the service.

Application traffic start is detected

- 7. The subscriber starts service traffic detected by the PCC rule enhanced with ADC.

- 8. The PCEF does not report the corresponding application traffic start to the SAPC as mute notification was requested.

Application traffic stop is detected

- 10. The subscriber stops service traffic detected by the PCC rule enhanced with ADC.
- 11. The PCEF does not report application stop to the SAPC as mute notification was requested.

4.4 ADC Error Handling

4.4.1 PCC Rule Error Handling

This traffic case shows an example of error handling in the installation of PCC rules enhanced with ADC. This is an extension of the PCC Rule Error Handling described in *Access and Charging Control (Gx)*.

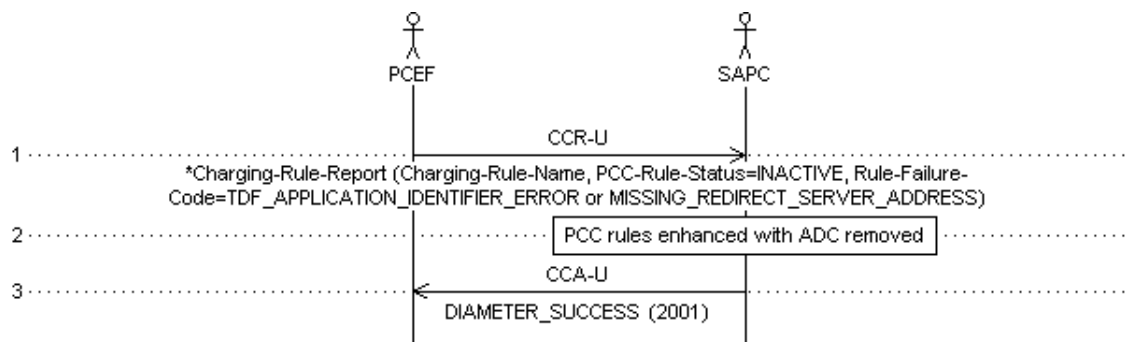


Figure 5 PCC Rule Error Handling

1. The SAPC receives a Gx CCR-Update message from the PCEF indicating that the previous installation of PCC rules enhanced with ADC has failed. The CCR-Update includes the Charging-Rule-Report AVP with the following AVPs:
 - The Charging-Rule-Name AVP for the affected PCC rules.
 - The PCC-Rule-Status AVP containing the value INACTIVE to indicate an error in the installation of the PCC rule.
 - The Rule-Failure-Code AVP containing the failure reason. It includes one of the following values:
 - TDF_APPLICATION_IDENTIFIER_ERROR (14), indicating that the TDF-Application-Identifier is invalid, unknown, or not applicable to the application required for detection.



- MISSING_REDIRECT_SERVER_ADDRESS (18), indicating no valid Redirect Server Address within the Redirect-Server-Address AVP is provided by the SAPC or not configured at the PCEF.
2. The SAPC updates the session information by removing the PCC rules enhanced with ADC and performs policy evaluation ignoring the affected PCC rules.

2: The SAPC updates the session information (removing the PCC rules affected) and performs policy evaluation ignoring the affected PCC rules.
 3. CCA-Update message is sent back to the PCEF.

4.4.2 Application Reporting Error Handling

Next table shows how the SAPC handles the errors when receiving a CCR-Update missing certain AVPs.

Table 1 Application Reporting Error Handling

Error Condition	Action	Code
The SAPC receives a CCR-U for an application start event with the TDF-Application-Instance-Identifier AVP, and the CCR-U for the corresponding stop event does not have it. ⁽¹⁾	The SAPC returns a CCA indicating an error.	Result-Code AVP set to DIAMETER_MISSING_AVP (5005)
The SAPC receive a CCR-U for an application start or stop event trigger but not Application-Detection-Information AVP or with Application-Detection-Information AVP but not TDF-Application-Identifier AVP inside.	The SAPC returns a CCA indicating an error.	Result-Code AVP set to DIAMETER_MISSING_AVP (5005)
The SAPC receive a CCR-U for an application start or stop event trigger with Application-Detection-Information AVP including a Flow-Information AVP, but no corresponding TDF-Application-Instance-Identifier AVP.	The SAPC returns a CCA indicating an error.	Result-Code AVP set to DIAMETER_MISSING_AVP (5005)

(1) In case the SAPC receives a CCR-U for an application start event without the TDF-Application-Instance-Identifier AVP, but the corresponding stop event has it, the SAPC will ignore application stop event trigger but reauthorize the session.





Reference List

Ericsson Documents

- [1] Access and Charging Control (Gx)
- [2] Subscription and Policy Management