

# Dynamic Policy Control (Rx)

## 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 Dynamic Policy Control functionality provided by the SAPC.



# Contents

<b>1</b>	<b>Dynamic Policy Control Introduction</b>	<b>1</b>
<b>2</b>	<b>Dynamic Policy Control Function</b>	<b>1</b>
2.1	Dynamic Policy Control Overview	1
2.2	Negotiation of Rx Interface Version and Supported Features	4
2.3	Session Binding	5
2.4	Classification of Dynamic Services	7
2.5	Authorization of Dynamic Services	9
2.6	Qualification of Dynamic Services	11
2.6.1	Allocation of QoS Information to Dynamic Services	12
2.6.2	Allocation of Charging Parameters to Dynamic Services	13
2.7	Generation of Dynamic PCC Rules	14
2.8	IP-CAN Session Reauthorization	19
2.9	Notification of Bearer Events to the AF	21
2.9.1	IP-CAN Session Termination	21
2.9.2	Service Data Flow Deactivation	21
2.9.3	Successful Resources Allocation	22
2.9.4	Network Location Information	23
2.10	IMS Related PCC Procedures over Rx	24
2.10.1	Gating Control	24
2.10.2	Support for SIP Forking	24
2.10.3	Single Radio Voice Call Continuity (SRVCC)	26
2.11	Handling of Race Conditions Related to Multiple AF Requests	27
<b>3</b>	<b>Dynamic Policy Control Network Deployments</b>	<b>29</b>
<b>4</b>	<b>Dynamic Policy Control Traffic Cases</b>	<b>29</b>
4.1	AF Session Lifetime	30
4.1.1	AF Session Establishment	30
4.1.2	AF Session Modification	33
4.1.3	AF Session Termination	36
4.2	Reauthorization of Dynamic Services	38
4.3	Notification of Bearer Events	40
4.3.1	Service Data Flow Deactivation	40
4.3.2	Successful Resources Allocation	42
4.3.3	Network Location Information (NetLoc)	44
4.4	IMS Related Procedures	58
4.4.1	SIP Forking	58
4.4.2	Single Radio Voice Call Continuity	61



4.5	Dynamic Policy Control Triggered by Application Service Detection	63
4.5.1	Dynamic QoS Control based on Detected Service	63
4.5.2	Deactivation of IP-CAN Session on Detection of Tethering Traffic	66
4.6	Handling of Race Conditions Related to Multiple AF Requests	68
4.7	Dynamic Policy Control Error Handling	71
	<b>Reference List</b>	<b>75</b>



# 1 Dynamic Policy Control Introduction

This document describes the Dynamic Policy Control function of the SAPC.

This function provides Policy and Charging Control (PCC) differentiated per subscriber for services that are dynamically negotiated taking into account information received from the Application Function (AF) over the Rx interface.

## 2 Dynamic Policy Control Function

### 2.1 Dynamic Policy Control Overview

The SAPC Dynamic Policy Control functionality adheres to the architecture of the standardized PCRF function of the 3GPP PCC architecture, its defined policy control interfaces (Gx, Rx), and logical network elements (PCEF, AF). The AF provides session and service information to the SAPC. The SAPC makes authorization and policy decisions, and sends the appropriate PCC rules to the PCEF, by using the PCRF initiated IP-CAN session modification procedure. This provides a mechanism for the AF to adapt dynamically the service delivery in the transport plane to the required conditions.

When a subscriber wants to establish a session with an AF, such as the P-CSCF or a streaming server, application level signalling is started. Examples of application level signalling include using the Session Initiation Protocol (SIP) in the case of the P-CSCF or the Real Time Session Protocol (RTSP) in the case of a streaming server. The AF notifies the activation of a session using the Rx protocol, and includes dynamic session information. The SAPC then generates policy control and charging information, and installs the applicable PCC rules in the PCEF with the corresponding QoS parameters.

Depending on the capabilities of the network and the UE, the default bearer can be used to transport the service or a dedicated bearer can be established. If a dedicated bearer cannot be established, the default bearer is shared among all the services running on the IP-CAN session.

Dynamic Policy Control comprises the following functions:

- Negotiation of Rx interface version and features supported for the AF session
- Session binding: associate the AF session with an existing IP-CAN session
- Classification (identification) and authorization of dynamic services
- Generation of dynamic PCC rules

- Allocation of QoS and Charging parameters to the authorized dynamic services
- Re-evaluation of previous policy decisions taken for the IP-CAN session, which includes:
  - Allow or reject IP-CAN session access
  - List of static and preconfigured services that are authorized for the IP-CAN session
  - QoS and charging parameters allocated to services currently running in the IP-CAN session
  - QoS parameters allocated to the default IP-CAN bearer
- Provisioning and removal of PCC rules and default bearer QoS to the PCEF
- Notification of bearer events to the AF
- IMS related P-CSCF procedures, such as gating control, Single Radio Voice Call Continuity, and SIP forking support

There are different network scenarios where Dynamic Policy Control is applied, and some of the previous functions are only performed in particular network scenarios. The service information provided by the AF can include information such as the set of IP flows required to deliver the service, the type of media (for example, audio, video), the application identifier, the requested bandwidth. This information is used by the SAPC to identify, authorize, and control one or more dynamic services, according to the configured policies and conditions. However, dynamic PCC rules are only generated when the AF provides information about the IP flows required to deliver the service.

Figure 1 shows a high-level flow of the establishment of a dynamic service that makes use of the IP Multimedia Subsystem. In this case, the service delivery (for example, multimedia telephony) requires the establishment of dedicated bearers. During IMS session negotiation, the AF (P-CSCF) derives the service information and performs a resource allocation request towards the SAPC for the media being setup. The SAPC associates the received service data flows with an existing IP-CAN session and creates a set of policy rules for the media negotiated, which triggers the PGW to create a new dedicated bearer for the media type negotiated.

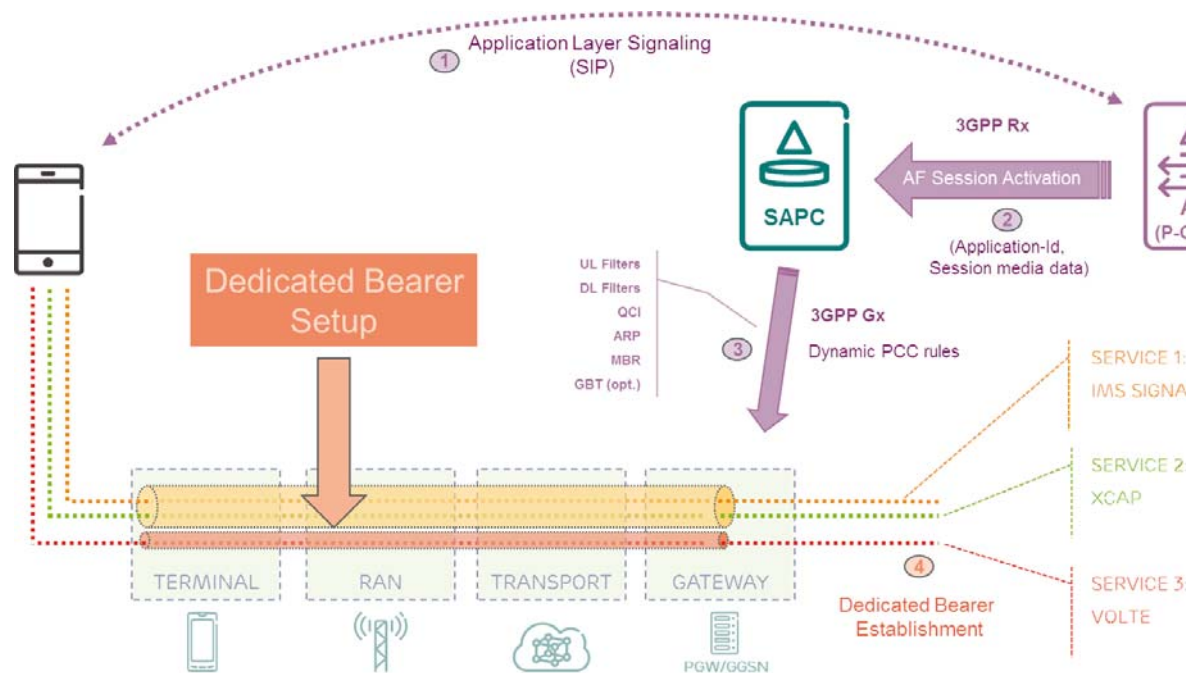


Figure 1 AF session establishment with session media data

In other network scenarios, the AF merely provides an application identifier over the Rx interface, and no specific information on the characteristics of the media session being established (session media data). This identifier is used by the SAPC to trigger the activation of a dynamic service, and to reevaluate the policy information associated with the services that are running on the IP-CAN session. As the IP flows required to deliver the service are not provided, the SAPC cannot generate dynamic PCC rules. Policy control is then performed by Service Access and Charging Control, and IP-CAN Bearer QoS Control. In this case, the SAPC updates the QoS for the default bearer or sends preconfigured PCC rules to indicate to the PCEF that a dedicated bearer must be established.

The following examples describe scenarios where the AF only provides partial service information to the SAPC:

- A DPI node, such as the SASN that, acting as an AF node towards the SAPC, indicates the establishment of a dynamic service over the Rx interface.
- A third-party application server or content provider (OTT) contacts the SAPC for authorizing the dynamic services and the QoS resources required for a negotiated application layer session.

Figure 2 shows a high-level flow of the establishment of a dynamic service from a DPI node acting as AF. The DPI node performs packet inspection on the data flow and detects when the user contacts a third-party content provider to start a video streaming service. The DPI node informs the SAPC about the activation of the streaming service, and the SAPC adapts the QoS of the default bearer to guarantee the service delivery.

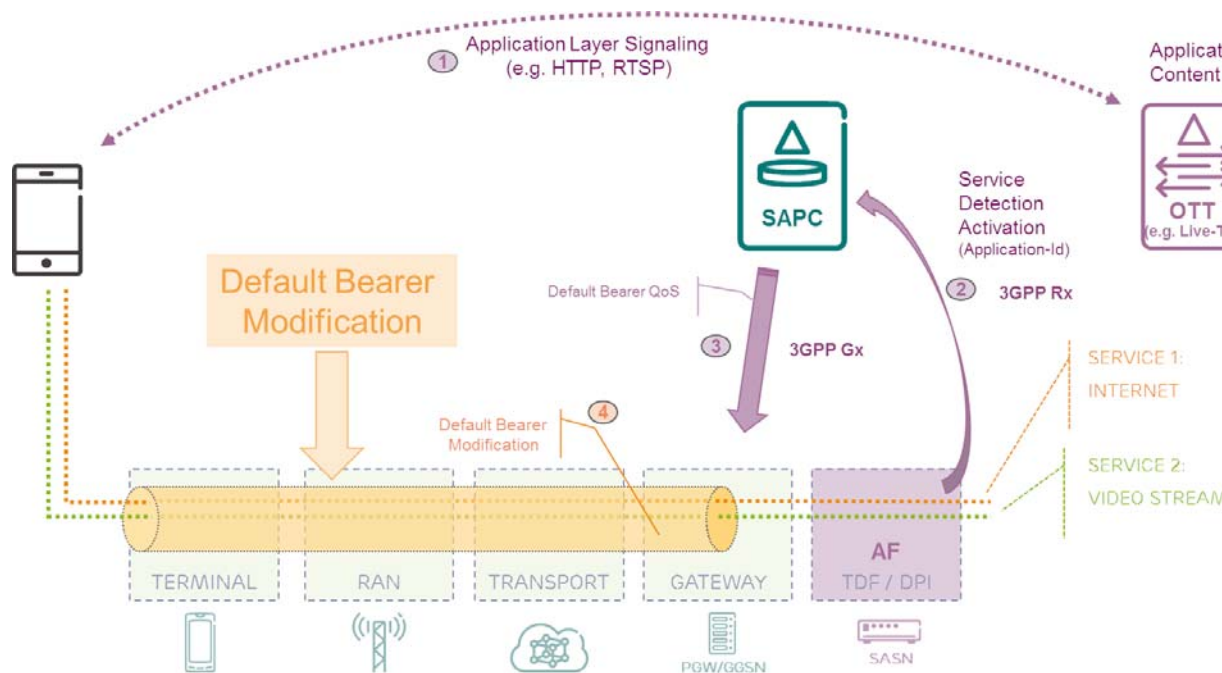


Figure 2 AF session establishment without session media data

## 2.2 Negotiation of Rx Interface Version and Supported Features

During session establishment, the AF indicates the set of supported features required for the AF session. The SAPC indicates, in the first answer message, the set of supported features that it has in common with the AF and that the SAPC supports during the lifetime of the session. The set of supported features includes the Rx interface version and the set of optional features required for the AF session. The SAPC supports Rx Release 9, Rx Release 10, and Rx Release 11, but the SAPC does not support any of the optional Rx features defined by 3GPP.

The AF provides the required Rx interface version in the initial AA-Request (AAR) command within the Supported-Features AVP. Only one instance of Supported-Features AVP with a Feature-List-ID of value 1 shall be provided, the SAPC ignores any additional feature lists. In addition, the SAPC ignores the value of Supported-Features AVP during AF session modification, if present in the AAR command.

The SAPC provides the negotiated Rx interface version in the initial AA-Answer (AAA) command within the Supported-Features AVP, only when the AF session establishment is successfully completed. If the AF is unable to interoperate using Rx Release 9 onwards, the SAPC rejects the AF session establishment with an error code according to the following:

- If the AF only supports Rx interface Release 7 standard, and therefore the Supported-Features AVP is absent from the AAR command, the SAPC returns DIAMETER\_MISSING\_AVP (5005)





- If the AF requests session establishment with Rx interface Release 8 standard, the SAPC returns DIAMETER\_INVALID\_AVP\_VALUE (5004)

## 2.3 Session Binding

Session binding is the association of the AF session information with an IP-CAN session.

The SAPC performs session binding only during AF session establishment. As a result from the session binding function, the SAPC identifies what IP-CAN session the current AF session is related to, and associates the described service IP flows in the AF session information with that IP-CAN session. Policy control decisions derived from AF session interactions are enforced in the associated IP-CAN session.

The SAPC must receive enough information in AA-Request message to bind the AF session to a single existing IP-CAN session. If the SAPC is not capable of executing the session binding or finds several candidate IP-CAN sessions to bind to, the SAPC sends an AA-Answer command to the AF with the Experimental-Result-Code AVP set to IP-CAN\_SESSION\_NOT\_AVAILABLE (5065).

The SAPC associates the AF session to the single IP-CAN session in function to the AVPs received over Rx interface according to the following order:

- 1 If the SAPC receives the Subscription-Id, the Called-Station-Id and the Framed-IP-Address (or Framed-IPv6-Prefix) AVPs:  
the SAPC compares the user IP address (Framed-IP-Address or Framed-IPv6-Prefix), the administrative subscriber identifier (mapped from Subscription-Id AVP), and the PDN information with the information received through the Gx interface.

In case SAPC does not find any candidate IP-CAN session to bind to, the session binding fails and the SAPC answers AF session establishment with an error. But if the subscription information received through the Rx interface is of type SIP-URI and the administrative subscriber identifier is not defined for the SIP-URI subscription information, the SAPC attempts to perform the binding as stated by the next items.

- 2 If the SAPC receives the IP-Domain-Id AVP through the Rx interface:  
the SAPC performs the association by comparing the domain identity (IP-Domain-Id AVP) with the PCEF identity (Origin-Host AVP) and other AVPs (the Called-Station-Id, the Subscription-Id, the Framed-IP-Address and the Framed-IPv6-Prefix) with the information received through the Gx interface according to preset directives.

The SAPC provides a configurable mapping between the Origin-Host received through the Gx interface and the IP-Domain-Id received through the Rx interface to correlate the PCEF identity with the domain identity.

The SAPC performs the session following these directives:



- a If the Called-Station-Id and the Framed-IP-Address (or Framed-IPv6-Prefix) AVPs are available:  
the SAPC compares the user IP address (Framed-IP-Address or Framed-IPv6-Prefix), the PDN information, and the domain identity (IP-Domain-Id AVP) with the information received through the Gx interface.

In case SAPC does not find any candidate IP-CAN session to bind to, the session binding fails and the SAPC answers AF session establishment with an error.

- b If the Subscription-Id and the Framed-IP-Address (or Framed-IPv6-Prefix) AVPs are available:  
the SAPC compares the user IP address (Framed-IP-Address or Framed-IPv6-Prefix), the administrative subscriber identifier (mapped from Subscription-Id AVP), and the domain identity (IP-Domain-Id AVP) with the information received through the Gx interface.

In case SAPC does not find any candidate IP-CAN session to bind to, the session binding fails and the SAPC answers AF session establishment with an error. But if the subscription information received through the Rx interface is of type SIP-URI and the administrative subscriber identifier is not defined for the SIP-URI subscription information, the SAPC performs the association based on the user IP address and the domain identity.

- c If the Framed-IP-Address or Framed-IPv6-Prefix AVPs is available:  
the SAPC performs the association by comparing the user IP address (Framed-IP-Address or Framed-IPv6-Prefix), and the domain identity (IP-Domain-Id AVP) with the information received through the Gx interface.

If the user IP address and the domain identity are received and not session matches or more than one session matches, the SAPC answers AF session establishment with error.

- 3 If the SAPC receives the Called-Station-Id and the Framed-IP-Address (or Framed-IPv6-Prefix) AVPs:  
the SAPC compares the user IP address (Framed-IP-Address or Framed-IPv6-Prefix), and the PDN information with the information received through the Gx interface.

If the user IP address and the PDN information are received and not session matches or more than one session matches, the SAPC answers AF session establishment with error.

- 4 If the SAPC receives the Subscription-Id and the Framed-IP-Address (or Framed-IPv6-Prefix) AVPs:  
the SAPC compares the user IP address (Framed-IP-Address or Framed-IPv6-Prefix), and the administrative subscriber identifier (mapped from Subscription-Id AVP).



In case SAPC does not find any candidate IP-CAN session to bind to, the session binding fails and the SAPC answers AF session establishment with an error. But if the subscription information received through the Rx interface is of type SIP-URI and the administrative subscriber identifier is not defined for the SIP-URI subscription information, the SAPC performs the association based on the user IP address.

- 5 If the SAPC receives the Framed-IP-Address or Framed-IPv6-Prefix AVPs: the SAPC performs the association by comparing the user IP address (Framed-IP-Address or Framed-IPv6-Prefix).

The administrative subscriber identifier is used to correlate the Subscription-Id AVPs received through the Rx interface with the information received through the Gx interface. The SAPC obtains the administrative subscriber identifier that is used for session binding, as follows.

- If multiple Subscription-Id AVPs are received through the Rx message, the SAPC selects one of them, based on configuration, to locate the administrative subscriber identifier.
- If the selection of subscription identifier type is not configured, the first received Subscription-Id AVP is selected.

It is possible to have several Rx sessions (from either the same or different AF nodes) that bind to the same IP-CAN session. Moreover, dual stack IPv6v4 IP-CAN sessions may have associated several IPv4 Rx sessions and several IPv6 Rx sessions at the same time.

To perform session binding in those networks handling IP address overlapping with the same PCEF (refer to [Access and Charging Control \(Gx\)](#)), the SAPC must receive Called-Station-Id information at AF session creation. For the case of IP address overlapping among different PCEFs, the SAPC must receive IP-Domain-Id or Subscription-Id AVP.

## 2.4 Classification of Dynamic Services

This function determines the services that are dynamically activated in the SAPC from information provided by the AF through the Rx interface. The AF provides session and service information (session media data) to the SAPC in the AA-Request command. The session media data (when provided) is structured into media components in the AA-Request command, which represent different data flows from the point of view of the AF. The SAPC makes use of this information to trigger the activation of one or more dynamic services, according to the configured conditions in the policies for dynamic service classification. The association between dynamic services and media components is fully flexible, so that a dynamic service in SAPC may comprise one or several AF media flows.

Dynamic service classification is performed at:

- AF session establishment



- Modification of an existing AF session to add new media

Dynamic service classification is a global policy in SAPC, meaning that it is applied to all active subscribers and subscriber groups. When a dynamic service is activated for a subscriber, it remains active until the AF terminates the session or removes the media stream that corresponds to the service. Modification of the AF session to update the characteristics of the media streams (session media data such as the IP flows, the requested bandwidth) does not trigger a re-evaluation of the policies for dynamic service classification.

The following information received from the AF can be evaluated to classify dynamic services:

- AF application identifier

It is the identifier of the service for which the user has negotiated the bearer resources. If SIP is used, the AF application identifier is extracted from the SIP headers.

- Media type

It is the type of media negotiated for a session component. For example, AUDIO, VIDEO, DATA, and TEXT.

- Destination ports

IP port or port range used to deliver the application service, which corresponds to the destination port of the uplink traffic or source port of the downlink traffic of the negotiated Session Media Data.

The SAPC evaluates the policies for Dynamic Service Classification, and the result of the service classification is the service identifier. The conditions (policy rules) to classify dynamic services can be configured in SAPC to match a wide range of media patterns received from the AF, in particular it is possible to classify:

- Dynamic services that comprise all media components in the AF session
- One dynamic service per media component in the AF session
- Dynamic services that have no media components associated (when no session media data is received from the AF, but only the AF application identifier)
- Dynamic services with an undefined number of media components

Page 9 shows examples of service classification patterns and the associated dynamic service identifier.

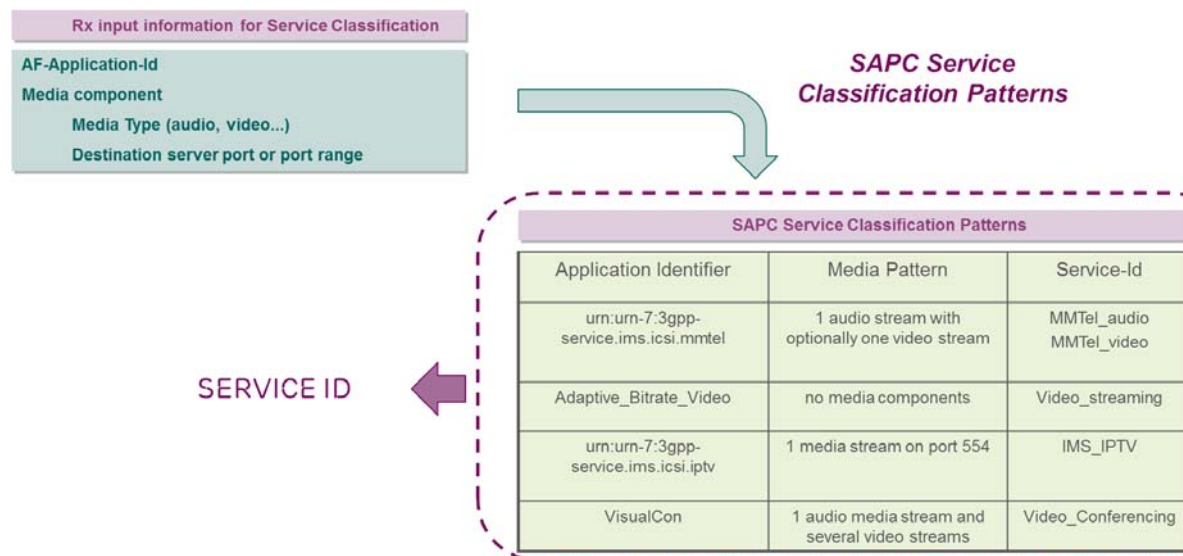


Figure 3 Example of dynamic service classification patterns

The output service identifier of the classification process is used as a reference to perform subsequent service authorization and qualification.

If there are no policies defined in the SAPC to match the information received in the AA-Request command and classify the relevant dynamic services, then the SAPC responds to the AF with an AA-Answer command including the Experimental-Result-Code AVP set to the value REQUESTED\_SERVICE\_NOT\_AUTHORIZED (5063), and creates a log.

## 2.5 Authorization of Dynamic Services

This function determines whether dynamic services are authorized for a given subscriber or subscriber group, under certain conditions (policies). By default, dynamic services are authorized.

Dynamic service authorization is performed in the following conditions:

- When a new dynamic service is classified for a subscriber as a result of
  - AF session establishment
  - Modification of an existing AF session to add new media
- During IP-CAN session reauthorization because of IP-CAN session modification or PCRF-initiated reauthorization

There are two ways to manage the authorization of dynamic services, by configuring a list of restricted services (a blacklist), or by service authorization policies.



First, the SAPC evaluates if the dynamic service is blacklisted according to the corresponding subscriber or subscriber group profile. If the dynamic service is blacklisted, the service is not authorized.

In addition, the SAPC can use information received from the access network as input for the service authorization decision, such as the Radio Access Technology and the Subscriber Location Information. To make the service authorization decision, the SAPC evaluates the policies for service authorization with the service identifier obtained during the classification process as resource.

**Note:** Time of day (ToD) policies are not supported in dynamic service authorization.

The actions taken by the SAPC when a dynamic service is classified but not authorized are different from the actions taken when a dynamic service currently running in the IP-CAN session becomes not authorized as a result of a change in the dynamic conditions that are evaluated.

### **Authorization of New Dynamic Services**

If the result of the authorization of a newly classified dynamic service is positive, the SAPC completes the AF session establishment and returns a successful AA-Answer command. If the dynamic service is not authorized, the SAPC responds to the AF with an AA-Answer command including the Experimental-Result-Code AVP set to the value REQUESTED\_SERVICE\_NOT\_AUTHORIZED (5063), and the service is not established in the IP-CAN session.

### **Reauthorization of Existing Dynamic Services in the IP-CAN session**

During IP-CAN session reauthorization, the SAPC evaluates again the policies to decide whether a dynamic service that is running in the IP-CAN session continues to be authorized. This enables SAPC to detect if the service blacklist or the information received from the access network has changed.

If the result of the authorization of an existing dynamic service is negative, the SAPC removes the corresponding PCC rule(s) from the IP-CAN session. In addition, the SAPC informs the AF (only if the AF has previously requested the subscription to INDICATION\_OF\_RELEASE\_OF\_BEARER or INDICATION\_OF\_FAILED\_RESOURCES\_ALLOCATION events) that the service has been deactivated.

When all the services in the AF session are no longer authorized, the SAPC informs the AF by sending an Abort-Session-Request (ASR) command. However, when there are still authorized services in the AF session, the SAPC informs the AF by sending a Re-Auth-Request (RAR) command including the list of service data flows that have been deactivated.



## 2.6 Qualification of Dynamic Services

After dynamic services are successfully classified and authorized, the SAPC determines the associated QoS information and the Charging parameters. If the dynamic service comprises AF media flows, this process results in the QoS information and the charging parameters associated with the dynamic PCC rules generated for the service. However, if the dynamic service has no media components associated, no dynamic PCC rules are generated with QoS and Charging information, and this functionality does not apply.

Dynamic service qualification is performed at:

- AF session establishment with associated media components
- Modification of an existing AF session
- IP-CAN session reauthorization because of IP-CAN session modification or PCRF-initiated reauthorization

The output of the qualification of a dynamic service is a QoS profile and Charging profile that contain the authorized QoS and Charging information for the dynamic PCC rules generated for the service. For newly established dynamic services, this process, together with the generation of dynamic PCC rules, results in new PCC rules sent to the PCEF in a Re-Auth-Request command. For existing dynamic services, the SAPC evaluates again the policies for qualification of dynamic service to detect changes. If the QoS or Charging information differs from what has been provisioned to the PCEF, the SAPC updates the existing PCC rules by sending a Re-Auth-Request command to the PCEF.

The SAPC determines the QoS and Charging information associated with a dynamic service evaluating service QoS policies and service Charging policies, respectively, according to the following precedence allocation:

- 1 Subject policy locator.
- 2 Subject group policy locator.
- 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. Refer to “Solving Policies Conflicts” section in *Subscription and Policy Management*.

However, if there are not applicable policies, or the policies are not fulfilled, the SAPC obtains the QoS and Charging profile statically assigned to the dynamic service.

**Note:** Time of day (ToD) policies are not supported in dynamic service qualification.



### 2.6.1 Allocation of QoS Information to Dynamic Services

The QoS information includes the QoS class identifier (authorized QoS class for the service data flow), the Allocation and Retention Priority (ARP) and authorized bit rates for uplink and downlink

To get the QoS Information associated with the dynamic service, the SAPC evaluates the QoS policies that apply to the service identifier that is obtained from the Dynamic Service Classification procedure. These policies can take into account subscriber information, access network information provided by the PCEF and media session information provided by the AF.

The QoS information is assigned per media component. For dynamic services that comprise several AF media flows, it is possible to allocate different QoS profiles to the different AF media components by including conditions such as the media type in the policy rules.

If the AF media component contains two subflows to deliver the service (two media subcomponents), the SAPC assigns the QoS information to each of the AF media subcomponents according to the usage indicated for this particular IP flow in the Flow-Usage AVP.

- If the media sub-component is used to transport media data such as RTP, the SAPC assigns the QoS profile obtained.
- If the media sub-component is used to transport media signalling data (RTCP), the SAPC generates the QoS information as follows:
  - The QCI and ARP values are set to the same value as in the QoS profile obtained.
  - The MBR value is obtained as 5% of the MBR value in the QoS profile obtained.
  - The GBR value (if applicable) is obtained as 5% of the GBR value in the QoS profile obtained.

If the QoS profiles obtained after the policy evaluation do not provide values for the QCI, MBR, or GBR, the SAPC applies the procedure defined in 3GPP to calculate the value of those QoS parameters.

This procedure is defined in Policy and Charging Control signalling flows and QoS parameter mapping, TS 29.213, chapter QoS parameter mapping Functions at PCRF.

- QCI is assigned depending on the media type and whether the IP flows are unidirectional or bidirectional, as shown in the next table.

Session Media Data	QoS Class Identifier
Media-Type AVP is not present	QCI = 9





Media-Type AVP set to AUDIO or VIDEO	QCI = 2, if IP flows are bidirectional  QCI = 4, if IP flows are unidirectional
Media-Type AVP set to APPLICATION	QCI = 2
Media-Type AVP set to DATA	QCI = 8
Media-Type AVP set to CONTROL	QCI = 6
Media-Type AVP set to TEXT, MESSAGE, OTHER	QCI = 9

- The MBR for the flows used to transport media data (RTP) in the uplink and downlink is obtained from the Max-Requested-Bandwidth-UL AVP and Max-Requested-Bandwidth-DL AVP respectively. If the AF does not provide the maximum requested bandwidth for an IP flow, the SAPC omits the MBR value in the dynamic PCC rule for this IP flow. If the AF does not provide a Flow-Description AVP in either the uplink or the downlink direction, the SAPC sets the MBR value to zero (0) in this direction.
- The MBR for the RTCP flows is obtained by applying this calculation:
  - The MBR for uplink = RS-Bandwidth + RR-Bandwidth
  - The MBR for downlink = RS-Bandwidth + RR-Bandwidth
  - If the RR-Bandwidth AVP is not received from the AF, the MBR assigned is the maximum of the value of the RS-Bandwidth and the 5% of the MBR assigned to the RTP flow
  - If the RS-Bandwidth AVP is not received from the AF, the MBR assigned is the maximum of the value of the RR-Bandwidth and the 5% of the MBR assigned to the RTP flow
  - If the RR-Bandwidth AVP and the RS-Bandwidth AVP are not received from the AF, the MBR assigned is the 5% of the MBR assigned to the RTP flow
- The GBR is assigned the same value as the MBR for both, the RTP and the RTCP flows. The GBR value is only included in the PCC rule for QCI values 1 to 4

If there are not applicable policies, or the policies are not fulfilled, the SAPC obtains the QoS profile provisioned to the dynamic service (static qualification).

## 2.6.2

### Allocation of Charging Parameters to Dynamic Services

The charging parameters define the Service Identifier, Rating Group, Reporting Level, Metering Method, and whether the online and offline charging interfaces are used.

To obtain the charging profile associated with a dynamic service, the SAPC evaluates the charging policies that apply to the service identifier that has been obtained in the Dynamic Service Classification procedure. These policies can take into account subscriber information, access network information provided by the PCEF and media session information provided by the AF. If there are not applicable policies, or the policies are not fulfilled, the SAPC obtains the Charging profile provisioned to the dynamic service (static qualification).

The charging information is assigned per media component associated with the dynamic service. Therefore, all dynamic PCC rules created for the same media component contain the same charging information.

For dynamic services that comprise several AF media flows, it is possible to allocate different Charging profiles to the different AF media components by including conditions such as the media type in the policy rules.

If the Charging profile obtained after the policy evaluation do not provide any of the optional charging parameters, this information is omitted from the dynamic PCC rule. Finally, if the procedure cannot obtain a charging profile, no charging information is included in the dynamic PCC rule

## 2.7 Generation of Dynamic PCC Rules

The SAPC receives information about the session that the user has negotiated with the AF through the Rx interface. This triggers the establishment of one or more dynamic services, by following the process of Dynamic Service Classification and Authorization. If the AF provides information about the IP flows required to deliver the service (media component information), the SAPC generates the policy control and charging information in the form of PCC rules. These dynamic PCC rules are installed in the PCEF through of the Gx protocol.

The SAPC generates one dynamic PCC rule for every media sub-component received from the AF. New dynamic PCC rules are generated when new dynamic services are established (that is, AF session establishment or modification of an existing AF session to add new media). Modification of the characteristics of existing dynamic services (that is, AF session modification) triggers a modification of the PCC rules that have been previously provisioned to the PCEF.

Figure 4 shows the relation between the AF service information received through the Rx interface and the PCC rule information that is generated by the SAPC and installed in the PCEF using the Gx interface.

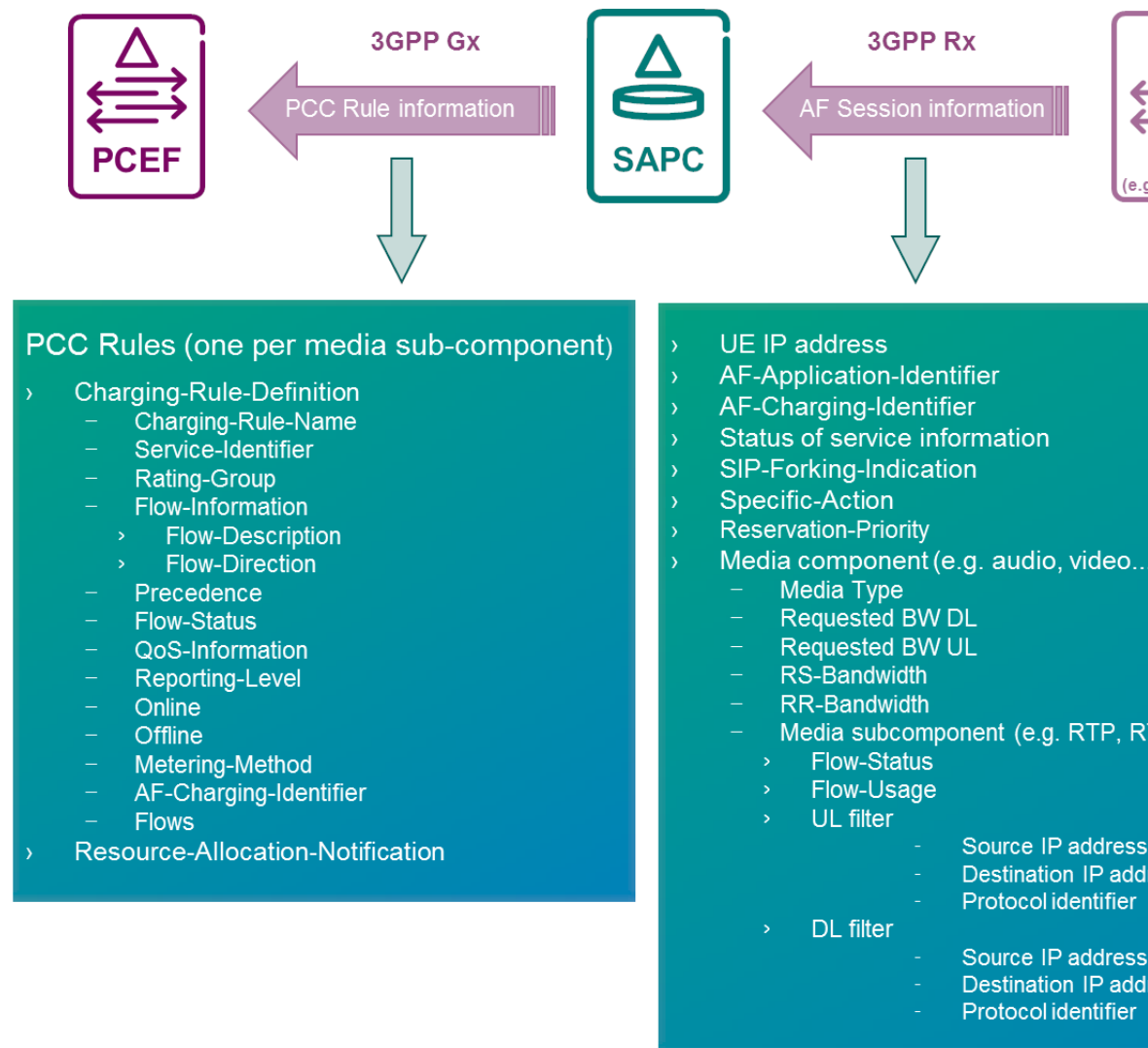


Figure 4 Information received from the AF and provided to the PCEF

The information received from the AF consists of the following (refer to Rx Interface Description for a complete list of supported AVPs):

— UE-IP-Address parameter

The IPv4 or IPv6 address allocated to the terminal attached to the AF. This is a mandatory parameter.

**Note:** In scenarios in which UE IP addresses are reused for different APNs or for different PCEFs (IP address overlapping), the AF must send the Subscription-Id and Called-Station-Id parameters.

— AF-Application-Identifier

The identifier of the particular application service that the AF session belongs to. In IMS deployments, the P-CSCF (AF) derives this information from the IMS communication service requested by the UE.

— AF-Charging-Identifier

The charging identifier used by the AF (for example, for IMS it is the IMS Charging Identifier). This information may be used for charging correlation with the access network charging records.

— Service-Info-Status

This parameter indicates the status of the service information that the AF provides to the SAPC, whether the application service has been fully negotiated between the two end points or the information is preliminary.

— SIP-Forking-Indication

This parameter indicates whether the AF session relates to a single SIP dialogue or to several SIP dialogues. See Section 2.10.2 on page 24.

— Specific-Action

The traffic plane events (such as release of a bearer) that the AF requires to be notified by the SAPC. See Section 2.9 on page 21.

— Reservation-Priority

The priority assigned to the AF session and media flows in the resource reservation request. The SAPC can take into account this value to assign the Allocation and Retention Priority (ARP) in the PCC rules installed in the PCEF, according to the Dynamic Service Qualification procedure.

— Media Component

It contains service information for a single media component within the AF session. For example, an IMS session for multimedia telephony can have one audio media component and one video media component. This parameter contains a Media-Component-Number, that indicates the ordinal number of the media component. A media component can be divided into several media subcomponents.

- Media-Type

The type of media of a session component, for example, audio or video

- Uplink requested bandwidth

The maximum bandwidth for an uplink IP flow requested by the AF. If the media component contains two media subcomponents, this refers to the bandwidth required to transport the media data (RTP) in the uplink direction.



- Downlink requested bandwidth

The maximum bandwidth for a downlink IP flow requested by the AF. If the media component contains two media subcomponents, this refers to the bandwidth required to transport the media data (RTP) in the downlink direction.

- RS-Bandwidth

The maximum required bandwidth for RTCP sender reports within the session component. This value, together with the RR-Bandwidth, sets the maximum required bandwidth to transport the media control information for an RTP session.

- RR-Bandwidth

The maximum required bandwidth for RTCP receiver reports within the session component. This value, together with the RS-Bandwidth, sets the maximum required bandwidth to transport the media control information for an RTP session.

- Media Subcomponent

Each Media-Subcomponent contains the IP filter definition for a set of IP flows. The IP filter definition describes the uplink or downlink IP flows, including the source and destination IPv4 or IPv6 addresses and ports. In addition, information regarding the Flow-Usage (for example, if the flow is RTCP or RTP) and Gating is included.

- Flow-Number

Ordinal number of the IP flow.

- Flow-Description

Describes the uplink or downlink IP flows. It includes Direction, Source IPv4 or IPv6 address, Destination IPv4 or IPv6 address, Source Port, Destination Port, Protocol.

- Flow-Usage

Set to “RTCP”, if media subcomponent refers to an RTCP flow and “no information” in any other case. It is an optional parameter with default value “NO INFORMATION”.

- Flow-Status

This parameter indicates whether the IP flows are enabled or disabled by the AF. This allows the SAPC to control the traffic flow through the PGW in the user plane (gating functionality). See Section 2.10.1 on page 24.



The SAPC generates the dynamic PCC rules using the information described previously in the Dynamic Services Classification and Service Authorization policies. The SAPC generates the corresponding dynamic PCC rules for each media component, and installs the corresponding PCC rules. There is one PCC rule for each media subcomponent, which implies that there is one PCC rule for each RTP flow and one PCC rule for each RTCP flow. If the SAPC does not receive any media components, no PCC rules are created.

The SAPC generates each PCC rule containing the following information:

— **PCC rule name**

A unique identifier for the PCC rule within the IP-CAN session, provisioned in the Charging-Rule-Name AVP. The SAPC assigns a new value for PCC rules generated when new dynamic services are established. At AF session modification, the PCC rule name remains the same.

The PCC rule name follows a specific format of four elements, delimited by the "@" character, with a maximum size of 63 characters. The PCC rule name begins with the service identifier that results from the dynamic service classification process, then continues with the Media-Component-Number and the Flow-Number, and finally includes a pseudo-random portion derived from the Rx diameter Session-Id.

— **Service Data Flow**

It consists of the Flow-Information, and Flow-Status AVPs included in the PCC rule. This information identifies the uplink and downlink IP flows of a media subcomponent. The SAPC obtains the service data flow from the media subcomponent UL and DL packet filter provided by the AF in the Flow-Description AVP.

— **Precedence**

This parameter determines the order, in which service data flow filters are applied at the PCEF. A PCC rule with lower precedence value shall be applied before a PCC rule with higher precedence value. The SAPC calculates the precedence value according to the completeness of the DL flows of the PCC rule, according to the following criteria:

- If the DL filter of the PCC rule is complete and defined with specific source and destination ports, the SAPC sets the precedence value to zero.
- If some information of the DL filter is missing or incomplete, the precedence value is increased. If the source IP is missing, the precedence is increased by 1. If the source IP is ANY, the precedence is increased by 2. If the source port is a list or a range, the precedence is increased by 1. If the source port is ANY, the precedence is increased by 2. If the destination port is a list or a range, the precedence is increased by 1. If the destination port is ANY, the precedence is increased by 2. If the destination IP is missing, the precedence is increased by 1. If the destination IP is ANY, the precedence is increased by 2.



#### — QoS Information

To generate the QoS-Information AVP that applies to the PCC rule, the SAPC applies the Dynamic Service Qualification procedure.

#### — Charging Information: : The charging information includes the following:

- The SAPC obtains the Rating Group, Reporting Level, Metering Method, and offline or online states by applying the Dynamic Service Qualification procedure.
  - Reporting-Level: Defines on what level the PCEF reports the usage for the related PCC rule. Reporting level can be at a combination of service identifier and rating group, or at rating group level
  - Metering-Method: Defines what parameters are metered for offline charging. Metering method can be duration, volume, or both
  - Offline: Defines whether the offline charging interface from the PCEF for the associated PCC rule is enabled
  - Online: Defines whether the online charging interface from the PCEF for the associated PCC rule is enabled
  - Rating-Group: The charging key for the PCC rule, used for rating purposes
  - Service-Identifier: The identity of the service or service component in the PCEF that the service data flow in a dynamic PCC rule relates to
- AF-Charging-Identifier
 

If the Reporting-Level AVP is set to the value SERVICE\_IDENTIFIER\_LEVEL (0), then the SAPC includes the AF-Charging-Identifier AVP in the dynamic PCC rule. The value of AF-Charging-Identifier is obtained from the data received from the AF.
- Flows
 

The flow identifiers of the IP flows related to a PCC rule, as provided by the AF. The SAPC includes the Flows AVP in the dynamic PCC rule only when the AF-Charging-Identifier AVP is also present.

#### — Resource Allocation Notification

This parameter is included when the allocation of resources for the related PCC rules must be confirmed, as requested by the AF

## 2.8 IP-CAN Session Reauthorization

Establishment, modification and termination of dynamic services also triggers in the SAPC a re-evaluation of all previous policy decisions taken for the IP-CAN

session. Examples of the application of session reauthorization owing to dynamic service establishment include the ability to apply Bearer QoS Control, Access and Charging Control and BW Management to other services running on the IP-CAN session.

Session reauthorization owing to dynamic service establishment is useful in the following example scenarios:

- For scenarios in which only the default bearer is supported, and an IMS service is established. In this case, the SAPC can downgrade the QoS of the rest of the services running on the default bearer, to guarantee IMS service delivery. Alternatively, the SAPC can upgrade the QoS of the default bearer to accommodate all services
- For scenarios in which a DPI box is acting as an AF, and does not provide media component description to the SAPC. In this case, a pre-configured PCC rule can be defined in the SAPC, associated with the activation of a dynamic service, that initiates the establishment of a dedicated bearer for the delivery of the service detected by the DPI box.

The SAPC performs reauthorization of the IP-CAN session at AF session establishment, AF session modification and AF session termination, regardless of the generation of dynamic PCC rules. The SAPC evaluates the applicable policies for the IP-CAN session, to perform the following functionality (refer to *Service Access and Charging Control* and *IP-CAN Bearer QoS Control*).

- IP-CAN session Access Control
- Service Access Control
- Service Charging Control
- Bearer QoS Control
- Bandwidth Management

The conditions (policy rules) for those functions are extended to be able to apply policy decisions based on the establishment of a dynamic service, as follows.

- Indication of dynamic service establishment

This function indicates if a dynamic service is running in the IP-CAN session, which means that the dynamic service has been successfully classified and authorized. This allows the SAPC for example to authorize and install static or preconfigured PCC rules based on whether a given dynamic service is running or not.

In addition, to calculate the QoS for the default bearer, the SAPC uses the Bearer QoS Control function extended with the following operations that can be used to take policy decisions.

- Maximum QoS for the dynamic services





This function returns a QoS profile composed of the highest value for every field in the QoS profile, out of the values obtained for each dynamic PCC rule running in the IP-CAN session.

- Aggregated QoS for the dynamic services

This function returns a QoS profile composed of the sum of the throughput parameters (GBRs and MBRs) out of the values obtained for each dynamic PCC rule running in the IP-CAN session, and selecting the highest value in the rest of the QoS parameters.

## 2.9 Notification of Bearer Events to the AF

The AF may request the SAPC to be notified about certain events on the user plane, such as when a bearer is released, by using the *Specific-Action* AVP in an initial *AA-Request* command. This enables the AF to react to traffic plane events by application level signalling.

The SAPC supports notification of the following traffic plane events:

- IP-CAN session termination
- Service Data Flow deactivation
- Successful resources allocation
- Network Location Information

The SAPC sends to the AF one notification message per traffic event, even in situations where several traffic plane events are reported simultaneously by the PCEF. For example, if the PCEF reports in the same *CC-Request* command that one dynamic PCC rule has been successfully installed and another dynamic PCC rule has been deactivated, the SAPC sends two separate *Re-Auth-Request* commands to the AF.

### 2.9.1 IP-CAN Session Termination

When an IP-CAN session is terminated, the SAPC informs the AF about the IP-CAN session termination by sending an *Abort-Session-Request* command to the AF on each active Rx Diameter session. As a result, the AF indicates the termination of the Rx session by sending a *Session-Termination-Request* command to the SAPC.

### 2.9.2 Service Data Flow Deactivation

When a dynamic PCC rule cannot be installed/activated or enforced at the PCEF, the SAPC deactivates the corresponding dynamic service and informs the AF that one or more service data flows have been deactivated. This function enables the

AF to react to events in the user plane by sending an AAR command to the SAPC to update the session information or an STR command to terminate the AF session.

The SAPC gets the knowledge that one or more service data flows have been deactivated, on reception of a Charging-Rule-Report AVP in a CC-Request command that includes the PCC-Rule-Status AVP set to the value INACTIVE, the list of failed PCC rules, and the failed reason code. Then the SAPC removes the PCC rule(s) from the IP-CAN session, performs IP-CAN session reauthorization, and notifies the AF if the AF has previously requested subscription to INDICATION\_OF\_RELEASE\_OF\_BEARER or INDICATION\_OF\_FAILED\_RESOURCES\_ALLOCATION events.

The notification from the SAPC details the affected IP flows, and includes a failure code that indicates the reason of the failure.

- If not all the service data flows within the AF session are reported as INACTIVE and the AF has requested to be notified, the SAPC sends a Re-Auth-Request command and reports the affected IP Flows encoded in the Flows AVP, the type of action encoded in the Specific-Action AVP, and the reason for the failure encoded in the Abort-Cause AVP. The SAPC sets the value of the Specific-Action AVP to match the subscription from the AF.
- When all the service data flows within the AF session are affected, the SAPC sends an Abort-Session-Request command on the Rx Diameter session related to the AF session, that includes the reason for the failure encoded in the Abort-Cause AVP.

The Abort-Cause AVP is set to the value BEARER\_RELEASED in all cases except when the Rule-Failure-Code AVP received from the PCEF is set to PS\_TO\_CS\_HANDOVER (refer to SRVCC for more details).

### 2.9.3 Successful Resources Allocation

The AF may request the SAPC to provide a notification when the resources associated to the corresponding service information have been allocated. In this case, the SAPC requests the PCEF to confirm that the resources associated to the corresponding dynamic PCC rules are successfully allocated, and on reception of the confirmation from the PCEF, the SAPC notifies the AF. This function applies to applications for which the successful resource allocation notification is required for their operation. The drawback is that subscription to this notification impacts the resource allocation signalling overhead towards the PCEF.

The procedure to provide indication of successful resources allocation is detailed in Section 4.3.2 on page 42.

- The AF sets the Specific-Action AVP to the value INDICATION\_OF\_SUCCESSFUL\_RESOURCES\_ALLOCATION in the initial AA-Request command.
- The SAPC derives the dynamic PCC rules from the service information and includes the Resource-Allocation-Notification AVP with



the value `ENABLE_NOTIFICATION` within the corresponding `Charging-Rule-Install` AVP(s).

- When resource allocation is successfully completed, the PCEF sends an event trigger indication with the value `SUCCESSFUL_RESOURCE_ALLOCATION`. The affected rules are indicated within the `Charging-Rule-Report` AVP with the `PCC-Rule-Status` AVP set to the value `ACTIVE`.
- On reception of the notification from the PCEF, the SAPC sends a `Re-Auth-Request` command with `Specific-Action` AVP set to the value `INDICATION_OF_SUCCESSFUL_RESOURCES_ALLOCATION` and the affected IP Flows encoded in the `Flows` AVP.

## 2.9.4 Network Location Information

Network Location Information (NetLoc) is an optional function, and the SAPC negotiates its support during Gx and AF session establishment. It enables the SAPC to report one time report network location information during the AF session establishment, modification, or termination.

During the AF session establishment or modification, when the SAPC receives a request to report the access network information (user location or MS timezone, or both) from the AF, the SAPC sets the access network information report parameters in the corresponding PCC rules according to the information required by the AF, and provisions them to the PCEF together with the `ACCESS_NETWORK_INFO_REPORT` event trigger (refer to [Access and Charging Control \(Gx\)](#), Reference [1] for more information about event triggers). When the SAPC receives the requested access network information together with the `ACCESS_NETWORK_INFO_REPORT` event trigger from the PCEF, the SAPC provides it to the AF.

During the AF session termination, IP-CAN session termination, or IP-CAN bearer release (if all the service data flows within the AF session are affected), when the SAPC receives the NetLoc request from the AF in the session termination request, the SAPC answers with the corresponding access network information received from the PCEF. During the IP-CAN bearer release, if not all the service data flows within the AF session are affected, the SAPC provides the corresponding access network information in the Rx reauthorization request to the AF.

### 2.9.4.1 Network Location Information Reporting Failure Handling

When the AF requests reporting the access network information during the AF session establishment, modification, or termination, and the PCEF does not support the access network information reporting, the SAPC responds to the AF indicating that access network information reporting is not supported.

When the AF requests reporting the access network information during the AF session establishment, modification, or termination, but the PCEF indicates that the access network currently serving the UE does not support access network information retrieval, the SAPC informs the AF of an access network information



reporting failure including also that the access network does not support access network information retrieval as failure reason.

## 2.10 IMS Related PCC Procedures over Rx

### 2.10.1 Gating Control

This function controls the flow of IP packets through the PCEF according to the information received from the AF. The SAPC receives the Flow-Status AVP from the AF and applies this information to the PCC rules installed on the PCEF. The Flow-Status can be received from the AF for the whole media component or for a media subcomponent. The Flow Status information provided for a media component applies to all IP flows within the media component, for which no corresponding information is being provided within Media-Sub-Component AVPs.

The following values can be used to perform gating:

— ENABLED-UPLINK (0)

This value is used to enable the associated uplink IP flows, and to disable the associated downlink IP flows.

— ENABLED-DOWNLINK (1)

This value is used to enable the associated downlink IP flows, and to disable the associated uplink IP flows.

— ENABLED (2)

This value is used to enable all associated IP flows in both directions.

— DISABLED (3)

This value is used to disable all associated IP flows in both directions.

If a Media-Sub-Component AVP under a Media-Component-Description AVP contains a Flow-Usage AVP with the value RTCP, then the corresponding RTCP IP flows in both directions are enabled, even if the Flow-Status AVP under the Media-Sub-Component AVP is set to ENABLED-UPLINK, ENABLED-DOWNLINK, or DISABLED.

### 2.10.2 Support for SIP Forking

SIP forking is the ability to send SIP request messages to multiple destinations, that correspond to multiple registered contact addresses in the IMS network. This allows the IMS network to attempt simultaneously the establishment of the application session in multiple destinations where the subscriber may be reached. The provisional response from each possible destination is called an early dialog.

Upon the reception of the first final response, the IMS releases the remaining early dialogs and completes application session establishment.

During SIP forking, the AF (P-CSCF) receives provisional responses from more than one terminating end point, and requests authorization and resources to the SAPC to accommodate for the most demanding early dialog. Each provisional response may have different service requirements (different IP flows, requested bandwidth, and so on), and it is not known which terminating endpoint will finally accept the application session until the final response is received. This implies that when the P-CSCF receives the first final response, only the media flows negotiated for this particular early dialog are authorized for the IMS session.

The procedure to support SIP forking is depicted in Figure 5.

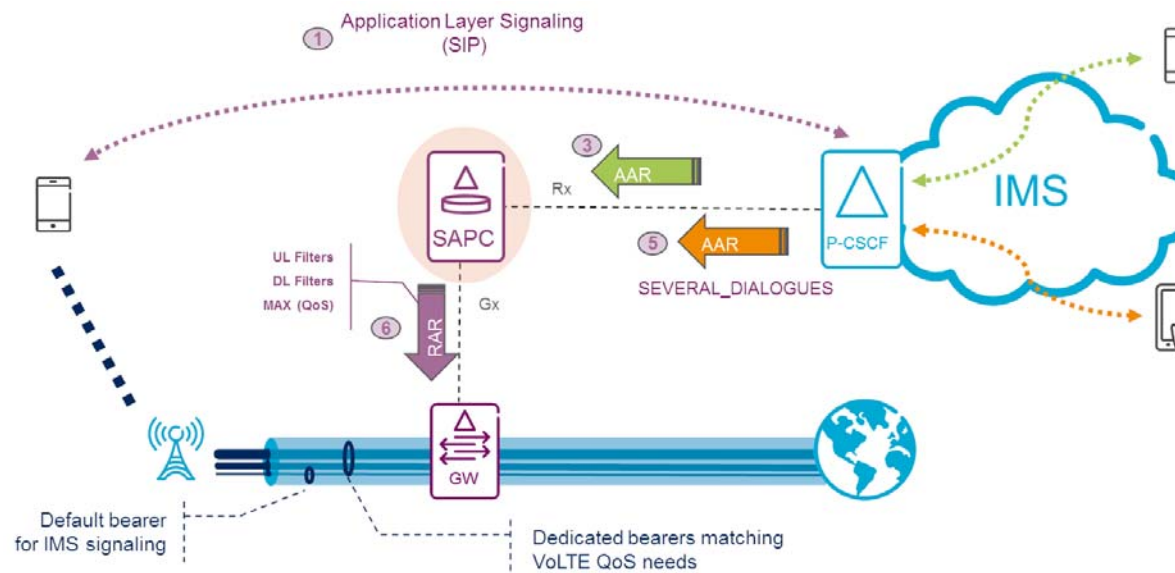


Figure 5 Overview of SIP Forking functionality

After the first AF session is established, for each subsequent provisional response establishing an extra early dialog, the P-CSCF sends an AA-Request command within the existing Diameter session containing the SIP-Forking-Indication AVP with the value SEVERAL\_DIALOGUES, and includes the service information derived from the latest provisional response.

Upon reception of service information for provisional responses, the SAPC authorizes any additional media components and any increased QoS requirements for the previously authorized media components. The SAPC authorizes the maximum bandwidth required by any of the dialogues, but not the sum of the bandwidths required by all dialogues. Thus, the SAPC updates the installed dynamic PCC rules and adds additional service data flow filters for each of the early dialogs, so that the QoS authorized for a media component is equal to the highest QoS requested for that media component by any of the forked responses.

The SAPC opens or closes the gates for service flows according to the Flow Status information received from the AF. However, if a media flow has been enabled

within previous service information, it shall remain enabled even if the SAPC receives service information that disables this flow ID within an AAR containing the SIP-Forking-Indication AVP with value SEVERAL\_DIALOGUES.

When receiving the first final SIP response, the P-CSCF sends an AA-Request command without the SIP-Forking-Indication AVP, and includes the full service information (applicable IP flows, requested bandwidth, and so on) derived from the dialogue of the final response.

When the SAPC receives an AA-Request command with no SIP-Forking-Indication AVP or with a SIP-Forking-Indication AVP with value SINGLE\_DIALOGUE, the SAPC updates the installed PCC rules information and QoS information to match only the requirements of the service information within this AA-Request. The SAPC also removes the PCC rules or individual service data flow filters not matching IP flows provided in the final response, and performs gating control according to the flow status information received in the final response.

### 2.10.3 Single Radio Voice Call Continuity (SRVCC)

Single Radio Voice Call Continuity (SRVCC) refers to the transfer of an IMS Multimedia Telephony call from the PS domain to the CS domain, when the UE can transmit and receive on only one of those access networks at a given time.

During the SRVCC procedure, the SAPC receives an indication from the PCEF that one or more PCC rules cannot be maintained because of PS to CS handover. The SAPC then informs the AF (only if the AF has previously requested the subscription to INDICATION\_OF\_RELEASE\_OF\_BEARER or INDICATION\_OF\_FAILED\_RESOURCES\_ALLOCATION events) that the bearer has been deactivated owing to PS to CS handover.

The procedure to support SRVCC is depicted in Figure 6.

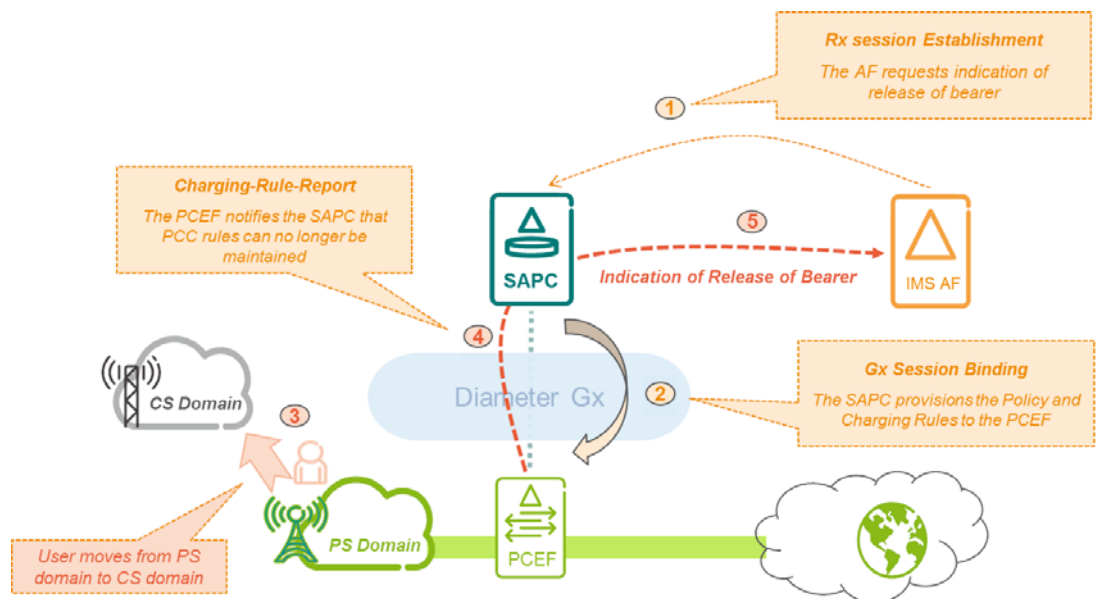


Figure 6 Overview of SRVCC functionality

When the IMS session is transferred from the PC domain to the CS domain, the PCEF sends a CC-Request command with a Charging-Rule-Report AVP that identifies the PCC rules that can no longer be maintained, and includes the PCC-Rule-Status AVP set to the value INACTIVE and the Rule-Failure-Code AVP set to the value PS\_TO\_CS\_HANDOVER. Then, the SAPC notifies the AF by using either a Re-Auth-Request command or an Abort-Session-Request command, including the Abort-Cause AVP set to the value PS\_TO\_CS\_HANDOVER.

- If not all the service data flows within the AF session are reported as INACTIVE and the AF has requested to be notified, the SAPC sends a Re-Auth-Request command and reports the affected IP Flows encoded in the Flows AVP and the type of action encoded in the Specific-Action AVP.
- When all the service data flows within the AF session are affected, the SAPC sends an Abort-Session-Request command on the Rx Diameter session related to the AF session.

## 2.11 Handling of Race Conditions Related to Multiple AF Requests

Network scenarios where multiple AF sessions are bound to the same IP-CAN session may lead to race conditions, due to traffic events that happen concurrently or within a short time frame. This situation may result in a state mismatch, where the wrong information is being maintained by the PCEF, the SAPC and/or the AF for the session.

Diameter race conditions may happen in the following situations:



- Concurrent PCEF-initiated and AF-initiated IP-CAN session modifications.

The main use case has been found in scenarios where the AF requires notification of successful resources allocation, which results in an increased rate of Credit-Control-Request (CCR) update messages from the PCEF to the SAPC. The problem occurs when a SAPC-initiated IP-CAN session modification (possibly triggered by AF interaction) overlaps in time with a PCEF-initiated IP-CAN session modification (possibly to notify the successful outcome of a previous session modification).

- Multiple AF requests within a short time period.

The main use case has been found in scenarios where the AF performs multiple Rx session creation/modification requests in short succession for the same user. This triggers SAPC to send Gx RAR messages at a high rate, potentially triggering a new session modification before the previous Gx RAR message has been acknowledged.

The SAPC is able to handle diameter race conditions, not only triggered by AF interactions but also due to other internal or external events that overlap in time. Refer to *Access and Charging Control (Gx)* for a complete functional description.

The procedure to handle race conditions due to multiple AF requests is as follows:

- When the SAPC receives a diameter AAR message from the AF, the SAPC answers AAA as usual, and follows the procedures described in *Access and Charging Control (Gx)*.
- Other AF interactions that occur for the same IP-CAN session during the time period where the SAPC is waiting for acknowledgment of a RAR message, do not trigger a modification of the IP-CAN session. The SAPC updates the AF session information, sends the AAA message and waits until the end of the time period or reception of the RAA message.
- When the RAA message is received or the timer expires, the SAPC performs the pending session reauthorization and sends a new RAR message including all the pending policy information to be communicated to the PCEF.
- If the RAA includes the result code `DIAMETER_PENDING_TRANSACTION` or `DIAMETER_OUT_OF_SPACE`, the new RAR message also contains information about the policies that failed to be enforced in the PCEF, as described in *Access and Charging Control (Gx)*.
- If the SAPC receives a CCR-U message when there is a previous Gx RAR pending to be acknowledged, the SAPC performs a session re-authorization depending on the event received in the CCR-U message, as usual. However, if the AF has requested the SAPC to report the access network information for this IP-CAN session, the SAPC skips policy evaluation for static, preconfigured, and dynamic services until the Gx RAA message is received or the timer expires.





## 3 Dynamic Policy Control Network Deployments

The SAPC can provide Dynamic Policy Control in the following network elements:

— In the bearer plane (PCEFs) side:

- Ericsson EPG, through Ericsson Gx+ Rel9 onwards.
- Ericsson SASN, through Ericsson Gx+ Rel9 onwards.
- Non-Ericsson PCEF, through standard Gx Rel9 onwards.

**Note:** The SAPC also supports multiple PCEFs deployments for Dynamic Policy Control, where for example the SASN is deployed together with a GGSN/PDN-GW, being dynamic PCC rules enforced in the GGSN-PDN GW.

— In the application plane (AF) side:

- Ericsson SBG, through standard Rx Rel9 onwards.
- Ericsson SASN, through standard Rx Rel9 onwards.
- Non-Ericsson AF, through standard Rx Rel9 onwards.

## 4 Dynamic Policy Control Traffic Cases

This chapter explains the interfaces involved in Dynamic Policy Control.

This chapter explains the traffic interactions between the network nodes involved in Dynamic Policy Control. For detailed description of each of the interfaces supported, the corresponding interface description should be consulted.

The precondition to all traffic cases is that a diameter connection is already established between the SAPC and the PCEF and between the SAPC and the AF. In addition, all the required policy controls are enabled for the PCEF, and support for dynamic PCC rules is enabled for the GGSN/PDN GW.

- The Service Access policy control is required to perform authorization of dynamic services.
- The Bearer QoS policy control is required to allocate QoS Information to dynamic services.

- The Service Charging policy control is required to allocate charging Information to dynamic services.

The `Session-Id` is a mandatory AVP for all the messages in the Rx protocol, to identify an AF session uniquely.

The precondition to all traffic cases is as follows:

- The availability of this function in the SAPC is under license control, otherwise SAPC rejects any Rx message by answering with Result-Code `DIAMETER_UNABLE_TO_COMPLY=5012`.
- The number of simultaneous Rx sessions has not reached the hard limit of the corresponding licensed Rx sessions capacity, otherwise SAPC rejects any new Rx session creation by answering with Result-Code `DIAMETER_UNABLE_TO_COMPLY=5012`.

## 4.1 AF Session Lifetime

This chapter shows the most common traffic cases that may happen during the life cycle of the AF session (establishment, modification, and termination), in network scenarios where the AF provides information about the IP flows required to deliver the service (media component information). The precondition for all traffic cases is that the UE has established an IP-CAN session.

### 4.1.1 AF Session Establishment

The following figure shows the signalling flow that takes place during AF session establishment and the main actions taken by the SAPC to perform dynamic policy control. This traffic case includes the scenario where network initiated bearers are supported (Bearer Control Mode is set to `UE_NW`), and also the scenario where network initiated bearers are not supported (Bearer Control Mode is set to `UE_ONLY`).

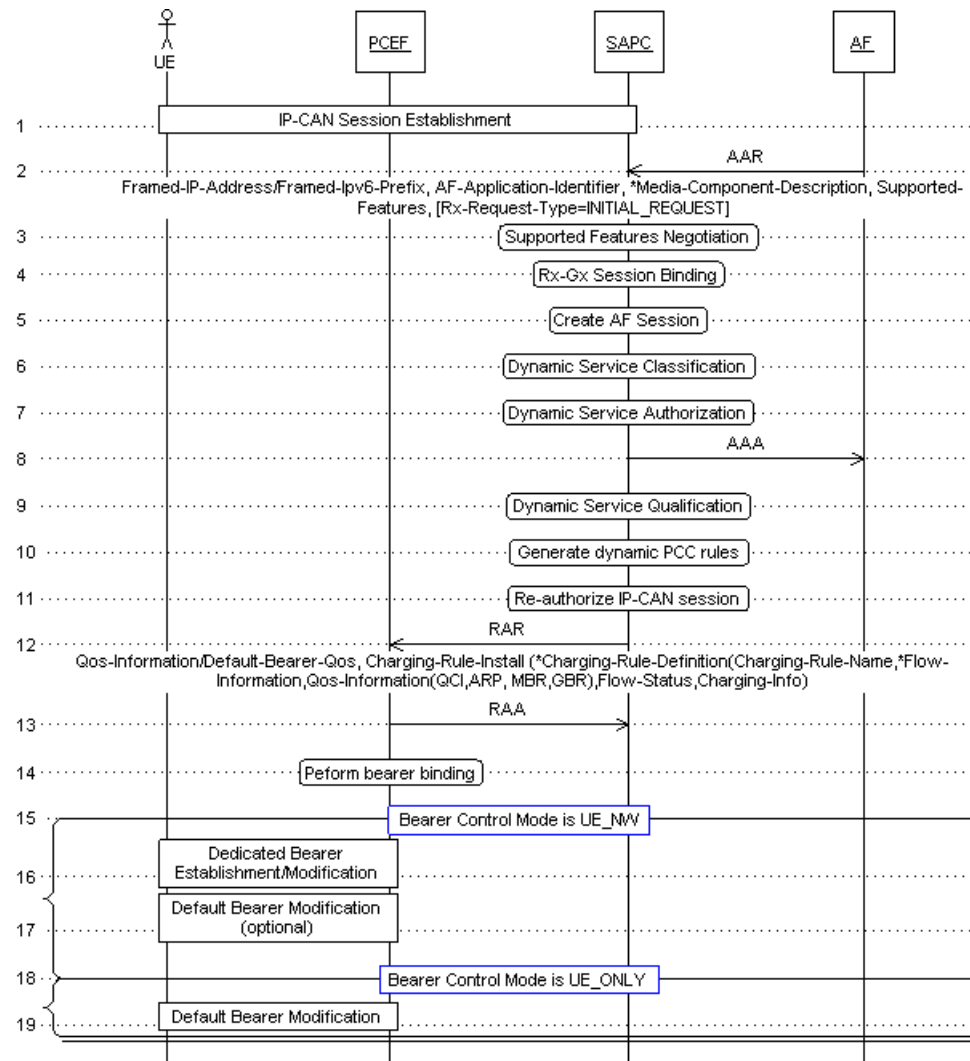


Figure 7 AF Session Establishment

- 1 The UE has established an IP-CAN session.
- 2 The SAPC receives an AAR message from the AF to establish a new AF session. The main information that the AF provides is:
  - The IPv4 or IPv6 address that identifies the UE terminal.
  - The AF-Application-Identifier AVP that typically permits to identify the particular service that the AF session belongs to.
  - The Media-Component-Description AVP(s), that contain service information for each media component within an AF session. This parameter includes the set of IP flows required to deliver the service, the type of media, the flow status information, and the requested bandwidth.



- The set of supported features required for the AF session, in the Supported-Features AVP.
  - Optionally, the following information may be also provided by the AF:
    - The charging identifier used by the AF, in the AF-Charging-Identifier AVP
    - The status of the service information provided by the AF, in the Service-Info-Status AVP.
    - The Called-Station-Id AVP and Subscription-Id AVP to assist session binding.
    - The priority assigned to the AF session, in the Reservation-Priority AVP.
    - The Rx-Request-Type AVP indicating INITIAL\_REQUEST (0).
  - If the Rx-Request-Type AVP is not received, the SAPC checks if there is an AF session created with the same received Session-Id. If an AF session already exists, continue in Section 4.1.2 on page 33, step 4.
- 3 The SAPC determines the set of supported features that it has in common with the AF, according to Section 2.2 on page 4.
    - If the Supported-Features AVP is not present in the AAR command, the SAPC rejects the AF session establishment with the error code DIAMETER\_MISSING\_AVP (5005).
    - If the AF requests session establishment with Rx interface Release 8, the SAPC returns the error code DIAMETER\_INVALID\_AVP\_VALUE (5004).
  - 4 The SAPC performs session binding and associates the AF session information with an existing IP-CAN session, according to Section 2.3 on page 5. If session binding is not successful, the SAPC sends an AAA command to the AF with the Experimental-Result-Code AVP set to IP-CAN\_SESSION\_NOT\_AVAILABLE (5065).
  - 5 The SAPC creates an AF session for this subscriber's request, linked to the bound IP-CAN session.
  - 6 The SAPC identifies the set of services corresponding to the AF session by performing the Service Classification (see Section 2.4 on page 7). If no dynamic service is successfully classified, then the SAPC rejects the AF session establishment with the Experimental-Result-Code AVP set to the value REQUESTED\_SERVICE\_NOT\_AUTHORIZED (5063).
  - 7 The SAPC determines if the classified dynamic services are authorized, according to Section 2.5 on page 9. If any of the dynamic services is not authorized, the SAPC rejects the AF session establishment with the Experimental-Result-Code AVP set to the value REQUESTED\_SERVICE\_NOT\_AUTHORIZED (5063).



- 8 The SAPC responds to the AF with an AA-Answer command indicating the operation result. If the request is successfully, the Result-Code AVP is set to the value SUCCESS. If the request is unsuccessful, an error code is indicated in either the Result-Code AVP (for generic diameter error codes) or in the Experimental-Result AVP (for Rx-specific error codes).
- 9 The SAPC determines the QoS and Charging information associated with the dynamic services that have been classified and authorized, by evaluating the service qualification policies. See Section 2.6 on page 10.
- 10 The SAPC generates the policy control and charging information in the form of dynamic PCC rules. One dynamic PCC rule is generated for every media sub-component received from the AF. See Section 2.7 on page 14.
- 11 The SAPC performs reauthorization of the IP-CAN session to reevaluate the previous policy decisions taken for the IP-CAN session according to the applicable policies. This permits for example to perform Service QoS Control and BW Management to remove or apply less bandwidth to other services that are running on the default bearer. The SAPC also performs Bearer QoS Control and calculates the quality of service that applies to the default bearer.
- 12 The SAPC sends to the PCEF the dynamic PCC rules including the QoS information for each PCC rule, the charging information, and the QoS information for the default bearer if necessary (this is, only if it differs from default bearer QoS information already provisioned to the PCEF). If the Bearer QoS policy control is not enabled for the PCEF, the SAPC sends the dynamic PCC rules with no QoS information. In addition, the SAPC may provision other PCC rules and policy decisions that result from the reauthorization of the IP-CAN session, within the same RAR command.
  - In 3GPP-GPRS access, the SAPC sends the quality of service information of the default bearer in the QoS-Information AVP.
  - In 3GPP-EPS access, the SAPC sends the quality of service information of the default bearer in the Default-EPS-Bearer-QoS AVP.
- 13 The PCEF accepts the installation of PCC rules.
- 14 The PCEF performs the bearer binding and modifies the default bearer (if applicable), according to the Bearer Control Mode selection.

#### 4.1.2

#### AF Session Modification

The following figure shows the signalling flow that takes place during AF session modification and the main actions taken by the SAPC to perform dynamic policy control. The AF session modification may only update the service information for existing media components, but may also add new media components and remove media components. Gating control is another scenario of AF session modification, where the AF signals the SAPC if the IP flow(s) are to be enabled or disabled to pass through the IP-CAN. This traffic case includes the scenario where network initiated bearers are supported (Bearer Control Mode is set to UE\_NW),

and also the scenario where network initiated bearers are not supported (Bearer Control Mode is set to UE\_ONLY).

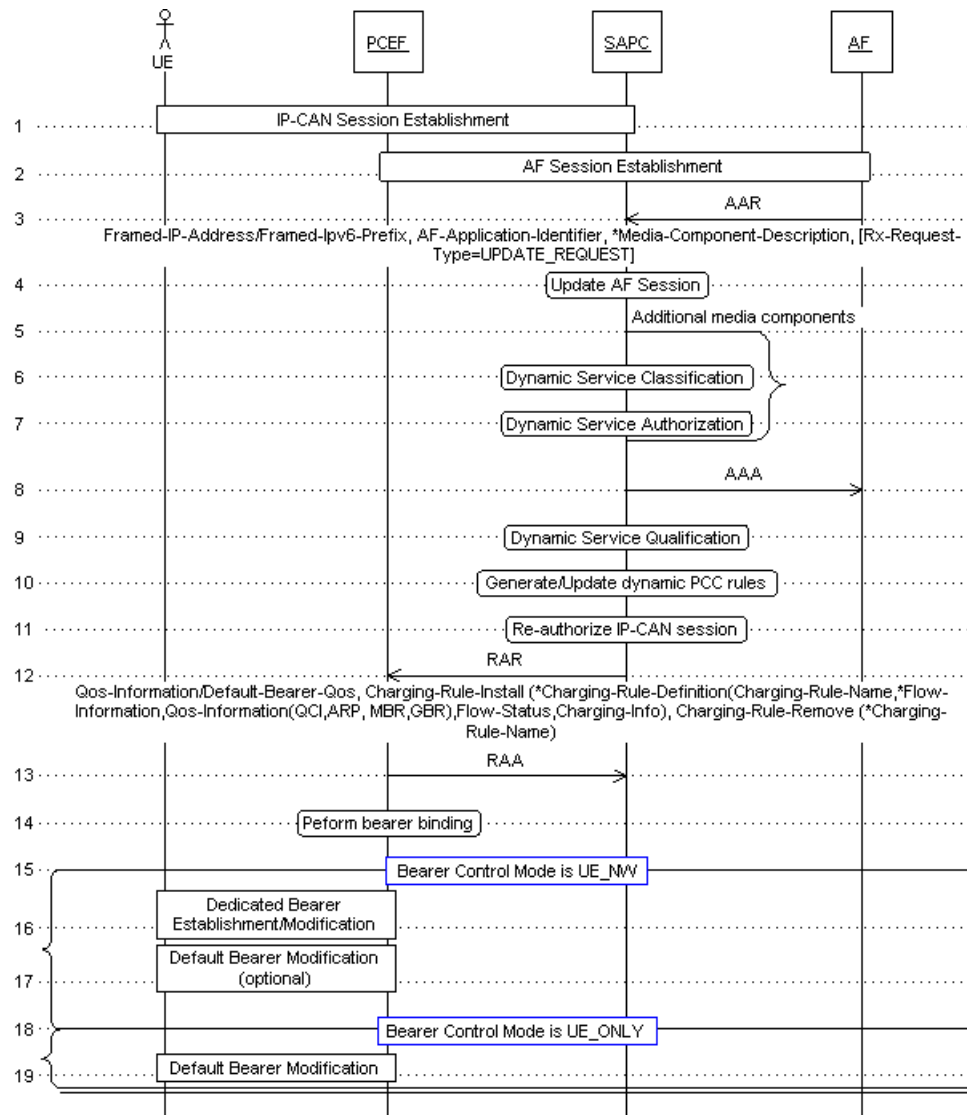


Figure 8 AF Session Modification

- 1 The UE has established an IP-CAN session.
- 2 The AF performs the session establishment procedure, as detailed in Section 4.1.1 on page 30.
- 3 The SAPC receives an AAR message from the AF to modify an existing AF session including the session identifier that identifies the AF session. The main information that the AF provides is the Media-Component-Description AVP(s) with the updated service information for each media component. If a



Media-Component-Description AVP is not supplied by the AF, or if optional AVP(s) within a Media-Component-Description AVP are omitted, but corresponding information has been provided in previous Diameter messages, the previous information for the corresponding IP flow(s) remains valid.

- If the AF performs gating control, the Media-Component-Description AVP(s) contains the flow status information, in the Flow-Status AVP, for the flows that are enabled or disabled to pass through the PCEF. See Section 2.10.1 on page 24 for more details. A typical use case is when the P-CSCF (AF), before the completion of the SIP session setup, enables or disables the media IP flows depending on operator policy, thus allowing or forbidding early media to be transferred end-to-end.
- If the AF modifies the requirements to deliver the application service (such as the set of IP flows, the requested bandwidth), the Media-Component-Description AVPs contain the updated service information for each media component in the AF session that needs to be modified. A typical example is when the P-CSCF (AF) modifies the bandwidth required to deliver the service because of the final negotiation of the codecs to be used end-to-end.
- If the AF adds a media flow to the Rx session, the AAR command contains a Media-Component-Description AVP with a new ordinal number in the Media-Component-Number AVP.
- If the AF removes a new media flow from the Rx session, the AAR command contains a Media-Component-Description AVP with the Flow-Status AVP set to the value REMOVED.

Optionally, the AF may also provide the Rx-Request-Type AVP indicating UPDATE\_REQUEST (1).

- 4 The SAPC updates the AF session state for this subscriber's request, according to the information provided by the AF.
- 5 If the SAPC identifies that the updated AF session contains new media components, the SAPC performs the dynamic service classification and authorization.
- 6 The SAPC identifies the set of new services to be added to the AF session by performing the Service Classification only for the additional media components. If the new media component(s) cannot be successfully classified, then the SAPC rejects the AF session modification with the Experimental-Result-Code AVP set to the value REQUESTED\_SERVICE\_NOT\_AUTHORIZED (5063).
- 7 The SAPC determines if the newly classified dynamic services are authorized, according to Section 2.5 on page 9. If any of the new dynamic services is not authorized, the SAPC rejects the AF session modification with the Experimental-Result-Code AVP set to the value REQUESTED\_SERVICE\_NOT\_AUTHORIZED (5063).

- 8 The SAPC responds to the AF with an AA-Answer command indicating the operation result. If the request is successfully, the Result-Code AVP is set to the value SUCCESS. If the request is unsuccessful, an error code is indicated.
- 9 The SAPC determines the QoS and Charging information associated with the new and existing dynamic services in the AF session, by evaluating the service qualification policies. See Section 2.6 on page 10.
- 10 The SAPC generates the new dynamic PCC rules, modifies the existing dynamic PCC rules, or deletes existing dynamic PCC rules in the IP-CAN session, depending on the information provided by the AF to add new media, update existing media or remove media components.
- 11 The SAPC performs reauthorization of the IP-CAN session to reevaluate the previous policy decisions taken for the IP-CAN session according to the applicable policies. The SAPC also performs Bearer QoS Control and calculates the quality of service that applies to the default bearer.
- 12 The SAPC provisions the policy control and charging information to the PCEF.
- 13 The PCEF accepts the installation of PCC rules and performs bearer binding according to the Bearer Control Mode selection at IP-CAN session establishment.

### 4.1.3

#### AF Session Termination

The following figure shows the signalling flow that takes place during AF session termination and the main actions taken by the SAPC to perform dynamic policy control.



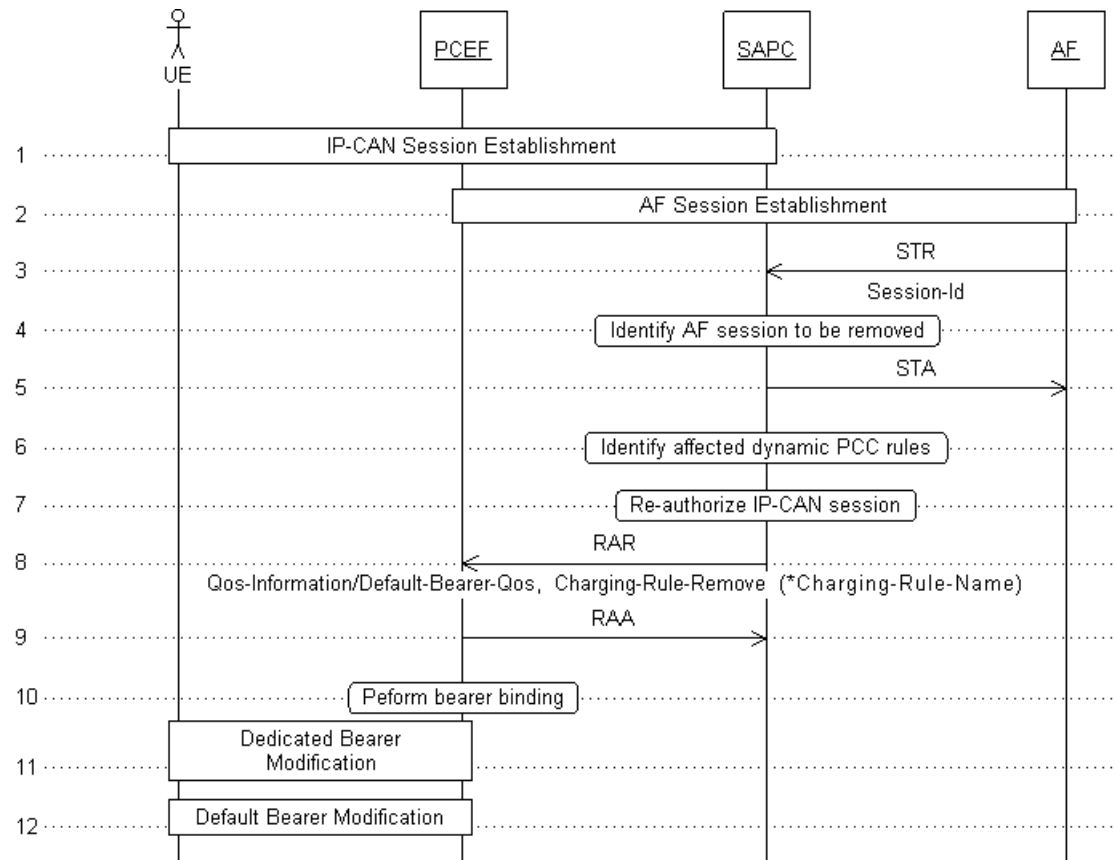


Figure 9 AF Session Termination

- 1 The UE has established an IP-CAN session.
- 2 The AF performs the session establishment procedure, as detailed in Section 4.1.1 on page 30.
- 3 The AF sends an STR to indicate the termination of the AF session.
- 4 The SAPC identifies the session to be removed. If the SAPC cannot find the AF session to be removed, the SAPC rejects the AF session termination and returns the Result-Code AVP set to the value DIAMETER\_UNKNOWN\_SESSION\_ID.
- 5 The SAPC accepts the termination of the AF session, and responds to the AF with a Session-Termination-Answer command indicating the operation result with value SUCCESS.
- 6 The SAPC identifies the affected PCC rules in the IP-CAN session.
- 7 The SAPC performs reauthorization of the IP-CAN session to reevaluate the previous policy decisions according to the applicable policies. The SAPC also performs Bearer QoS Control and calculates the quality of service that applies to the default bearer.



- 8 The SAPC sends a RAR command to the PCEF to remove the affected PCC rules, and the QoS information for the default bearer if necessary. In addition, the SAPC may provision other PCC rules and policy decisions that result from the reauthorization of the IP-CAN session, within the same RAR command.
- 9 The PCEF accepts the removal of the PCC rules, and the modification of the default bearer (if applicable).
- 10 The PCEF performs the bearer binding and modifies the default bearer (if applicable), according to the Bearer Control Mode selection at IP-CAN session establishment.

## 4.2 Reauthorization of Dynamic Services

The following figure shows the signalling flow that takes place during IP-CAN session modification triggered by the PCEF, and the main actions taken by the SAPC to perform dynamic policy control. An example of use case is when the operator has established a policy to authorize only a particular dynamic service (for example video media from the AF) for specific access networks or subscriber location.

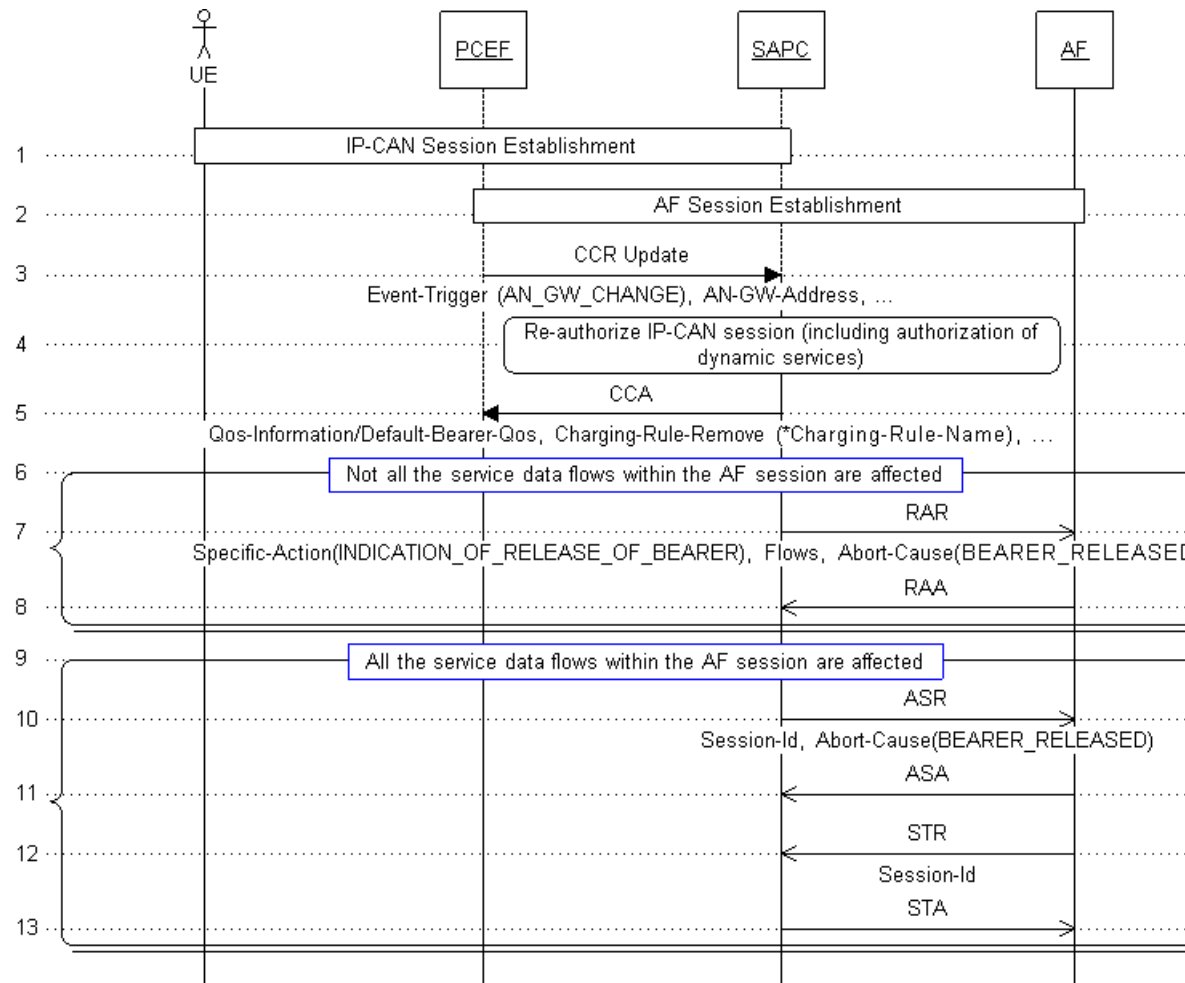


Figure 10 Reauthorization of Dynamic Services during IP-CAN Session Modification

- 1 The UE has established an IP-CAN session.
- 2 The AF performs the session establishment procedure, as detailed in Section 4.1.1 on page 30. In addition, the AF subscribes to the Specific-Action AVP of type INDICATION\_OF\_RELEASE\_OF\_BEARER. The SAPC authorizes the dynamic services and sends the PCC rules to the PCEF.
- 3 The SAPC receives a CCR Update message from the PCEF indicating IP-CAN session modification, and the new/modified parameters together with the associated event-triggers. In this use case, the CCR Update message indicates that the serving Access Node gateway has changed to the value encoded in the AN-GW-Address AVP.
- 4 The SAPC performs reauthorization of the IP-CAN session, including the reauthorization and qualification of all dynamic services running in the IP-CAN session, according to the applicable policies and the new information received. If the result of the authorization of an existing dynamic service



is negative, the SAPC deactivates the dynamic service and removes the corresponding PCC rule(s) from the IP-CAN session.

- 5 The SAPC sends a CCA message to the PCEF including only the new/modified Policy and Charging Control information.
- 6 If any of the existing dynamic services in the IP-CAN session is not authorized, the SAPC notifies the AF:
  - 7. When there are still authorized services in the AF session, the SAPC informs the AF by sending a RAR command with Specific-Action AVP set to the value INDICATION\_OF\_RELEASE\_OF\_BEARER, including the list of service data flows that have been deactivated in the Flows AVP and the reason for the failure set in the Abort-Cause AVP to the value BEARER\_RELEASED.
  - 10. When all the services in the AF session are rejected, the SAPC informs the AF by sending an ASR command including the reason for the failure set in the Abort-Cause AVP to the value BEARER\_RELEASED.

## 4.3 Notification of Bearer Events

### 4.3.1 Service Data Flow Deactivation

The following figure shows the signalling flow that takes place when dynamic PCC rules cannot be installed/activated or enforced at the PCEF, and the main actions taken by the SAPC to perform dynamic policy control.

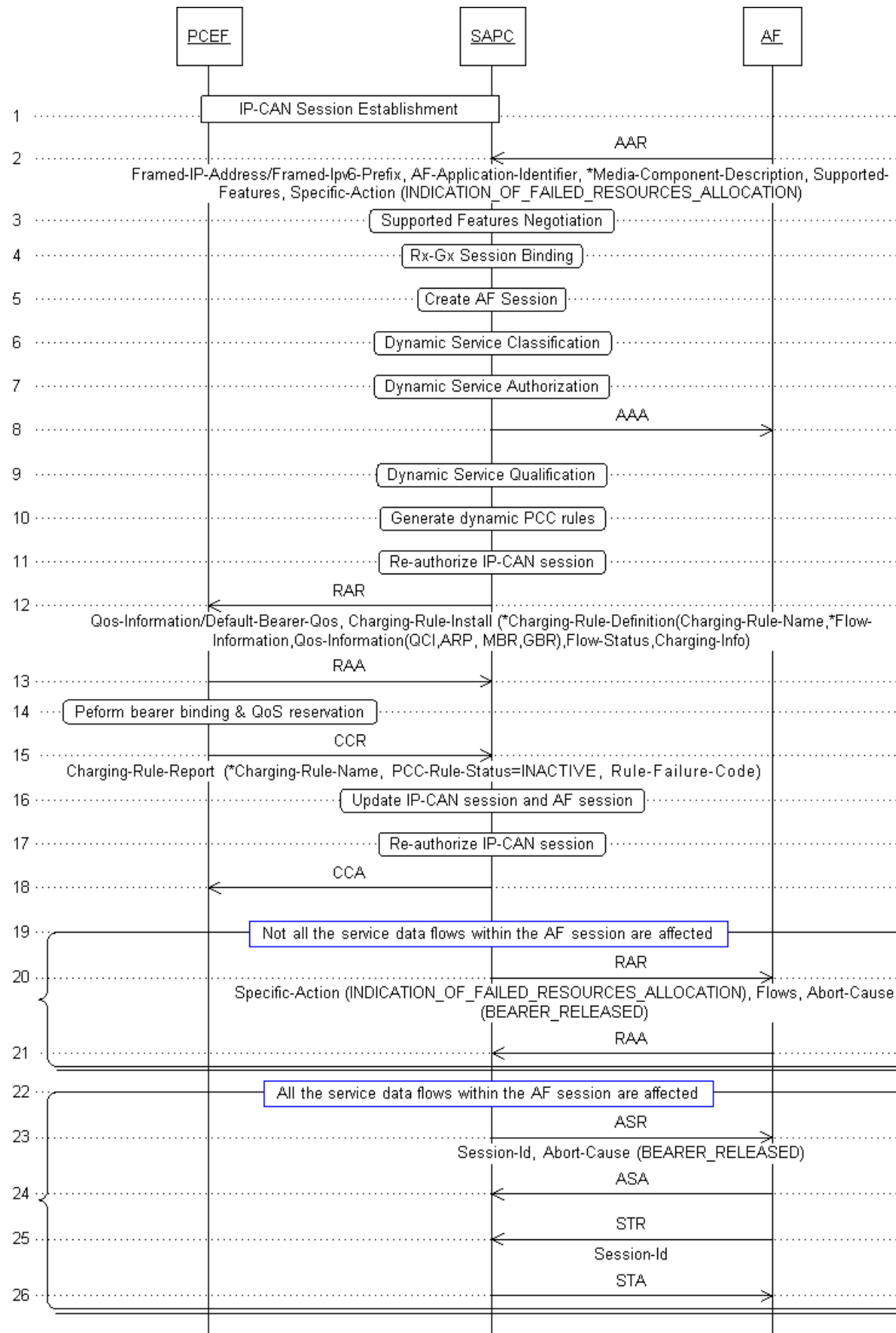


Figure 11 Notification of Inactive Service Data Flows to the AF



- Steps 1–14 are similar to the ones explained in section AF Session Establishment. Next, the main differences are highlighted.
- 2. In addition to the service information, the SAPC receives the list of bearer events that the AF requests to be notified in the Specific Action AVP. In this use case, the AF subscribes to Specific Action of value INDICATION\_OF\_FAILED\_RESOURCES\_ALLOCATION, however the AF may also subscribe to Specific Action of value INDICATION\_OF\_RELEASE\_OF\_BEARER or to both notification events.
- 15. The PCEF sends a CCR-Update that includes a Charging-Rule-Report AVP with the PCC-Rule-Status AVP set to the value INACTIVE, the list of failed PCC rules, and the failed reason code detailed in the Rule-Failure-Code AVP. This indicates to the SAPC that one or more service data flows in the AF session have been deactivated.
- 16. The SAPC removes the failed PCC rule(s) from the IP-CAN session and removes the affected media components and sub-components from the AF session.
- 17. The SAPC performs reauthorization of the IP-CAN session, as described in Section 4.2 on page 38.
- 18. The SAPC sends a CCA message to the PCEF including the new/modified Policy and Charging Control information
- 20. If not all the service data flows within the AF session are affected and the AF has requested to be notified, SAPC sends a RAR message to the AF, including the Specific Action, the deactivated IP Flows encoded in the Flows AVP and the reason for the failure encoded in the Abort-Cause AVP. The SAPC sets the Specific-Action AVP to INDICATION\_OF\_RELEASE\_OF\_BEARER or INDICATION\_OF\_FAILED\_RESOURCES\_ALLOCATION according to the notification event the AF has previously subscribed to. The SAPC sets the Abort-Cause AVP to the value BEARER\_RELEASED in all cases except when the Rule-Failure-Code AVP received from the PCEF is set to PS\_TO\_CS\_HANDOVER (see Section 4.4.2 on page 61).
- 23. If all the service data flows within the AF session are deactivated, the SAPC informs the AF by sending an ASR command, including the reason for the failure encoded in the Abort-Cause AVP. The SAPC sets the Abort-Cause AVP to the value BEARER\_RELEASED in all cases except when the Rule-Failure-Code AVP received from the PCEF is set to PS\_TO\_CS\_HANDOVER. The SAPC sends the ASR command in this case regardless of whether the AF has previously subscribed to any notification event.

### 4.3.2 Successful Resources Allocation

The following figure shows the signalling flow that takes place for the notification of successful installation of dynamic PCC rules to the AF, and the main actions



taken by the SAPC to perform dynamic policy control. A precondition for this use case is that the event-trigger `SUCCESSFUL_RESOURCE_ALLOCATION` is included in the list of events that the SAPC is configured to subscribe to.

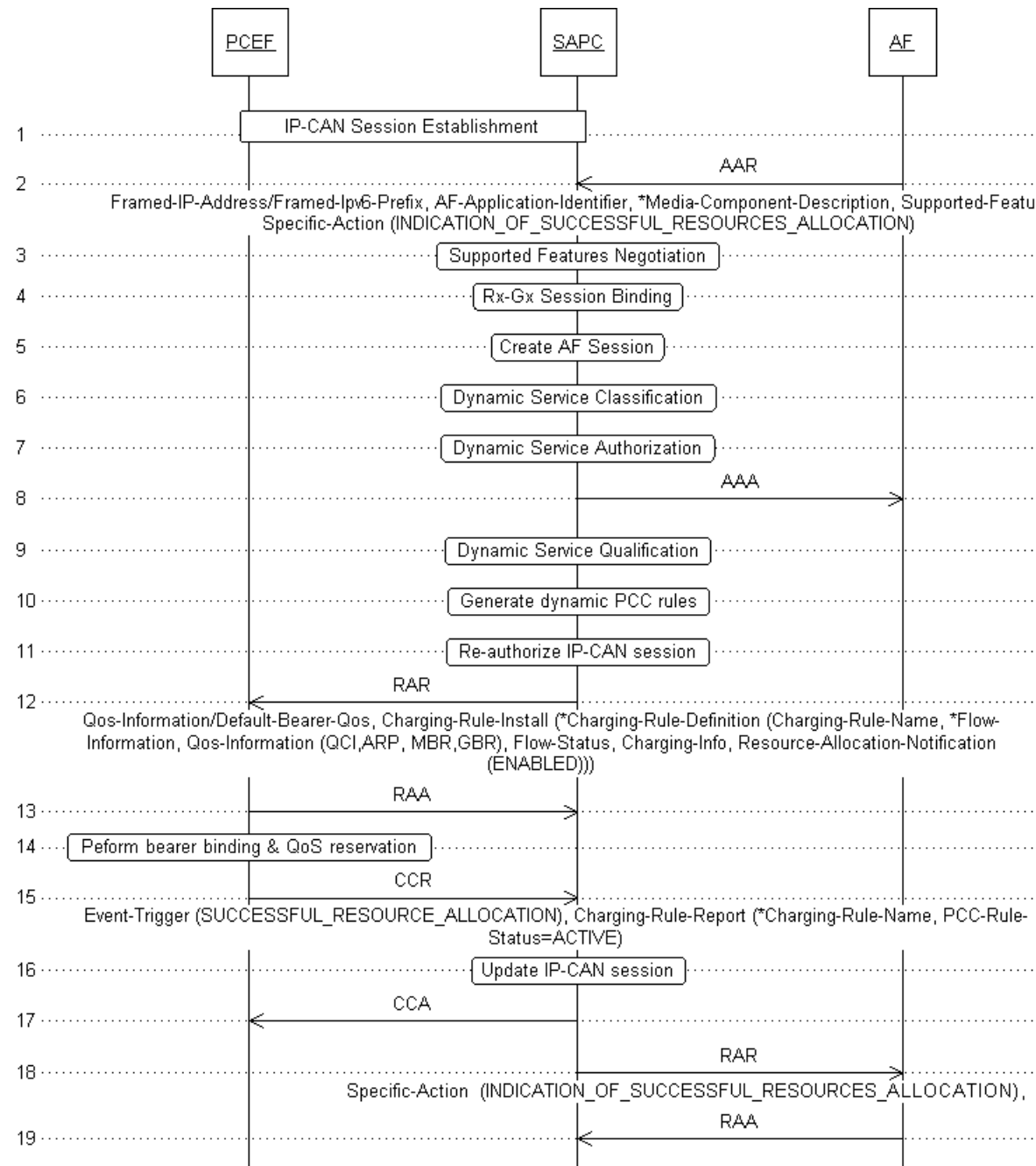


Figure 12 Notification of Successful Resources Allocation to the AF

— Steps 1–14 are similar to the ones explained in section AF Session Establishment. Next, the main differences are highlighted.



- 1. During IP-CAN session establishment, the SAPC provides the Event-Trigger AVP with the value SUCCESSFUL\_RESOURCE\_ALLOCATION.
- 2. In addition to the service information, the SAPC receives the list of bearer events that the AF requests to be notified in the Specific Action AVP, including the value INDICATION\_OF\_SUCCESSFUL\_RESOURCES\_ALLOCATION.
- 12. For each generated dynamic PCC rule, the SAPC includes the Resource-Allocation-Notification AVP set to ENABLED to indicate the PCEF that a confirmation about resource allocation is required.
- 15. The PCEF sends a CCR-Update with Event-Trigger AVP set to SUCCESSFUL\_RESOURCE\_ALLOCATION, that includes a Charging-Rule-Report AVP with the PCC-Rule-Status AVP set to the value ACTIVE, and the list of PCC rules that have been successfully installed/activated.
- 16. The SAPC updates the IP-CAN session and identifies the affected PCC rule(s) and the corresponding AF media components.
- 17. The SAPC accepts the notification.

**Note:** Reception of a CCR command that includes only Event-Trigger AVP set to SUCCESSFUL\_RESOURCE\_ALLOCATION, does not trigger a policy re-evaluation at the SAPC.
- 18. The SAPC sends a RAR command to the AF with Specific-Action AVP set to the value INDICATION\_OF\_SUCCESSFUL\_RESOURCES\_ALLOCATION and the affected IP Flows encoded in the Flows AVP
- 19. The AF accepts the notification.

### 4.3.3 Network Location Information (NetLoc)

The Network Location Information (NetLoc) is an optional function.





## 4.3.3.1

## AF Session Creation or Modification to Add a Media Component

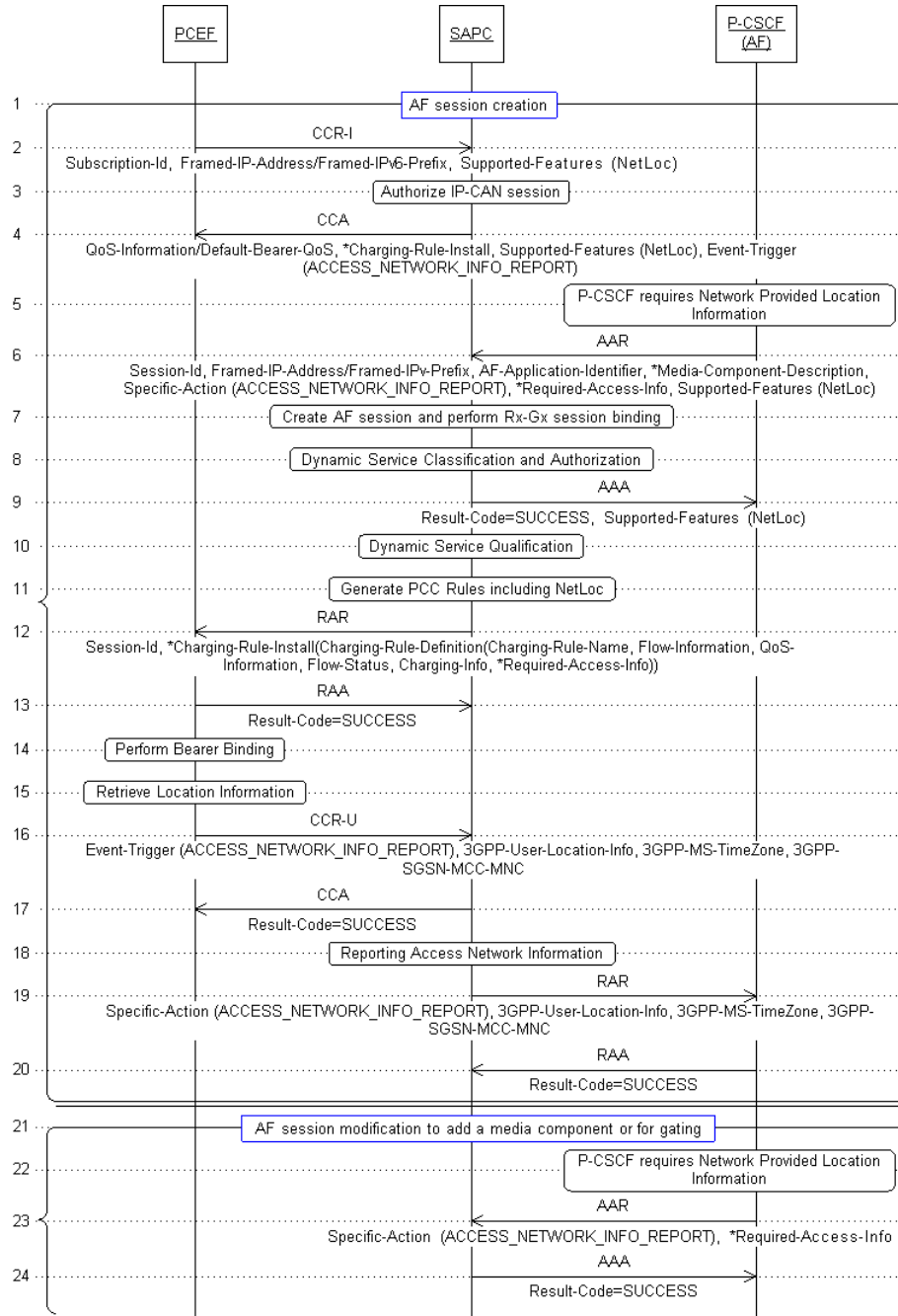


Figure 13 Network Location Information during AF Session Creation or Modification to Add a Media Component



## AF Session Creation

- 2. The SAPC receives a Gx CCR-Initial command from the PCEF indicating an IP-CAN session establishment, which includes the Supported-Features AVP with the NetLoc bit set.
- 3. The SAPC authorizes the IP-CAN session.
- 4. If the corresponding license for Netloc is active, the SAPC sends a CCA-Initial command to the PCEF including the Supported-Features AVP with the NetLoc bit set and the Event-Trigger AVP with ACCESS\_NETWORK\_INFO\_REPORT (45) (if this event is configured).

**Note:** If the corresponding license for Netloc is not active, the SAPC accepts IP-CAN session establishment and ignores the Netloc feature bit in Supported-Features AVP.

- 5. The AF requires the SAPC for the access network information (user location or MS timezone, or both) at the AF session establishment.
- 6. The AF sends an AAR command to the SAPC including the Supported-Features AVP with the NetLoc bit set, the Specific-Action AVP with the value ACCESS\_NETWORK\_INFO\_REPORT, and the Required-Access-Info AVP with the required access network information (USER\_LOCATION (0) or MS\_TIME\_ZONE (1)). Two instances of Required-Access-Info AVP are received in case both information types are required.
- 7. The SAPC creates the AF session and binds the AF session with the existing IP-CAN session.
- 8. The SAPC identifies the service corresponding to the AF session by performing the service classification and performs the service authorization of the previously identified service.
- 9. The SAPC sends an AAA command through the Rx interface including the Result-Code parameter with the value "SUCCESS" (code 2001) and the Supported-Features AVP with the NetLoc bit set. If the PCEF does not support the Network Location Information function, the following steps are not performed. For detailed information, see Section 4.3.3.6.1 on page 54.
- 10. The SAPC performs the dynamic service qualification to generate, for example, the QoS information that applies to the PCC rules.
- 11. The SAPC generates the PCC rules including Network Location Information required by the AF, if the PCEF supports the NetLoc function.
- 12. The SAPC sends an RAR command including the Required-Access-Info AVP inside the Charging-Rule-Definition AVP to the PCEF to request for the access network information, either with USER\_LOCATION (0) or MS\_TIME\_ZONE (1) value. Two instances of Required-Access-Info AVP are included in case both information type is required by the AF.



- 13. The PCEF accepts the installation of PCC rules and sends an RAA command in response.
- 14. The PCEF performs bearer binding.
- 15. The PCEF retrieves location information from the network.
- 16. The PCEF sends a CCR-Update command to the SAPC to report the access network information including the Event Trigger (ACCESS\_NETWORK\_INFO\_REPORT), the 3GPP-User-Location-Info AVP (if available) or the 3GPP-SGSN-MCC-MNC AVP (only used if 3GPP-User-Location-Info AVP is not available), and/or the 3GPP-MS-TimeZone AVP (if available).

**Note:** When the CCR-Update command includes only this Event Trigger, the IP-CAN session is not reauthorized.

- 17. The SAPC sends a CCA-Update command to the PCEF in response.
- 18. The SAPC determines to report the network information received to the AFs which requested NetLoc.

One CCR-U with Netloc may cause multiple Rx RARs towards all AFs which requested Netloc for that IP-CAN session.

- 19. The SAPC sends an RAR command to the AF to report the access network information by including the 3GPP-User-Location-Info AVP (if available), the 3GPP-MS-TimeZone AVP (if available), and the 3GPP-SGSN-MCC-MNC AVP (if 3GPP-User-Location-Info AVP is not available) and the Specific-Action AVP set to ACCESS\_NETWORK\_INFO\_REPORT.

If the SAPC receives several CCR-U commands with the ACCESS\_NETWORK\_INFO\_REPORT event trigger, for example one CCR-U for each PCC rule sent in previous Gx RAR, the first CCR-U with NetLoc information provokes RARs to all the AFs having requested NetLoc.

- 20. The AF sends an RAA command to the SAPC including the Result-Code parameter with the value "SUCCESS" (code 2001).

#### AF Session Modification to Add a Media Component or for Gating

- 22. The AF requires the SAPC for the access network information (user location or MS timezone, or both) at the AF session modification to add a media component.
- 23. The AF sends an AAR command to the SAPC, including the Specific-Action AVP with the value ACCESS\_NETWORK\_INFO\_REPORT and the Required-Access-Info AVP with the required access network information (USER\_LOCATION (0) or MS\_TIME\_ZONE (1)). Two instances of Required-Access-Info AVP are received in case both information types are required.
- 24. The SAPC accepts the message with an AAA command.



— The use case follows as described from step 10 to 20.

**Note:** The NetLoc request applies to all the new and updated PCC rules. If it is an AF session modification for gating, NetLoc is requested for the modified PCC rules.

#### 4.3.3.2

#### AF Session Modification to Remove a Media Component or Media Subcomponent

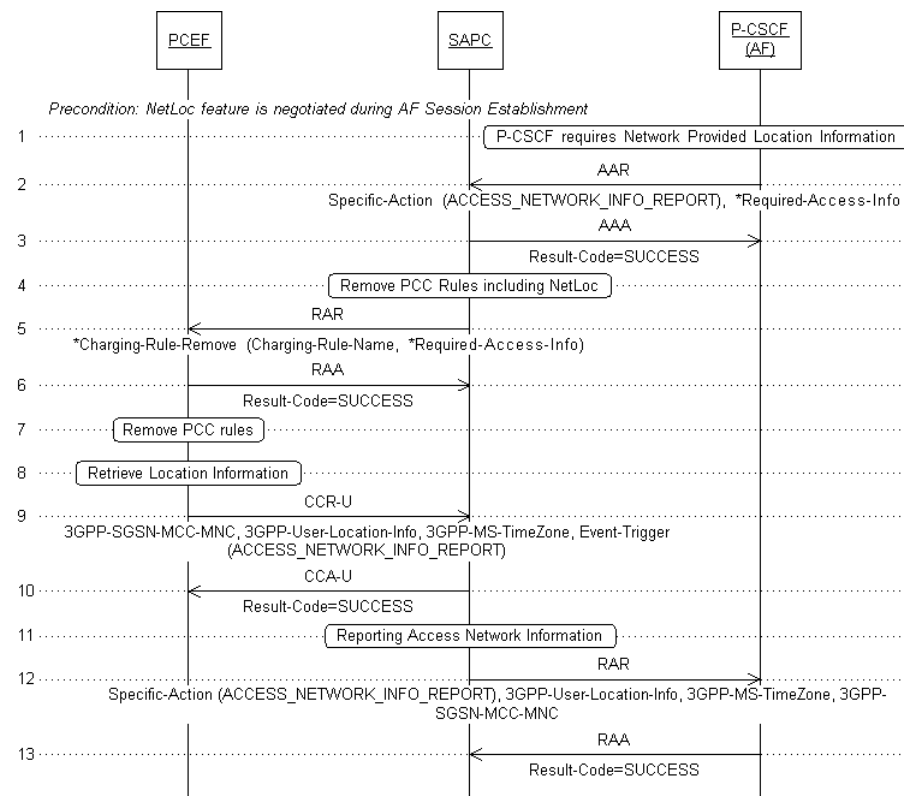


Figure 14 Network Location Information during AF Session Modification to Remove a Media Component or Media Subcomponent

The precondition is that the NetLoc function is negotiated during IP-CAN session establishment and AF session establishment. The SAPC sent the ACCESS\_NETWORK\_INFO\_REPORT event trigger during the IP-CAN session establishment.

- 1. The AF requires the SAPC for the access network information (user location or MS timezone, or both) at the AF session modification to remove a media component or a media subcomponent.
- 2. The AF sends an AAR command to the SAPC, including the Specific-Action AVP with the value ACCESS\_NETWORK\_INFO\_REPORT and the Required-Access-Info AVP with the required access network information (USER\_LOCATION (0) or MS\_TIME\_ZONE (1)). Two instances of



Required-Access-Info AVP are received in case both information types are required.

- 3. The SAPC sends an AAA command through the Rx interface including the Result-Code parameter with the value "SUCCESS" (code 2001).
- 4. The SAPC removes the PCC rules including Network Location Information.
- 5. The SAPC sends an RAR command including the Required-Access-Info AVP inside the Charging-Rule-Remove AVP to the PCEF to request for the access network information, either with USER\_LOCATION (0) or MS\_TIME\_ZONE (1) value. Two instances of Required-Access-Info AVP are included in case both information types are required by the AF.
- 6. The PCEF accepts the message with an RAA command.
- 7. The PCEF removes the PCC rules.
- 8-13. Same to step 15-20 of Section 4.3.3.1 on page 44.

#### 4.3.3.3

#### AF Session Termination

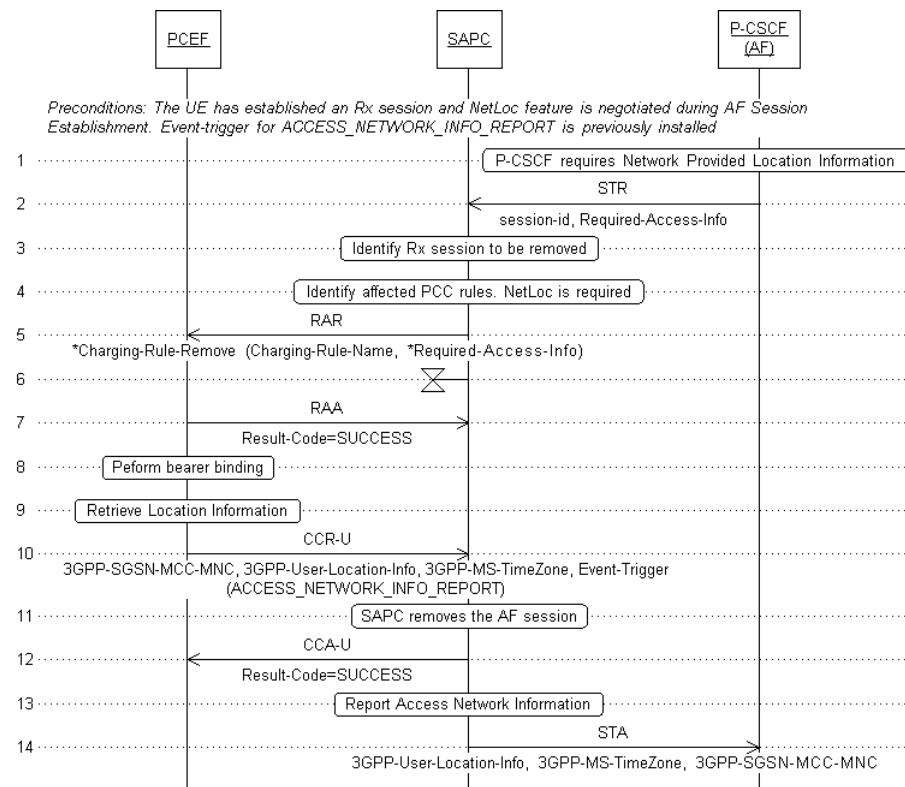


Figure 15 Network Location Information during AF Session Termination

- 1 The AF requires the SAPC for the access network information (user location or MS timezone, or both) at the AF session termination.



- 2 The AF sends an STR command to indicate the termination of the AF session. The STR command includes the Required-Access-Info AVP with the required access network information (USER\_LOCATION (0) or MS\_TIME\_ZONE (1)). Two instances of Required-Access-Info AVP are received in case both information types are required.
- 3 The SAPC identifies the session to be removed.
- 4 The SAPC identifies affected PCC rules.
- 5 The SAPC sends an RAR command including the Required-Access-Info AVP inside the Charging-Rule-Remove AVP to the PCEF to request for the access network information, either with USER\_LOCATION (0) or MS\_TIME\_ZONE (1) value. Two instances of Required-Access-Info AVP are received in case both information types are required.
- 6 The SAPC starts a timer to wait for CCR-Update with access network information.  
  
**Note:** If the timer expires before the SAPC receives CCR-U with access network information, the SAPC returns STA to the AF without any access network information and logs WARNING condition. Otherwise, the timer ends after sending STA message.
- 7 The PCEF accepts the removal of the PCC rules with an RAA answer.
- 8 The PCEF performs bearer binding.
- 9 The PCEF retrieves the location information.
- 10 The PCEF sends a CCR-U command to the SAPC to report the access network information including the Event Trigger (ACCESS\_NETWORK\_INFO\_REPORT), the 3GPP-User-Location-Info AVP (if available) or the 3GPP-SGSN-MCC-MNC AVP (only used if 3GPP-User-Location-Info AVP is not available), and/or the 3GPP-MS-TimeZone AVP (if available).  
  
**Note:** When the CCR-Update command includes only this Event Trigger, the IP-CAN session is not reauthorized.
- 11 The SAPC removes the AF session.
- 12 The SAPC accepts the CCR-U with CCA-U.
- 13 The SAPC determines to report the network information received to the AF which requested NetLoc.
- 14 The SAPC sends an STA command to the AF with the received access network information including the 3GPP-User-Location-Info AVP (if available) or the 3GPP-SGSN-MCC-MNC AVP (if 3GPP-User-Location-Info AVP is not available), and/or the 3GPP-MS-TimeZone AVP (if available).



The preconditions are that the UE has established an AF session, the NetLoc function is negotiated during the AF session establishment and the Event-Trigger for ACCESS\_NETWORK\_INFO\_REPORT is previously installed.

#### 4.3.3.4

#### IP-CAN Session Termination

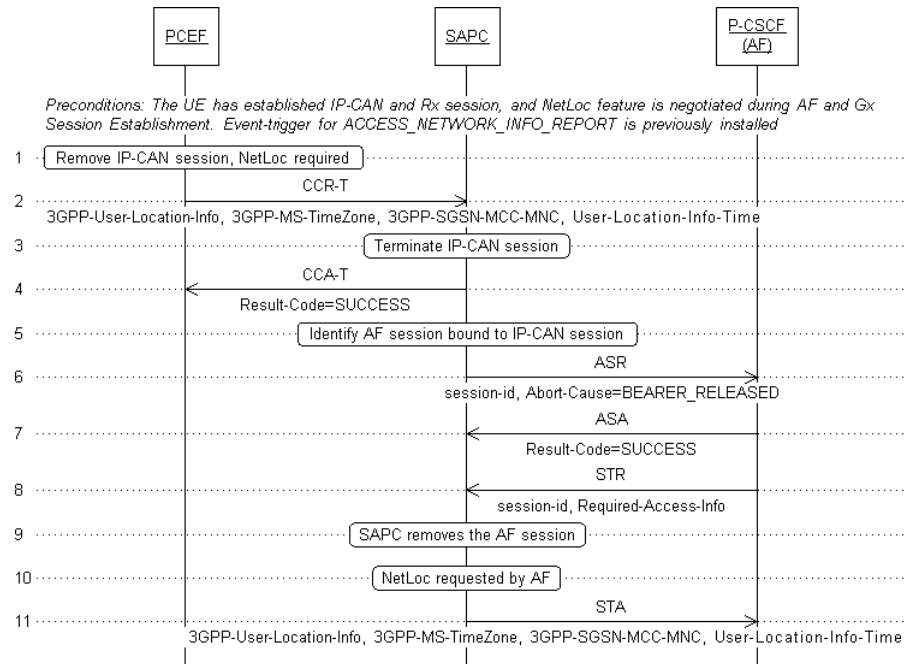


Figure 16 Network Location Information during IP-CAN Session Termination

- 1 The PCEF removes the IP-CAN session and retrieves the Network Location Information.
- 2 The PCEF sends a CCR-Terminate command with the access network information including the 3GPP-User-Location-Info AVP (if available) or the 3GPP-SGSN-MCC-MNC AVP (if 3GPP-User-Location-Info AVP is not available), the User-Location-Info-Time AVP (if available), and/or the 3GPP-MS-TimeZone AVP (if available).
- 3 The SAPC terminates the IP-CAN session.
- 4 The SAPC sends the CCA-Terminate answer to the PCEF, including the Result-Code parameter with the value "SUCCESS" (code 2001).
- 5 The SAPC identifies the AF session bound to the IP-CAN session.
- 6 The SAPC sends an ASR command to AF, including the Abort-Cause AVP set to BEARER\_RELEASED.
- 7 The AF answers with an ASA message.

- 8 The AF sends an STR command to request the termination of the AF session. The STR command includes the Required-Access-Info AVP with the required access network information (USER\_LOCATION (0) or MS\_TIME\_ZONE (1)). Two instances of Required-Access-Info AVP are received in case both information types are required.
- 9 The SAPC removes the AF session.
- 10 The SAPC determines to report the network information received to the AF which requested NetLoc.
- 11 The SAPC sends an STA command to the AF with the access network Information including the 3GPP-User-Location-Info AVP (if available) or the 3GPP-SGSN-MCC-MNC AVP (if 3GPP-User-Location-Info AVP is not available), the User-Location-Info-Time AVP (if available), and/or the 3GPP-MS-TimeZone AVP (if available).

#### 4.3.3.5

#### IP-CAN Bearer Release

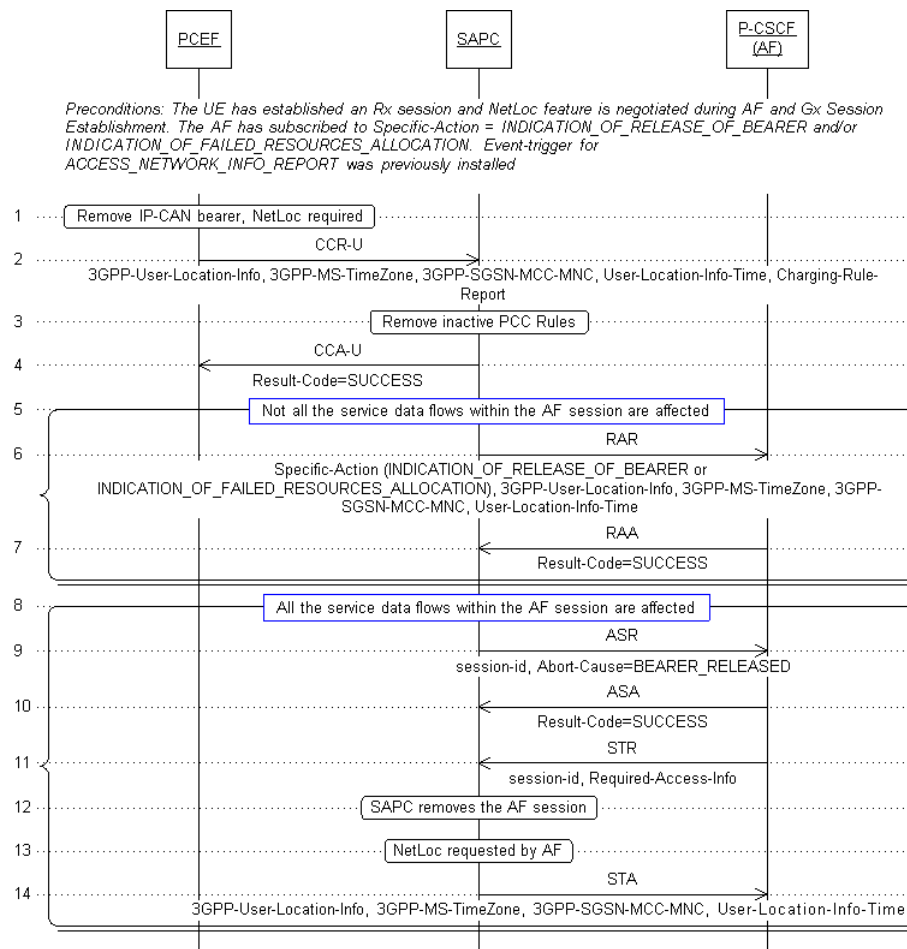


Figure 17 Network Location Information during IP-CAN Bearer Release





- 1. The PCEF removes the IP-CAN bearer and retrieves the Network Location Information.
- 2. The PCEF sends a CCR-U command to the SAPC with the access network information including the 3GPP-User-Location-Info AVP (if available) or the 3GPP-SGSN-MCC-MNC AVP (only used if 3GPP-User-Location-Info AVP is not available), the User-Location-Info-Time AVP (if available), and/or the 3GPP-MS-TimeZone AVP (if available), and Charging-Rule-Report AVP.
- 3. The SAPC removes inactive PCC rules.
- 4. The SAPC sends a CCA-U answer to the PCEF.
- 5-7. If not all the service data flows within AF session are affected, the SAPC sends an RAR command to the AF to report the access network information including the 3GPP-User-Location-Info AVP (if available) or the 3GPP-SGSN-MCC-MNC AVP (if 3GPP-User-Location-Info AVP is not available), the User-Location-Info-Time AVP (if available), the 3GPP-MS-TimeZone AVP (if available), and the Specific-Action AVP set to INDICATION\_OF\_RELEASE\_OF\_BEARER or INDICATION\_OF\_FAILED\_RESOURCES\_ALLOCATION.
- 8-16. If all the service data flows within AF session are affected, the steps are the same to step 6-11 of Section 4.3.3.4 on page 51.

### 4.3.3.6 Failure Handling of AF Session Creation or Modification

#### 4.3.3.6.1 Failure Handling when the PCEF does not Support NetLoc

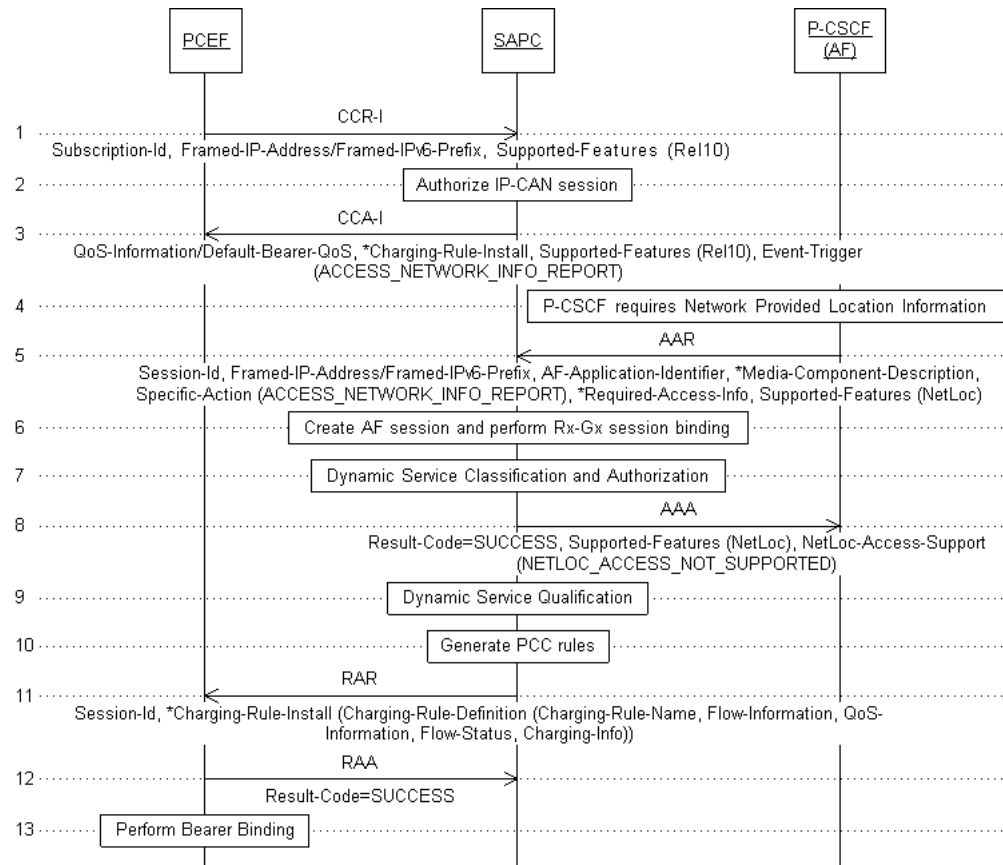


Figure 18 Failure Handling when the PCEF does not Support NetLoc

- 1 The SAPC receives a Gx CCR-Initial command from the PCEF indicating an IP-CAN session establishment without including the NetLoc feature bit set in the Supported-Features AVP.
- 2 The SAPC authorizes the IP-CAN session.
- 3 The SAPC accepts IP-CAN session establishment including the Supported-Features AVP without the NetLoc bit set, and the Event-Trigger AVP with ACCESS\_NETWORK\_INFO\_REPORT (45) (if this event is configured).
- 4 The AF requires the SAPC for the access network information (user location or MS timezone, or both) at the AF session establishment.
- 5 The AF sends an AAR command to the SAPC including the Supported Features AVP with the NetLoc bit set, the Specific-Action AVP with the value



ACCESS\_NETWORK\_INFO\_REPORT, and the Required-Access-Info AVP with the required access network information.

- 6 The SAPC creates the AF session and binds the AF session with the existing IP-CAN session.
- 7 The SAPC identifies the service corresponding to the AF session by performing the service classification and performs the service authorization of the previously identified service.
- 8 Because the PCEF does not support the NetLoc function, the SAPC sends an AAA command to the AF including a NetLoc-Access-Support AVP with the value of 0 (NETLOC\_ACCESS\_NOT\_SUPPORTED) through the Rx interface. The NetLoc bit in the Supported Features AVP is set.
- 9 The SAPC performs the dynamic service qualification to generate, for example, the QoS information that applies to the PCC rules.
- 10 The SAPC generates the PCC rules.
- 11 Because the PCEF does not support the NetLoc function, the SAPC sends an RAR command and the Charging-Rule-Install AVP to the PCEF to install the PCC rules, without the Required-Access-Info AVP within the Charging-Rule-Definition AVP.
- 12 The PCEF accepts the installation of PCC rules and sends an RAA command in response.
- 13 The PCEF performs bearer binding.

#### 4.3.3.6.2

#### Failure Handling when the IP-CAN Session does not Support NetLoc

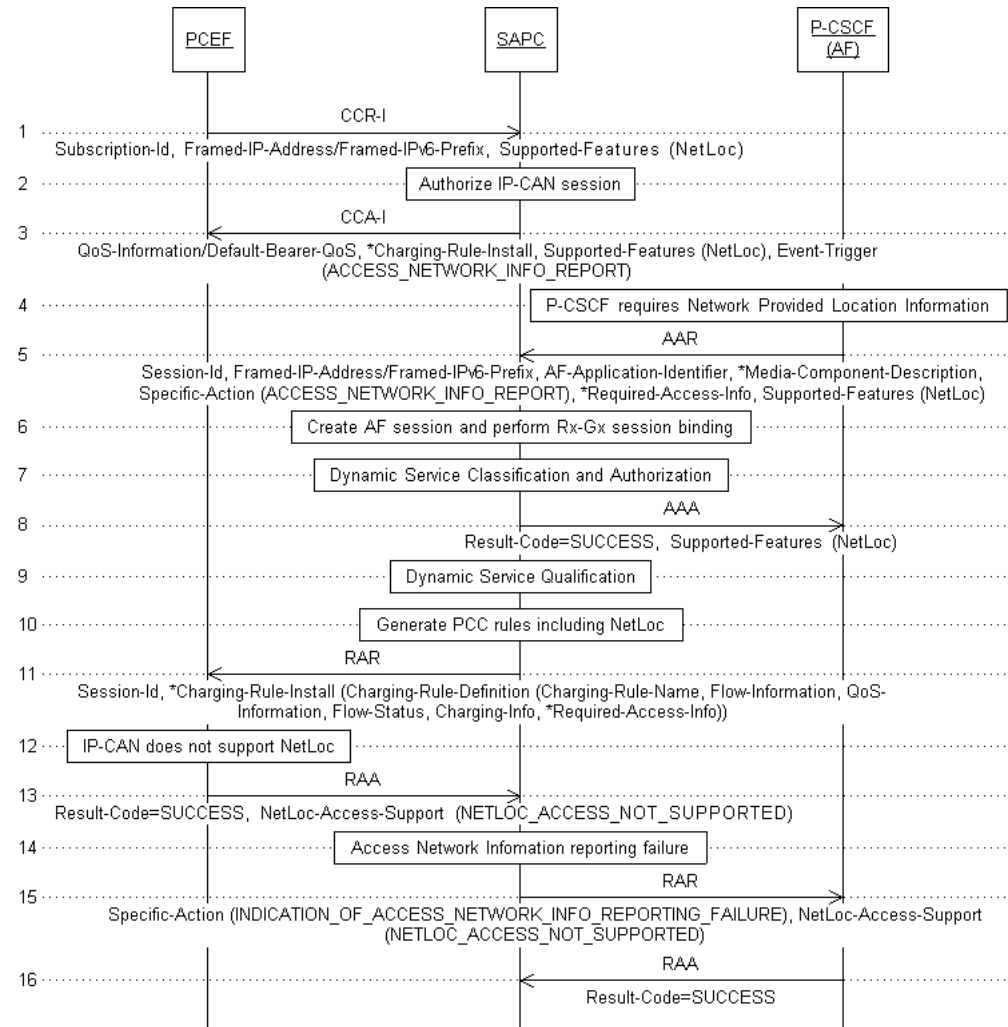


Figure 19 Failure Handling when the IP-CAN Session does not Support NetLoc

- 1-11. Same to step 1-11 of Section 4.3.3.1 on page 44.
- 12. The access network currently serving the UE does not support access network information retrieval.
- 13. The PCEF sends an RAA command to the SAPC including the NetLoc-Access-Support AVP with the value of 0 (NETLOC\_ACCESS\_NOT\_SUPPORTED).
- 14. The SAPC considers this situation as an Access Network Information Reporting failure.
- 15. The SAPC sends an RAR command to the AF including Specific-Action AVP set to INDICATION\_OF\_ACCESS\_NETWORK\_INFO\_REPORTING\_FAILURE



and the NetLoc-Access-Support AVP with value 0 (NETLOC\_ACCESS\_NOT\_SUPPORTED) as failure reason.

- 16. The AF sends an RAA command to the SAPC including the Result-Code parameter with the value "SUCCESS" (code 2001).

### 4.3.3.7 Failure Handling of AF Session Termination

#### 4.3.3.7.1 Failure Handling when the PCEF does not Support NetLoc

This use case is similar to the AF Session Creation in Section 4.3.3.6.1 on page 54, but with the following difference:

During AF session termination, the SAPC answers with an STA command to the AF including the NetLoc-Access-Support AVP with value 0 (NETLOC\_ACCESS\_NOT\_SUPPORTED) as failure reason. For the AF session termination procedure, see Section 4.3.3.3 on page 49.

#### 4.3.3.7.2 Failure Handling when the IP-CAN Session does not Support NetLoc

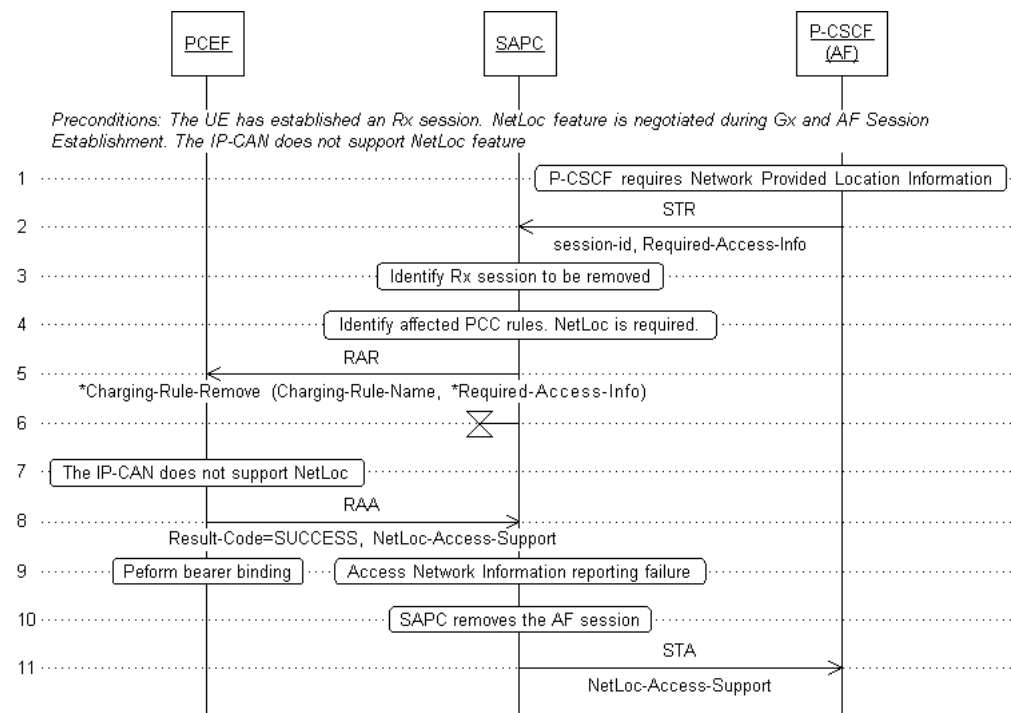


Figure 20 Failure Handling of AF Session Termination when the IP-CAN Session does not Support NetLoc

- Step 1-5. Same to step 1-5 of Section 4.3.3.3 on page 49.
- 6. The access network currently serving the UE does not support access network information retrieval.

- 7. The PCEF accepts the removal of PCC rules and sends an RAA command in response. The RAA command includes the NetLoc-Access-Support AVP set to the value of 0 (NETLOC\_ACCESS\_NOT\_SUPPORTED) and the Result-Code parameter with the value "SUCCESS" (code 2001).
- 8. The SAPC considers the situation as an access network information reporting failure.
- 9. The SAPC removes the AF session.
- 10. The SAPC sends an STA command to the AF including a NetLoc-Access-Support AVP with the value of 0 (NETLOC\_ACCESS\_NOT\_SUPPORTED).

## 4.4 IMS Related Procedures

### 4.4.1 SIP Forking

The following figure shows the signalling flow that takes place when the IMS network performs SIP forking and the AF (P-CSCF) receives provisional responses from more than one possible contact destination. In this particular traffic case, the UE initiates a voice-over-LTE call setup towards a remote UE that has two contact addresses registered in the IMS network. Each terminating end point initiates an early dialog and request authorization and resource reservation to the SAPC. Finally the remote party answers the call.

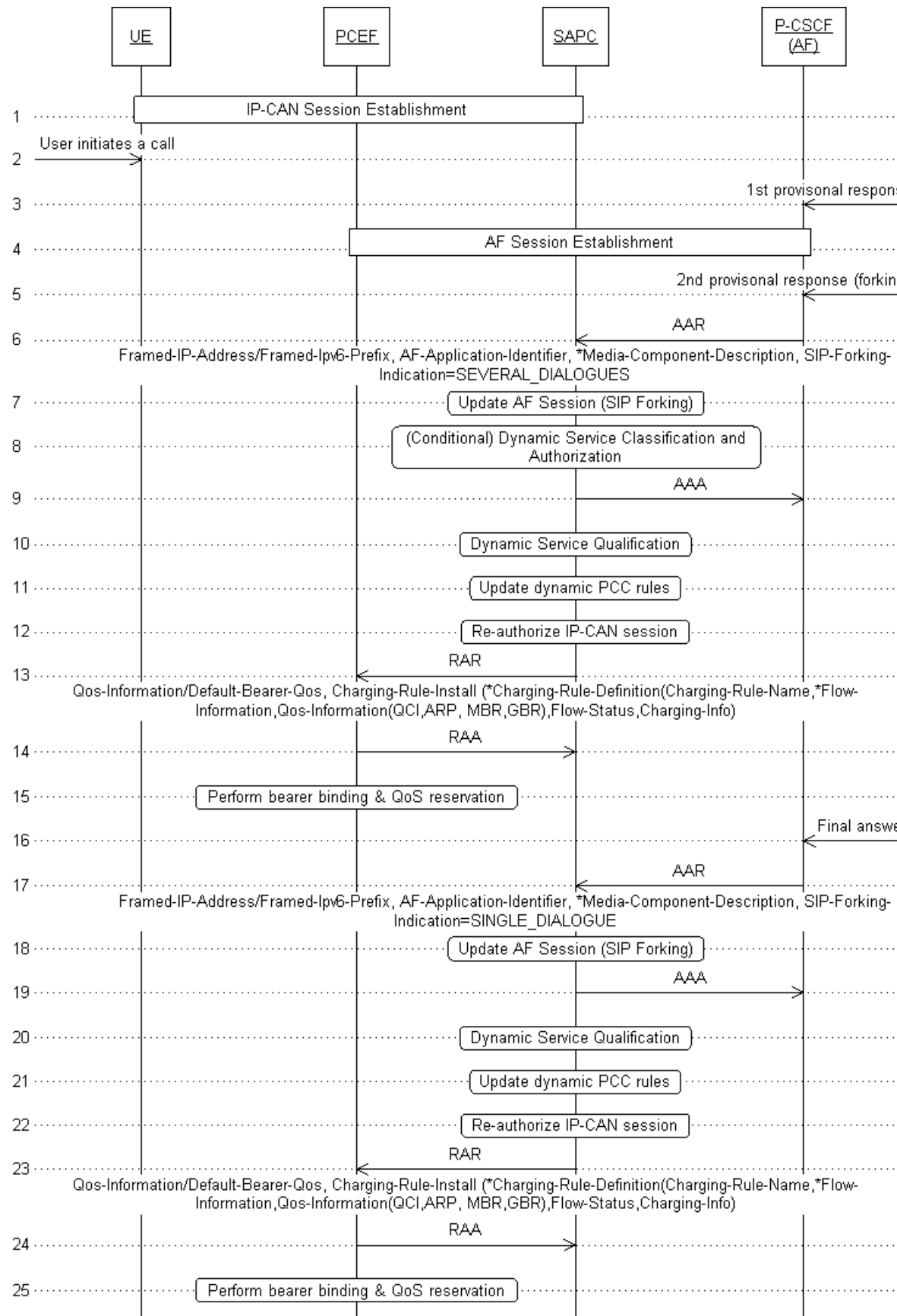


Figure 21 SIP Forking

- 1. The UE has established an IP-CAN session.
- 2. The UE initiates a voice-over-LTE call setup towards a remote UE that has two contact addresses registered in the IMS network.
- 3. The AF (P-CSCF) receives the provisional response from one of the possible contact destinations.
- 4. The AF performs the session establishment procedure to request authorization and resource reservation to the SAPC, as detailed in Section 4.1.1 on page 30. For this traffic case, as an example, the AAR command includes one media component of type AUDIO, with a bandwidth requirement of 29 kbps. The SAPC generates two dynamic PCC rules: one for the RTP media sub-component, and another PCC rule for the RTCP media sub-component.
- 5. The AF (P-CSCF) receives the provisional response from another possible contact destination because of forking.
- 6. The SAPC receives an AAR message from the AF to modify an existing AF session including the session identifier and the SIP-Forking-Indication AVP set to the value SEVERAL\_DIALOGUES. The AF provides the service information for this provisional response within the Media-Component-Description AVP(s). For this traffic case, as an example, the AAR command includes one media component of type AUDIO, with a bandwidth requirement of 41 kbps.
  - If the second provisional response contains additional media (for example, VIDEO), the AAR command contains a Media-Component-Description AVP with a new ordinal number in the Media-Component-Number AVP.
- 7. The SAPC updates the AF session state taking into account that this is a provisional response because of forking. This means that the SAPC does not overwrite the existing session information with the information received from the AF, but the SAPC needs to merge the information received from both forking legs.
- 8. If the SAPC identifies that the updated AF session contains new media components, the SAPC performs the dynamic service classification and authorization of the new media.
- 9. The SAPC responds to the AF with an AA-Answer command indicating the operation result. If the request is successfully, the Result-Code AVP is set to the value SUCCESS. If the request is unsuccessful, an error code is indicated.
- 10. The SAPC determines the QoS and Charging information so that the SAPC authorizes the maximum bandwidth required by any of the dialogues, but not the sum of the bandwidths required by all dialogues.
  - If the second provisional response contains additional media (for example, VIDEO), the SAPC also determines the QoS and Charging information associated with any additional dynamic service.





- 11. The SAPC updates the installed dynamic PCC rules for the first provisional response, and adds the additional service data flow filters corresponding to the second provisional response, so that the QoS authorized for a media component is equal to the highest QoS requested for that media component by any of the forked responses. For this traffic case, as an example, the MBR/GBR is set to 41 kbps.
  - If the second provisional response contains additional media (for example, VIDEO), the SAPC generates new dynamic PCC rules.
- 12-15. The SAPC performs the reauthorization of the IP-CAN session and provisions the policy control and charging information to the PCEF.
- 16. When the terminating party answers the call, the AF (P-CSCF) receives the final SIP response.
- 17. The SAPC receives an AAR message from the AF to modify an existing AF session with no SIP-Forking-Indication AVP or with the SIP-Forking-Indication AVP set to the value SINGLE\_DIALOGUE. The AF provides the full service information for the SIP session within the Media-Component-Description AVP(s), including the applicable Flow-Description AVP(s) and Flow-Status AVP(s).
- 18. The SAPC updates the AF session state to match the requirements of the service information within this final AAR message only.
- 19. The SAPC responds to the AF with an AA-Answer command indicating the operation result.
- 20-22. The SAPC determines the QoS and Charging information according to the service information provided in the final AAR message, updates the installed dynamic PCC rules and performs the reauthorization of the IP-CAN session.
- 23-25. The SAPC provisions the policy control and charging information to the PCEF.

#### 4.4.2 Single Radio Voice Call Continuity

The following figure shows the signalling flow that takes place when dynamic PCC rules cannot be installed/activated or enforced at the PCEF, and the main actions taken by the SAPC to perform dynamic policy control.

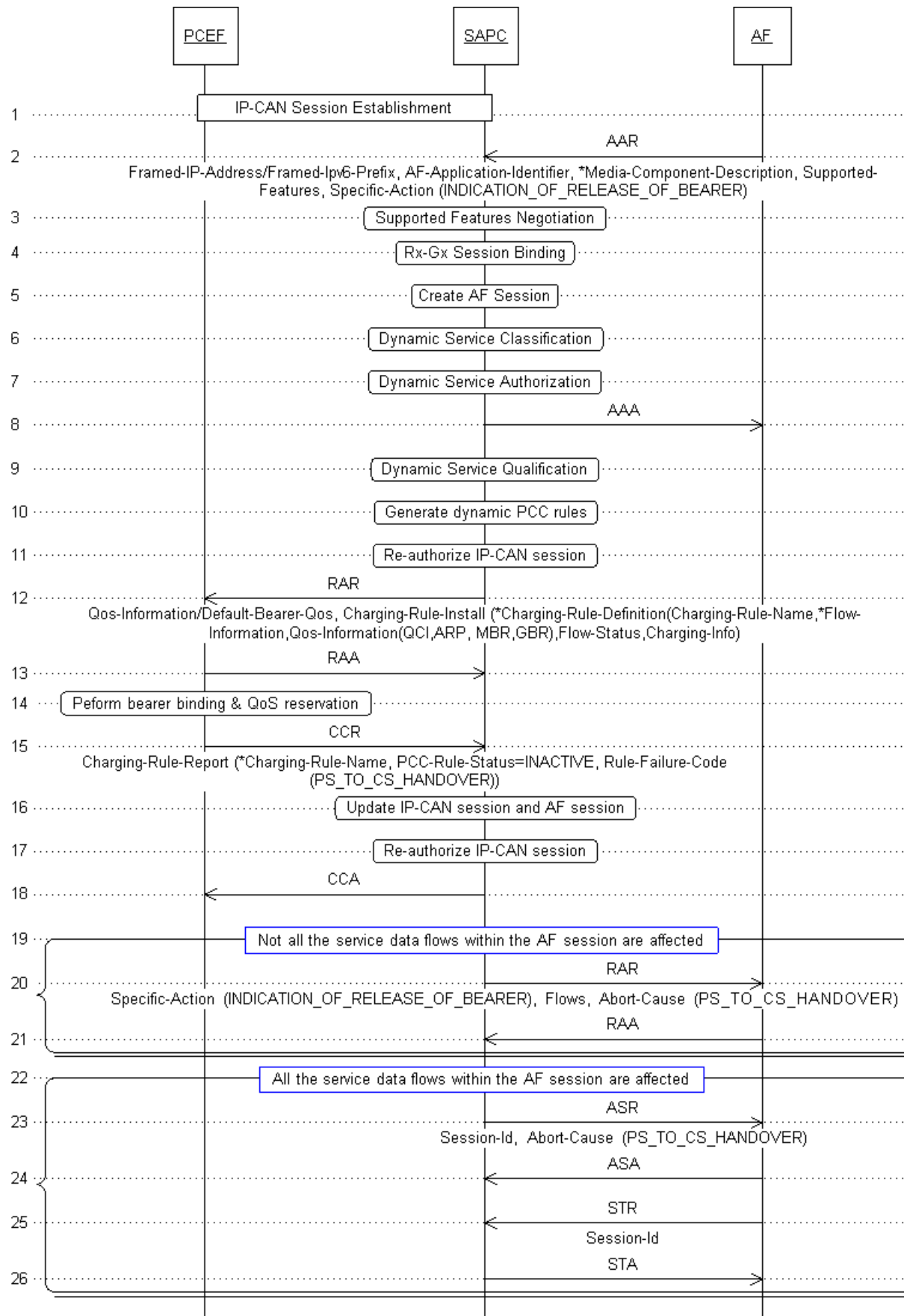


Figure 22 Single Radio Voice Call Continuity



This traffic case is similar to the one explained in section Service Data Flow Deactivation. The main differences are highlighted below.

- 2. In addition to the service information, the SAPC receives the list of bearer events that the AF requests to be notified in the *Specific Action AVP*, which includes the value *INDICATION\_OF\_RELEASE\_OF\_BEARER*.
- 15. The PCEF sends a CCR-Update that includes a *Charging-Rule-Report AVP* with the *PCC-Rule-Status AVP* set to the value *INACTIVE*, the list of failed PCC rules, and the *Rule-Failure-Code AVP* set to the value *PS\_TO\_CS\_HANDOVER*. This indicates to the SAPC that the PCC rule(s) could not be maintained because of PS to CS handover.
- 20. If not all the service data flows within the AF session are affected and the AF has requested to be notified, SAPC sends a RAR message to the AF with the *Abort-Cause AVP* set to the value *PS\_TO\_CS\_HANDOVER*, the list of deactivated IP Flows encoded in the *Flows AVP* and the *Specific-Action AVP* set to *INDICATION\_OF\_RELEASE\_OF\_BEARER*.
- 23. If all the service data flows within the AF session are deactivated, the SAPC informs the AF by sending an ASR command, including the *Abort-Cause AVP* set to the value *PS\_TO\_CS\_HANDOVER*. The SAPC sends the ASR command in this case regardless of whether the AF has previously subscribed to any notification event.

## 4.5 Dynamic Policy Control Triggered by Application Service Detection

This chapter shows the most common traffic cases that may happen in network scenarios where the AF does not provide specific information about the IP flows required to deliver the service (the media component information is not present), but merely provides an application identifier that triggers the activation of a dynamic service in the SAPC.

A typical example is when a DPI node, such as the SASN (acting as AF) detects the start of an application service and reports this event to the SAPC over the Rx interface. Then the SAPC does not generate dynamic PCC rules, but reevaluates the applicable policies for the IP-CAN session based on the received information about the service detection. As a result, the SAPC may, for example, upgrade the QoS of the default bearer to accommodate the application service, terminate the IP-CAN session (for example in the case of tethering) or reduce the assigned QoS for that service (for example, P2P service throttling).

### 4.5.1 Dynamic QoS Control based on Detected Service

This traffic case shows how the SAPC upgrades the QoS of the default bearer when a SASN/DPI node detects the start of a streaming service. In addition, the SAPC can also request the PCEF to initiate the establishment of a dedicated bearer for the delivery of the service.

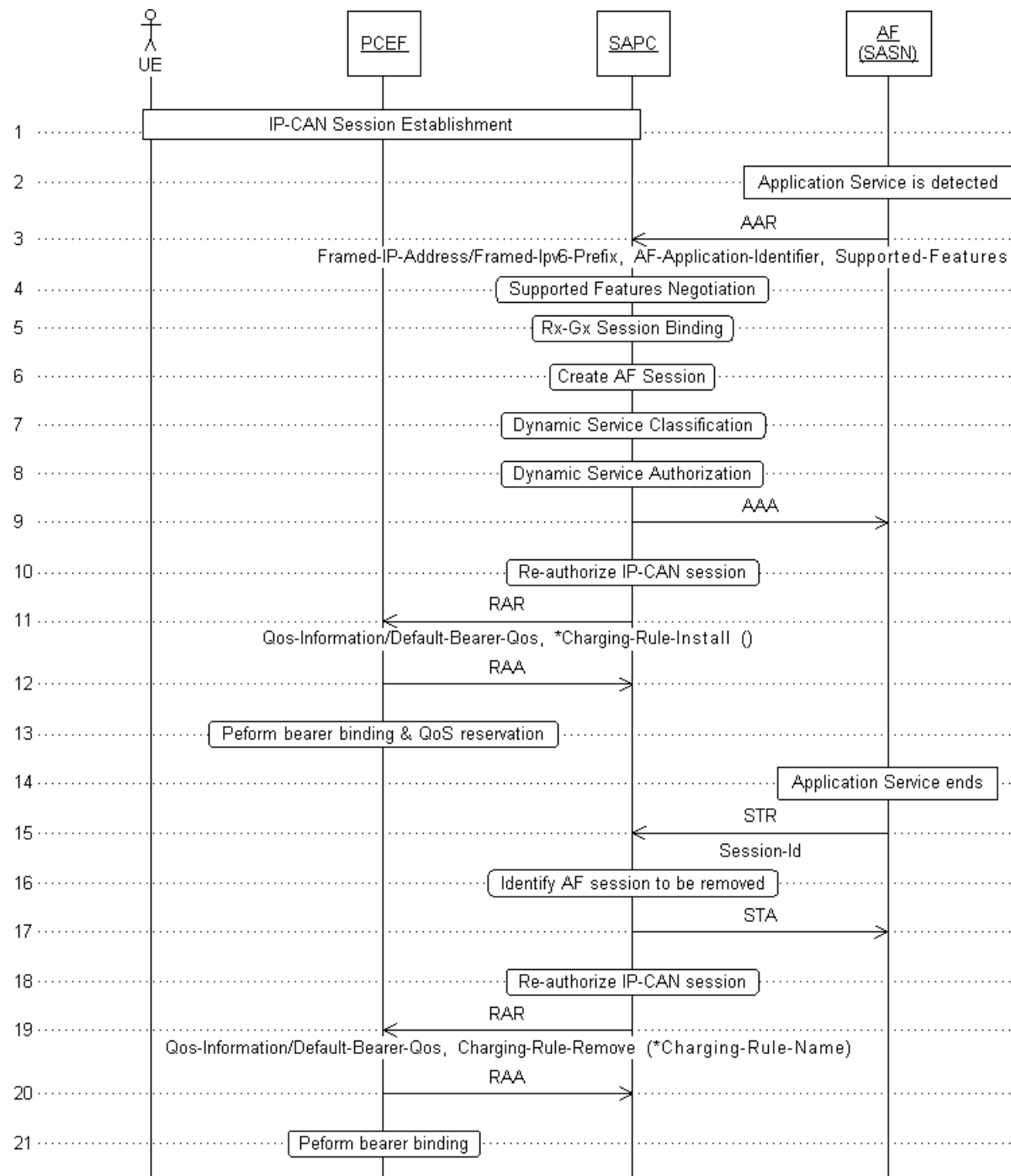


Figure 23 Dynamic QoS based on Detected Service

- 1. The UE has established an IP-CAN session.
- 2. The AF (SASN) detects the start of an application service through packet inspection.



- 3. The AF (SASN) reports the activation of an application service to the SAPC using the Rx interface. The SAPC receives an AAR message from the AF to establish a new AF session. The main information that the AF provides is:
  - The IPv4 or IPv6 address that identifies the UE terminal.
  - The AF-Application-Identifier AVP that identifies the application service that has been detected.
  - The set of supported features required for the AF session, in the Supported-Features AVP.
- Steps 4–9 are similar to the ones explained in section AF Session Establishment.
- 10. The SAPC performs reauthorization of the IP-CAN session based on the information received about the detected service, the subscription information, and the applicable policies. For this use case, the SAPC upgrades the QoS for the default bearer. In addition, the SAPC may also authorize other static or pre-configured services for the IP-CAN session. This permits for example to select pre-configured PCC rules defined in the SAPC that are installed when a notification of service activation is received from the AF. These pre-configured PCC rules can have a QCI different than the QCI of the default bearer, and the installation of these PCC rules triggers the establishment of a dedicated bearer.
- 11. The SAPC sends to the PCEF the quality of service for the default bearer and optionally additional PCC rules and QoS information that result from the policy evaluation.
- 12. The PCEF accepts the modification of the default bearer and the installation/removal of PCC rules.
- 13. The PCEF performs the bearer binding and modifies the default bearer. In addition, the PCEF initiates a dedicated bearer if there is not an existing one that fulfills the quality of service requirements of the provisioned PCC rules.
- 14. The AF (SASN) detects the stop of the application service through packet inspection.
- 15. The AF (SASN) notifies the stop of the application service to the SAPC sending an STR message that includes the session identifier,
- 18. The SAPC performs reauthorization of the IP-CAN session based on condition that the application service has stopped. For this use case, the SAPC reevaluates the QoS to apply to the default bearer and downgrades the QoS back to the original state. In addition, the SAPC may also remove other static or pre-configured services from the IP-CAN session. This permits the SAPC to trigger the release of the dedicated bearer that was set up when the application service was detected.
- 19. The SAPC sends to the PCEF the quality of service for the default bearer and removes the PCC rules.



- 21. The PCEF performs the bearer binding and modifies the default bearer. If applicable, the PCEF also removes the PCC rules and releases the dedicated bearer.

#### **4.5.2 Deactivation of IP-CAN Session on Detection of Tethering Traffic**

This traffic case shows an example of IP-CAN session termination initiated by the SAPC upon detection of tethering traffic.

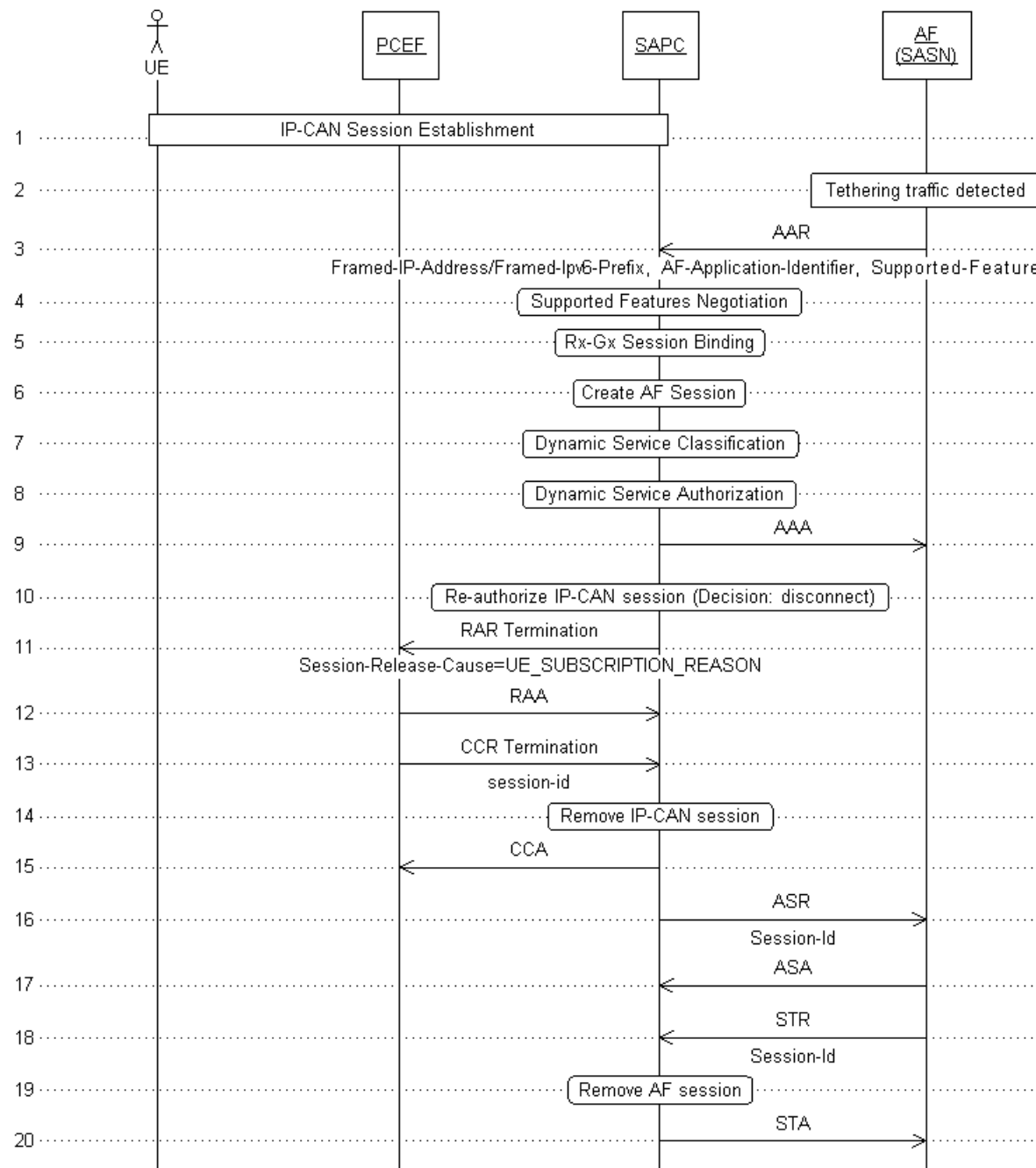


Figure 24 Deactivation of IP-CAN Session on Detection of Tethering Traffic

- 1. The UE has established an IP-CAN session.
- 2. The AF (SASN) detects the start of tethering traffic through packet inspection.



- 3. The AF (SASN) reports the detection of tethering traffic to the SAPC using the Rx interface. The SAPC receives an AAR message from the AF to establish a new AF session. The main information that the AF provides is:
  - The IPv4 or IPv6 address that identifies the UE terminal.
  - The AF-Application-Identifier AVP that identifies the application service that has been detected (tethering).
  - The set of supported features required for the AF session, in the Supported-Features AVP.
- Steps 4–9 are similar to the ones explained in section AF Session Establishment.
- 10. The SAPC performs reauthorization of the IP-CAN session based on the information received about the detected service. For this use case, the SAPC decides to reject the IP-CAN session.
- 11. The SAPC sends an RAR message to the PCEF with Session-Release-Cause AVP set to the value UE\_SUBSCRIPTION\_REASON, to request the termination of the IP-CAN session.
- 12-13. The PCEF answers with an RAA command and sends a CCR Termination message to the SAPC.
- 16. The SAPC informs the AF about the IP-CAN session termination by sending an ASR command on each active Rx Diameter session.

## 4.6 Handling of Race Conditions Related to Multiple AF Requests

The following signalling flow shows how the SAPC handles diameter race condition errors related to multiple AF requests for the same in an IP-CAN session.

In this particular traffic case, the UE (a first responder such as Police, Fire Fighter or Medical Emergency) access the Public Safety LTE network, and is granted a dedicated communication control channel to the Public Safety Agency (PSA). When an incident occurs, the PSA (AF) elevates the priority of the control channel to the UE, and also establishes additional dedicated bearers for data transmission. Moreover, the PSA (AF) requires the SAPC to notify the successful outcome of the resource allocation procedure related to the public safety services.

This results in the AF performing multiple Rx session creation and modification requests in short succession for the same subscriber and IP-CAN session that may overlap in time with CCR-U messages from the PCEF.



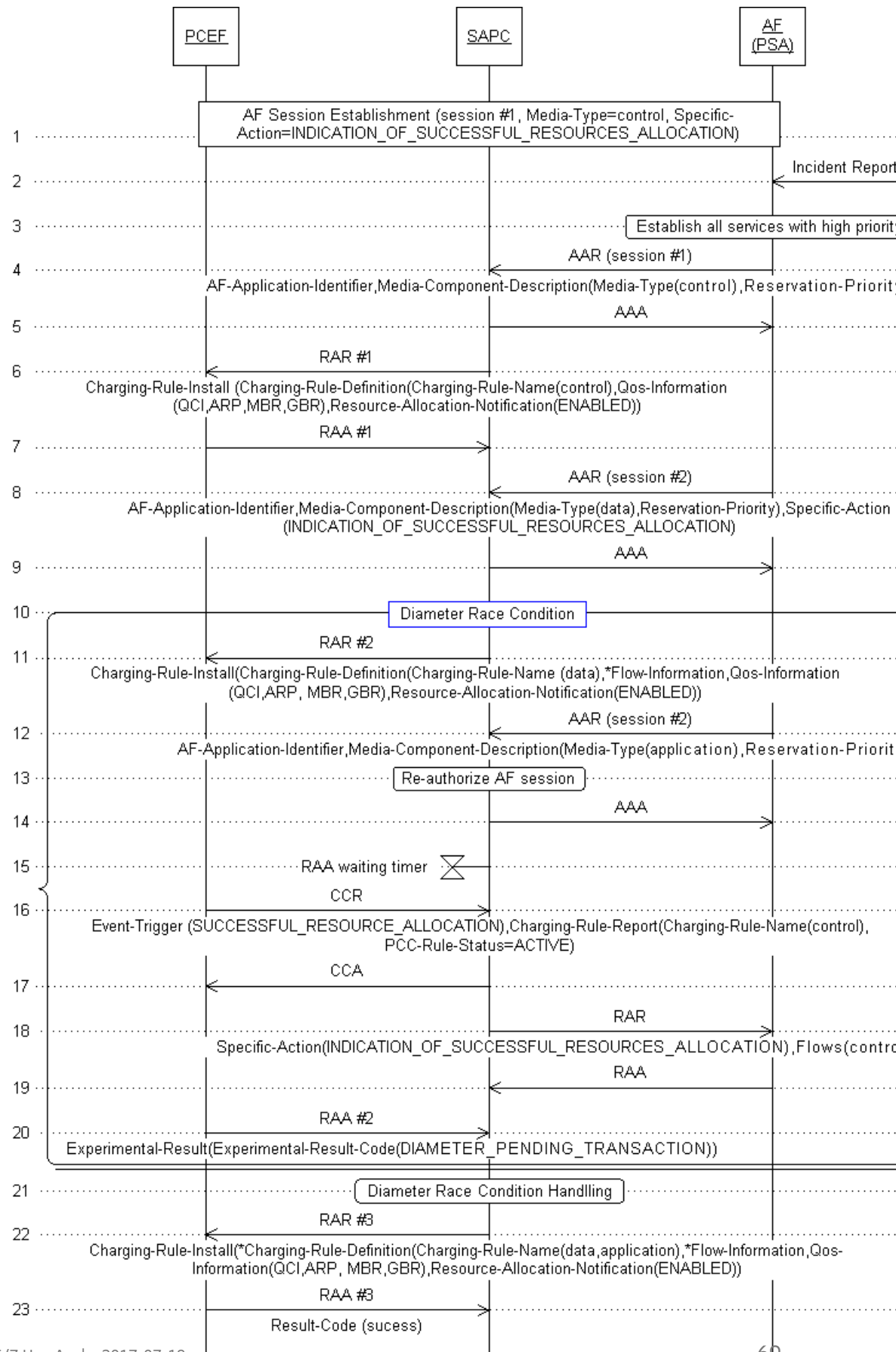


Figure 25 Handling of Race Conditions Related to Multiple AF Requests

- 1. The AF performs the session establishment procedure, as detailed in Section 4.1.1 on page 30. In this traffic case, the AAR command includes one media component of type CONTROL, and the AF subscribes to notifications of successful resources allocation.
- 2-3. The AF requires the establishment of high priority services for the subscriber, for example due to reception of an incident report from the Public Safety Application (PSA).
- 4. The AF sends an AAR message to the SAPC to modify the priority level of the CONTROL media path.
- 5. The SAPC updates the AF session and responds with an AAA command to the AF.
- 6. The SAPC sends an RAR message to the PCEF to update the installed dynamic PCC rules for the CONTROL service with higher priority level. The RAR message includes the Resource-Allocation-Notification AVP set to ENABLED to indicate the PCEF that a confirmation about resource allocation is required.
- 7. The PCEF accepts the installation of the PCC rules.
- 8. The SAPC receives an AAR message from the AF to establish a new AF session including a media component of type DATA, and the request to provide a notification when the resources associated to the corresponding service information have been allocated.
- 9. The SAPC binds the new AF session to the same IP-CAN session that is associated to the AF session established in step 1. The SAPC performs a re-authorization of the AF session and responds with an AAA command to the AF.

#### **Diameter Race Condition**

- 11. The SAPC sends an RAR message to the PCEF to install the dynamic PCC rules for the DATA service with high priority level, including the indication to the PCEF that a confirmation about resource allocation is required. This message overlaps in time with a PCEF-initiated IP-CAN session modification in step 16, creating a race condition situation.
- 12. The SAPC receives an AAR message from the AF to add a media component of type APPLICATION to the AF session established in step 8.
- 13-14. The SAPC updates the AF session and responds with an AAA command to the AF.
- 15. The SAPC detects that there is a previous Gx RAR pending to be acknowledged for the same IP-CAN session, and starts a timer to wait for the RAA message. No Gx RAR message is sent to the PCEF at this point in time.
- 16. The SAPC receives the CCR-U message with the notification from the PCEF that the resources associated to the CONTROL service information



have been successfully allocated. This message overlaps in time with a SAPC-initiated IP-CAN session modification in step 11, creating a race condition situation

- 17. The SAPC accepts the notification and does not perform a policy re-evaluation if the CCR command only includes the Event-Trigger AVP set to SUCCESSFUL\_RESOURCE\_ALLOCATION.

**Note:** In general, the SAPC performs a reauthorization of the IP-CAN session based on the information received in the CCR-U message, and sends the updated policy control information in the CCA. However, if the AF has requested the SAPC to report the access network information for this IP-CAN session (for example in step 12), the SAPC skips policy evaluation for static, preconfigured, and dynamic services in the IP-CAN session re-authorization.

- 18-19. The SAPC notifies the AF that the resources associated to the CONTROL service information have been successfully allocated.
- 20. As a result of the race condition situation, the PCEF rejects the RAR message from the SAPC in step 11 and sends an RAA with an Experimental-Result AVP including the Experimental-Result-Code AVP set to DIAMETER\_PENDING\_TRANSACTION.
- 21. The SAPC stops the timer set in step 15. If the configured maximum number of reattempts is not reached, the SAPC performs a reauthorization of the IP-CAN session and determines the policy control information pending to be sent to the PCEF (for details see [Access and Charging Control \(Gx\)](#)).
- 22. The SAPC sends a re-attempting RAR message to the PCEF with the latest policy information. In this case, the SAPC includes the PCC rules to be installed for the DATA service and also for the APPLICATION service.
- 23. The PCEF accepts the installation of the PCC rules and returns an RAA message including the Result-Code AVP with value SUCCESS.

## 4.7 Dynamic Policy Control Error Handling

This section describes how the SAPC handles protocol errors and session failures.

Table 1 Error Handling

Error Condition	Action	Code
The SAPC receives an AAR and the corresponding IP-CAN session is not found, or more than one matching IP-CAN session is found.	The SAPC rejects the AF session establishment and returns an AAA indicating an error	Experimental-Result-Code AVP set to IP-CAN_SESSION_NOT_AVAILABLE 5065



Error Condition	Action	Code
The SAPC receives an AAR that cannot be complied owing to an internal error.)	The SAPC rejects the transaction and returns an AAA indicating an error	Result-Code AVP set to UNABLE_TO_COMPLY 5012
The SAPC receives an AAR with a mandatory parameter missed (for example the UE IP address in the AF session establishment)	The SAPC rejects the transaction and returns an AAA indicating an error	Result-Code AVP set to DIAMETER_MISSING_AV P 5005
The SAPC receives an AF session establishment request with Rx interface Release 7 standard	The SAPC rejects the AF session establishment and returns an AAA indicating an error	Result-Code AVP set to DIAMETER_MISSING_AV P 5005
The SAPC receives an AF session establishment request with Rx interface Release 8 standard	The SAPC rejects the AF session establishment and returns an AAA indicating an error	Result-Code AVP set to DIAMETER_INVALID_AV P_VALUE 5004
The SAPC receives an AAR with the Rx-Request-Type AVP set to UPDATE_REQUEST (1) but the SAPC does not have an existing Rx session to be modified.	The SAPC rejects the transaction and returns an AAA indicating an error	Result-Code AVP set to DIAMETER_UNKNOWN_SESSION_ID 5002
The SAPC receives an AAR with the Rx-Request-Type AVP set to PCSCF_RESTORATION (2).	The SAPC rejects the transaction and returns an AAA indicating an error	Result-Code AVP set to DIAMETER_INVALID_AV P_VALUE 5004
The SAPC receives an STR and the AF session is not found (although the IP-CAN session exists)	The SAPC returns a STA indicating an error	Result-Code AVP set to DIAMETER_UNKNOWN_SESSION_ID 5002



Error Condition	Action	Code
The SAPC receives an AAR and the corresponding service is not authorized	The SAPC rejects the transaction and returns an AAA indicating an error	Experimental-Result-Code AVP set to REQUESTED_SERVICE_NOT_AUTHORIZED 5063
The SAPC receives an AAR with new media information and no dynamic service is successfully classified	The SAPC rejects the AF session establishment or modification and returns an AAA indicating an error	Experimental-Result-Code AVP set to REQUESTED_SERVICE_NOT_AUTHORIZED 5063
The SAPC receives an AAR to remove a media component and the AF session is not found.	The SAPC rejects the AF session establishment and returns an AAA indicating an error	Result-Code AVP set to DIAMETER_UNKNOWN_SESSION_ID 5002
The SAPC receives a DIAMETER_UNKNOWN_SESSION_ID error result in the Rx RAA message from the AF	The SAPC deletes the AF session and sends a Gx RAR message towards PCEF to remove the corresponding PCC rules	
The SAPC receives any error result in the ASA message from the AF	The SAPC deletes the AF session	
The SAPC receives a DIAMETER_UNKNOWN_SESSION_ID error result in the Gx RAA message from the PCEF	The SAPC deletes the IP-CAN session, and terminates the related AF sessions by sending an ASR command.	DIAMETER_AUTHORIZATION_REJECTED = 5003





## Reference List

### Ericsson Documents

- [1] Access and Charging Control (Gx)
- [2] Availability and Scalability
- [3] Bearer QoS and Bandwidth Management
- [4] Rx Interface Description
- [5] Subscription and Policy Management

### Standards

- [6] Policy and Charging Control signalling flows and QoS parameter mapping, 3GPP TS 29.213.
- [7] IP Multimedia Subsystem (IMS) emergency sessions, 3GPP TS 23.167.