Final draft **ETSI ES 282 003** V2.0.0 (2008-03)

Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control Sub-System (RACS): Functional Architecture

ETSI

Reference

RES/TISPAN-02036-NGN-R2

Keywords

architecture, control, system

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00   Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or
perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF).
In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive
within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status.
Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This ETSI Standard (ES) has been produced by ETSI Technical Committee Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN), and is now submitted for the ETSI standards Membership Approval Procedure.

The present document describes the architecture of the Resource and Admission Control Sub-System (RACS) identified in the overall TISPAN NGN architecture.

1 Scope

The present document describes the functional architecture for the Resource and Admission Control Sub-System (RACS), in TISPAN NGN Release 2, in line with the service requirements described in TS 181 005 [1] and with the QoS Requirements described in TS 181 018 [13]. Moreover, it further indicates high level stage 2 requirements in order to allow the description of its functional operation.

The functional architecture and system description developed in the present document is based on the Release 2 requirements for RACS developed in ES 282 001 [2].

RACS is the TISPAN NGN Sub-System responsible for the implementation of policy-based transport control features, by using procedures and mechanisms that handle resource reservation and admission control for both unicast and multicast traffic in access and core networks.

Besides acting as a Resource Control Framework, RACS also includes support for controlling Network Address Translation (NAT) at the edge of networks and for assisting in remote NAT traversal.

Furthermore, RACS also covers aspects related to the derivation, modification, and installation of traffic policies, end to end quality of service, transport-level charging. and overload control.

Hereinafter, the restrictions applicable to some RACS NGN topics for the present document are listed:

- the CPN requirements impact will not be handled;

- only single access and single core domains will be handled;

- the interconnection between domains through the Ri' interdomain reference point is limited to scenarios involving only wholesale and roaming between two domains;

- the e2e QoS handling is limited to scenarios involving only wholesale and roaming between two domains;

- other QoS handling aspects, e.g. QoS monitoring and QoS reporting, are covered only in an informative annex;

- the Metro topic aspects are covered in informative annex D; and

- the multicast topic is limited to scenarios involving only a single domain.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific.

- For a specific reference, subsequent revisions do not apply.

- Non-specific reference may be made only to a complete document or a part thereof and only in the following cases:

    - if it is accepted that it will be possible to use all future changes of the referenced document for the purposes of the referring document;

    - for informative references.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

For online referenced documents, information sufficient to identify and locate the source shall be provided. Preferably, the primary source of the referenced document should be cited, in order to ensure traceability. Furthermore, the reference should, as far as possible, remain valid for the expected life of the document. The reference shall include the method of access to the referenced document and the full network address, with the same punctuation and use of upper case and lower case letters.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are indispensable for the application of the present document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

[1]   ETSI TS 181 005: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Service and Capability Requirements".

[2]   ETSI ES 282 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture Release 1".

[3]   IETF RFC 3312: "Integration of Resource Management and Session Initiation Protocol (SIP)".

[4]   IETF RFC 2475: "An Architecture for Differentiated Services".

[5]   ETSI ES 282 004: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture; Network Attachment Sub-System (NASS)".

[6]   ETSI TR 180 000: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Terminology".

[7]   ETSI TS 123 107: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Quality of Service (QoS) concept and architecture (3GPP TS 23.107)".

[8]   ITU-T Recommendation Y.1541: "Network performance objectives for IP-based services".

[9]   IETF RFC 3198: "Terminology for Policy-Based Management".

[10]   IETF RFC 2753: "A Framework for Policy-based Admission Control".

[11]   DSL-Forum: "DSL Policy Control Framework (PCF)", Draft Working Text WT-134.

[12]   Damianou, N. et. al.: "The Ponder policy based Management toolkit", August 2002.

[13]   ETSI TS 181 018: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Requirements for QoS in a NGN".

[14]   ETSI TS 187 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN SECurity (SEC); Requirements".

2.2 Informative references

[15]   ETSI TS 182 027: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IPTV Architecture; IPTV functions supported by the IMS subsystem".

3   Definitions and abbreviations

3.1   Definitions

For the purposes of the present document, the terms and definitions given in TR 180 000 [6] and the following apply:

access network policies: policies which are used to make decisions for resource admission control and are designed to derive the traffic policies to be enforced by the A-RACF

> NOTE: Access network policies are constructed using Conditions and Actions that are specifically supported by A-RACFs. An example would be a policy which checks the condition that resources are available and the action to reserve the resource.

Application Function (AF): functional entity that offers applications the control of IP bearer resources when required

> NOTE: The AF is capable of communicating with the RACS to transfer dynamic QoS-related service information.

application session: end-to-end user session, which is setup by an AF (using SIP or another protocol) and requires one or more resource reservations to take place

> NOTE: An application session may involve one, two or more end users.

BGF service: traffic flow function performed by the BGF Functional Entity on media flows and/or the allocation of BGF resources

DiffServ: DiffServ networks classify packets into one of a small number of aggregated flows or "classes", based on the DiffServ code point (DSCP) in the packet's IP header

gate: operates on a unidirectional flow of packets, i.e. in either the upstream or downstream direction

> NOTE: A gate consists of a packet classifier, and a gate status (open/closed). When a gate is open, the packets in the flow are accepted. When a gate is closed, all of the packets in the flow are dropped.

"Last mile" access network segment: comprises the functional elements that enable communication between a CPN and an Access Node

local A-RACF policies: specific Access network policies that are currently active on an A-RACF (may be a subset of all access network policies)

> NOTE: Local A-RACF policies are instances of Access network policies.

local SPDF policies: specific Service based policies that are currently active on an SPDF (may be a subset of all service based policies)

> NOTE: Local SPDF policies are instances of Service based policies.

media flow: uni-directional media stream of a particular type, which is specified by two endpoint identifiers, bandwidth and class of service

NAT: generic term for Network Address Translation that includes NAT-PT and NA(P)T

overbooking admission control: situation whereby the A-RACF considers that different AF-sessions can reserve the same resources bearing in mind that these resources cannot be committed to more than one AF-session at a time

> NOTE: This enables optimal resource management in certain service conditions (e.g. Call Hold, Communication waiting).

policy: set of rules which govern the choices in behaviour of a system and that are comprised of conditions and actions, where conditions are evaluated when triggered by an event

> NOTE 1:   See annex B for further details.

> NOTE 2:   The content of policies is outside of the scope of the present document.

QoS classes: As defined in ITU-T Recommendation Y.1541 [8] and TS 123 107 [7].

QoS "Push" model: model where the RACS "pushes" traffic policies to the transport functions to enforce its policy decisions

NOTE: In this model, the CPN does not itself support native application independent QoS procedures.

QoS "Pull" model: model where, upon request from the transport processing functions, the RACS provides traffic policies to the transport processing functions

NOTE: The request from the transport processing functions may itself, for example, be triggered by path-coupled requests coming from user equipment and/or transport network elements.

resource: allocatable physical network capability

NOTE 1: A resource can be characterized by a set of parameters, including, but not limited to; memory bandwidth forwarding capacity, scheduling capacity, or other.

NOTE 2: Description and measurement metric of a resource is technology dependent.

resource identifier: single key or group of keys used to refer to a resource

NOTE: Resource identifiers can be can be the same as or derived from Layer-1 keys (e.g. physical port or reference point), Layer-2 keys (e.g. Ethernet VLAN ID), or Layer-3 keys (e.g. IP-address).

resource reservation session: set of one or more media flows, which are reserved for a period of time in order to execute an application session

NOTE: A resource reservation session may be uni-directional or bi-directional.

service based policies: policies designed to be enforced by an SPDF

NOTE: Service based policies are constructed using Conditions and Actions that are specifically supported by SPDFs. An example would be a policy in which a condition is the type of service required and the action to request the service from either the A-RACF or BGF.

traffic policies: policies for which the execution trigger is the arrival of a data packet, and for which the action(s) constitutes some form of processing of this packet before it is forwarded to another device, are known as traffic policies

xDSL: type of access network supported by the NGN, based on the different flavours of the xDSL technology, that have their resources controlled by RACS

3.2   Abbreviations

For the purposes of the present document, the following abbreviations apply:

ACP	Admission Control Process
ACSR	Authorization based on Contents of the Service Request
AF	Application Function
A-RACF	Access-Resource and Admission Control Function
ASP	Application Service Provider
BGF	Border Gateway Function
BGS	Border Gateway Services
BTF	Basic Transport Functions
C-BGF	Core Border Gateway Function
CCI	Charging Correlation Information
CLF	Connectivity session Location and repository Function
CMFE	Coordination of Messages between FEs
CPN	Customer Premises Network
C-RACF	Core-Resource and Admission Control Function
CSCF	Call Session Control Function
DHCP	Dynamic Host Configuration Protocol
DITP	Derivation and Installation of Traffic Policies
DSCP	Differentiated Service Code Point

DSFE	Discovery of Subsequent FE
e4	reference point e4
ECF	Elementary Control Function
EFF	Elementary Forwarding Function
FDP	Final Decision Point
FQDN	Fully Qualified Domain Name
GC	Gate Control
Gq'	reference point Gq'
HMRP	Handling of Media Request Priority
HSRP	Handling of Service Request Priority
Ia	reference point Ia
IBCF	Interconnection Border Control Function
I-BGF	Interconnection Border Gateway Function
IETF	Internet Engineering Task Force
IMS	IP Multimedia Sub-System
IP	Internet Protocol
IPMC	IP Packet Marking Control
LSP	Label Switched Path
MITP	Modification and Installation of new Traffic Policies
MLD	Multicast Listener Discovery
MPLS	MultiProtocol Label Switching
NA(P)T	Network Address and optional Port Translation
NAPTC	NAPT control and NAT traversal
NASS	Network Attachment Sub-System
NAT	Network Address Translation
NAT-PT	NAT Address Translation and Protocol Translation
NGN	Next Generation Network
NPAH	Network Policy Assembly Handling
OSS	Operations Support Systems
P-CSCF	Proxy-CSCF
PPP	Point to Point Protocol
QMTD	QoS and Priority Mapping - Technology Dependent
QMTI	QoS and Priority Mapping - Technology Independent
QoS	Quality of Service
RACS	Resource and Admission Control Sub-System
RCEF	Resource Control Enforcement Function
Rd'	Reference point Rd'
Re	Reference point Re
Rf	Reference point Rf
Ri'	Reference point Ri'
RLC	Rate Limiting Control
Rq	Reference point Rq
Rr	reference point Rr
RRP	Reservation of Resources Process
RTCP	Real Time Control Protocol
RTP	Real Time Protocol
SBP	Service Based Policy control
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SPDF	Service-based Policy Decision Function
SSAP	Storage of Subscriber Access Profile
SSBP	Selection of a Service based Policy
TCP	Transmission Control Protocol
TDDP	Technology Dependent Decision Point
TISPAN	Telecommunications and Internet converged Services and Protocols for Advanced Networking
TRSF	Topology and Resource Store Function
UDP	User Datagram Protocol
UE	User Equipment
UNI	User-to-Network Interface
VC	Virtual Channel
VLAN	Virtual Local Access Network
VoIP	Voice over IP

VP   Virtual Path
VPN   Virtual Private Network
x-RACF   Generic Resource and Admission Control Function

4   General description of RACS

4.1   High Level functional overview

RACS is the NGN Sub-System responsible for elements of policy control, resource reservation and admission control. RACS also includes support for core Border Gateway Services (BGS) including Network Address Translator (NAT).

RACS essentially provides policy based transport control services to applications. This enables applications to request and reserve transport resources from the transport networks within the scope of RACS.

RACS scope extends to the access and core networks, as well as to points of interconnection between them in order to support e2e QoS. In the present document, the e2e QoS handling is limited to scenarios involving only wholesale and roaming between two domains.

By offering a set of generic policy based transport control services to applications, RACS ensures that any existing or future application shall be able to request transport resources appropriate to that service as long as the application supports the interface to RACS defined in this architecture specification.

Moreover, by offering a level of hidden interaction between applications and the transport resources themselves, RACS also ensures that applications do not need to be aware of the underlying transport networks. As an example, RACS allows for real-time multimedia services (VoIP, Videoconferencing, Video on Demand, on-line gaming) to request some particular bandwidth and/or address mediation capabilities for the service from the network. As the network element responsible for policy based transport control, RACS evaluates these requests in the context of predefined policy rules, which the network operator has provisioned. RACS reserves the appropriate resources and admits the request provided the request passes the policy tests and the appropriate resources are available in the transport network. Therefore, RACS offers the means for an operator to enforce admission control and set the respective bearer service policies.

In addition, RACS also provides the means for value-added services to obtain network resources that are necessary to offer services to the end-user.

RACS is resource-reservation session aware but application session agnostic, i.e. it can support transport resource reservations for both session based and non-session based applications.

RACS also provides access to services provided by the Border Gateway Function. Examples of those services are gate control, NAT and hosted NAT transversal.

Basically, RACS offers to applications the following set of functionalities on a one per RACS resource reservation session request basis:

- Admission Control: RACS implements Admission Control to the access and aggregation segment of the network. One can imagine various types of admission control going from a strict admission control where any overbooking is to be prevented, to admission control that allows for a certain degree of over subscription or even a trivial admission control where the authorization step is considered sufficient to grant access to the service.

- Resource reservation: RACS implements a resource reservation mechanism that permits applications to request bearer resources in the access, aggregation, and core networks.

NOTE: Resource reservation mechanisms in the core network are not standardized in the present document.

- Policy Control: RACS uses service based local policies to determine how to support requests from applications for transport resources. Based on available information about resource availability and on other policy rules, e.g. priority of the application, RACS determines if a request can be supported and (if successful) RACS authorizes appropriate transport resources and derives L2/L3 traffic polices to be enforced by the bearer service network elements.

- NAT transversal: RACS controls the transversal of far end (remote) NAT.

- NAT/Gate control: RACS controls near-end NAT at the borders of the NGN core network and at the border between a core network and an access network.

RACS offers services to applications that may reside in different administrative domains.

4.2   Functional Requirements

The functional requirements of the RACS are developed in the present document in line with TS 181 005 [1].

4.2.1   R1 Requirements

In the following, the stage 2 requirements applicable to Release 1 are listed.

4.2.1.1   Overall

The overall requirements related to the scope of Release 1 have been identified as:

[1]   RACS shall only provide policy based transport control services within the access networks and at points of interconnection between core networks. There is no requirement for RACS to provide service coverage for core networks themselves or to customer networks.

[2]   The RACS shall hold a logical view of the different transport segments within its control. As one example, for xDSL access, this must include at least the last-mile and the aggregation network.

4.2.1.2   Transport Control Service Requests

The requirements related to the transport control of service requests performed by AFs have been identified as:

[3]   The RACS shall provide policy based transport control services, e.g. policy control, resource reservation, policing, gate control and IP address mediation, to Application Functions (AFs).

[4]   The RACS services shall be made available to all service control Sub-Systems as well as to the Applications domain.

[5]   The RACS services shall not be specific to any Application Function (AF) or service Sub-System.

[6]   The RACS shall be capable of supporting multiple Application Functions (AFs).

[7]   The RACS shall offer services to Application Functions (AFs) that may reside in different administrative domains.

[8]   The RACS shall be able to authenticate and authorize the Application Function (AF).

[9]   RACS shall set the bearer/transport function with network-level attributes that match to the transport control service requests, e.g. bandwidth, QoS, etc.

[10]   The RACS services shall either be chosen by an Application Function (AF) at a given time for use in the context of the application service provided by the application or be triggered by a transfer processing function.

[11]   The RACS shall be prepared to support at least eight different priority types defined in such a way that any number of them may be simultaneously active. This number of priorities is envisaged to support different priorities for national usage, e.g. emergency service.

4.2.1.3   Resource Handling

The requirements related to the resource handling, i.e. resource reservation, resource management, etc., have been identified as:

[12]   The RACS shall provide a mechanism to the Application Function (AF) entity through which it can reserve resources in the access network, i.e. RACS reserves resources on behalf of AFs.

[13] The RACS shall be able to react on prioritization request signalled by an Application Function (AF) for transport control by modifying allocated resources.

[14] RACS shall support all the following resource reservation scenarios:

- a resource reservation where admission control is only required for the "last-mile" access network segment, but is not required for the aggregation network segment;

NOTE: For the definitions of access network segment, aggregation network segment, and core network segment, please see ES 282 001 [2].

- a resource reservation where admission control is only required for the aggregation network segment, but is not required for the "last mile" access network segment;

- a resource reservation where admission control is required for both "last mile" access network and aggregation network segments.

[15] The RACS shall support a versatile set of resource management schemes, suitable for coping with all target deployment architectures:

- a Single-stage resource management model providing resource management services in a mode where reserved resources are immediately available upon successful reservation;

- a Two-stage reserve-commit resource management model that can be leveraged in support of services that aim to support charging per service-invocation and require as such service-theft-prevention solutions;

- an Authorize-reserve-commit resource management model supporting service-based local policy control under coordination of a network-hosted application function.

[16] The RACS shall notify the Application Function (AF) in the case that a previously allocated resource must be relinquished. This may be triggered by an administrative decision or by a faulty condition.

[17] The RACS shall support requests from Application Functions (AFs) to modify the parameters of their existing transport resource reservations. Requests of this type may result in a new admission control step and/or installing of new L2/L3 traffic policies.

[18] The RACS shall provide feedback messages to the Application Function (AF) either approving or rejecting the transport control service reservation, commit or modify requests.

[19] The RACS shall support both soft-state and hard-state resource management approaches. Soft-state operation will assure robustness of resource management services in an environment with multiple applications. In both cases:

- granularity of resource reservation, removal, and modification facilities shall be at the level of individual service flows;

- the RACS shall support facilities for the explicit removal of previously established resource reservations;

- the RACS shall support facilities for the explicit modification of previously established resource reservations.

[20] The RACS shall provide the necessary functions to support Sub-Systems in the Service Layer that implement a segmented resource management model RFC 3312 [3] An example of such a Sub-System is the IMS, where resource reservation for each participating party in an application session (e.g. multi-party conversational SIP-based sessions) is needed.

4.2.1.4   QoS Management

The requirements related to QoS Management have been identified as:

[21]   The RACS shall support a "Push" model for initiating policy based transport control service requests. In this model service requests are "pushed" to RACS from the Application Function (AF). RACS services these requests, and if the service requests from the AFs are in line with policies established by the operators and stored in the Sub-System, and if appropriate transport resources are available, then RACS "pushes" requests down to the transport processing functions to obtain the appropriate transport resources.

[22]   RACS architecture shall ensure QoS aware NGN service delivery by adopting at least one of the following two models for dynamic QoS control:

-    **guaranteed QoS:** traffic delivery service with absolute numerical bounds on some or all of the QoS parameters, such as throughput, latency, jitter and loss.

NOTE 1:   The bounds may be derived due to physical limits, or due to the enforcement of limits such as those encountered through mechanisms like rate policing. The bounds may result from designating a class of network performance objectives for packet transfer.

-    **relative QoS:** traffic delivery service without absolute numerical bounds on the achieved bandwidth, packet delay or packet loss rates.

NOTE 2:   The circumstances where certain classes of traffic are handled differently from other classes of traffic, and the classes achieve different levels of QoS, are described.

4.2.1.5   Traffic Handling

The requirements related to the traffic handling have been identified as:

[23]   The RACS shall not be aware of application session, it shall be aware of a set the media flows in a resource reservation request, which may in turn belong to one or multiple application sessions.

[24]   The RACS shall support transport control service requests from Application Functions (AF) for uni- and bi-directional, symmetric and asymmetric, unicast and multicast, up- and downstream traffic. However, multicast is not further developed in RACS Release 1.

[25]   The RACS shall support allocation of resources in the transport network that have different traffic characteristics, for example packet loss.

4.2.1.6   Charging and Overload Control

The requirements related to charging and overload control have been identified as:

[26]   The RACS shall be able to export charging information and resource reservation session metrics. For Release 1 charging should be limited to off-line charging.

[27]   The RACS shall support appropriate overload control mechanisms in order to prevent overload within the RACS itself and also within the requesting AFs. This applies to all RACS to AF reference points. However, the overload control mechanism is not further developed in this architecture document.

4.2.2   R2 Requirements

In the following, the stage 2 requirements applicable to Release 2 are listed, either as enhancements or as entirely new requirements.

4.2.2.1   Overall

For the present document, no overall requirements have been specifically identified except those mentioned in clause 1, together with the restrictions mentioned there in the bullet item list.

4.2.2.2 Resource Handling

The requirements related to improvements on resource handling have been identified as:

[28] The RACS shall provide a mechanism enabling the Application Function (AF) entity to schedule resource reservations, i.e. to reserve resources at a requested time and not immediately after the AF request.

[29] Resource admission control should support service changes (i.e. upgrading or downgrading) triggered at the application function level, based upon current network loads and link quality status, as detected by the underlying transport processing functions.

4.2.2.3 QoS Management

The enhanced or new requirements related to QoS Management have been identified as:

[30] The RACS shall support communication between instances of RACS located in different administrative domains within NGN networks, which enables those RACS instances to interact with each other for the resource reservation over multiple administrative domains.

[31] The RACS shall be capable of receiving network triggers originated by multiple Transfer Processing Functions, e.g. to commit previously authorized and reserved resources.

[32] The RACS shall support the QoS resource reservation mechanisms described below for initiating policy based transport control requests. In these models, traffic policies are "pushed" from the RACS to the transport functions on receipt of a request from an Application Function (AF) or are "pulled" from the RACS by the underlying network transport elements, on receipt of a QoS request from a UE or from another network transport element i.e.:

- in the "Push" mode, the RACS pushes traffic policies to the transport functions on receipt of a path-decoupled request for resource authorization and/or reservation from an Application Function (AF) or from an interconnected RACS entity;

- in the "Pull" mode, traffic policies are "pulled" by transport functions from the RACS on receipt of path-coupled resource requests. This requires that the user equipment and/or a network element are capable of sending QoS-related requests using a path-coupled signalling mechanism. The subsequent treatment associated to the authorization, admission control, reservation control, and policy enforcement, follows the same principles as those defined for the "Push" mode, except that use may be made of a specific binding mechanism;

  In both cases, RACS only services these requests if they are in line with policies established by the operators and stored in the Sub-System, and if appropriate transport resources are available.

4.2.2.4 e2e QoS Handling

In the present document, the e2e QoS handling is limited to scenarios involving only wholesale and roaming between two domains.

4.2.2.5 Multicast/Unicast Handling

In the present document, the multicast/unicast handling is limited to scenarios involving only a single domain.

The requirements related to improvements on multicast/unicast handling have been identified as:

[33] The multicast resource admission control mechanism should make it possible for a service provider to provide authorization and policies for multicast service (e.g. Access Profile).

[34] The multicast resource admission control mechanism should make it possible for a service provider to provide multicast service along with other NGN services.

[35] The multicast resource control mechanism should support rapid modification of reservations, to support capabilities such as fast channel zapping.

[36] The multicast resource admission control mechanism should enable harmonization between unicast and multicast resource admission control.

[37] The multicast resource admission control mechanism should make it possible for a service provider to provide charging information for multicast service.

4.2.2.6   Topology and Resource Information Retrieval

The enhanced or new requirements related to topology and resource information retrieval have been identified as:

[38] The RACS shall be able to retrieve topology and resource information needed to manage resource reservations in the different transport segments within its control, either:

- from local configurations;

- from multiple external systems;

- from several network entities; or

- from any combination of local configurations, external systems and network entities.

In the case where RACS retrieves information form multiple external systems, and/or several network entities:

- it shall provide a single point of contact for topology and resource information;

- it shall be possible to retrieve topology and resource information through both information "push" and information "pull" from external systems and network entities;

- it shall be possible to transfer topology and resource information from external systems and network entities both as complete information sets and as deltas to previously transferred information by a particular information source.

In the present document, these topology and resource information topics are only covered in annex E.

4.2.2.7   Network Deployment Scenarios

The enhanced or new requirements related to network deployment scenarios have been identified as:

[39] The RACS shall support multiple network deployment scenarios in order to allow for different business models. The details about what network deployment scenarios are supported are defined in annex D below.

4.2.2.8   Charging and Overload Control

In the present document, there are no further requirements related with charging and overload control beyond those defined in Release 1. New reference points supporting charging within RACS have been provided.

5   RACS functional architecture derivation basis

In this clause, the technical issues related to some of the functional requirements identified above, e.g. unicast and multicast, charging, and QoS management, which may have impact in the RACS architecture definition, are described.

5.1   Resource Control for Unicast and Multicast

In present document, the multicast/unicast handling is limited to scenarios involving only a single domain.

When offering IMS and/or non-IMS based services using unicast, the demand for these services can occasionally exceed the capacity offered by the access and aggregation network although this network may be carefully dimensioned. Unexpected usage patterns and/or popularity of specific services introduce an uncertainty complicating any dimensioning task aiming at cost effective network usage. These basic issues related to providing predictable quality for unpredictable services constitutes the motivation for the resource admission control functions provided by RACS. Beyond resource admission control for various unicast services, IPTV services further demands such control also for multicast.

In order to provide an attractive IPTV service, providers offer bundles of TV channels to subscribers with a very large number of channels. By doing so, some of the TV channels remain frequently unwatched. When IPTV traffic is carried over shared network resources along with VoD traffic and Internet traffic, the number of TV channels offered to subscribers may be greater than the number of channels that can be simultaneously carried over the access and aggregation network. In addition, some channels will be watched by more than one user on a given Access Node. Therefore, multicast is likely to be used. It should be noted though that the usage of multicast is also likely to be combined with usage of unicast for IPTV service such as trick mode or other personalized service offerings.

In this configuration, the risk of congestion is high and this will result in the degradation of the QoS being provided, as well as in the difficulty to attend to new service requests. It is therefore of utmost importance to monitor, and prevent this situation if possible. Hence, new mechanisms should be implemented in RACS to achieve this goal.

## 5.1.1	Resource control scenarios

### 5.1.1.1	Identification of Resources

One aspect of unicast and multicast resource control is the identification of the contended bandwidth resource and the decision whether resource admission control needs to be applied to the identified resource. With reference to figure 1, which is based on ES 282 001 [2], figure 2, three segments for unicast and multicast traffic control can be identified:

1)	*Access segment*: User access line bandwidth resource. Examples for unicast resource admission control on the access segment include cases where different and independent IMS and/or non-IMS based services compete for the bandwidth of this segment and may together demand more bandwidth than what is available before or after bandwidth is set aside for active multicast services. Examples for multicast resource admission control on the access segment include cases where the service provider's service-package offering is not tightly tied to the bandwidth of the access segment, thus allowing multiple concurrent multicast and/or unicast streams which overwhelm the available resources of this segment.

2)	*Aggregation segment*: Access-node to aggregation node(s) link or Layer-2 topology bandwidth. Examples common for both unicast and multicast resource admission control on the aggregation segment include cases where a peak unicast and/or multicast bandwidth needs to be enforced or where the access network provider sells "unicast and/or multicast bandwidth packages" to service providers as part of a transport wholesale offering.

3)	*Core segment*: Core transport and Layer-3 aggregation bandwidth resources. Examples common for both unicast and multicast resource admission control in the core network segment include cases where the provisioned transport bandwidth is insufficient or a peak unicast and/or multicast bandwidth needs to be enforced.
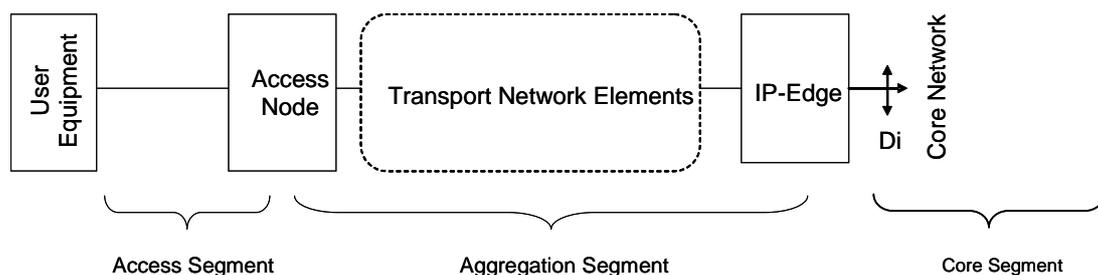
**Figure 1: Network Segments
(based on ES 282 001, figure 2b)**

### 5.1.1.2	Multicast Resource Admission Decision Specifics

Multicast resource control is not limited to managing bandwidth resources only, as it also manages the amount of state kept on transport network elements to conduct multicast traffic forwarding. Multicast state management is implementation dependent, and could be required in all of the above mentioned segments.

A generic policy for multicast resource control therefore handles bandwidth resources and state resources jointly.

5.1.1.3 Resource Admission Decision Prerequisites

Unicast and Multicast resource admission control has a number of prerequisites which are as follows:

1) Availability of a resource admission control function for the resources in question.

2) The ability of the resource admission control function to receive a trigger resource request event and attribute it to the location/path which is associated with the request, i.e. the congestion point(s).

3) The capability of the resource admission control function to determine what amount of resources the resource request event represents (e.g. description of multicast groups and their corresponding bandwidth requirements). It is assumed that the information contained in the resource request is sufficient to determine the required QoS and state to be kept on a network transport function.

4) The ability of the resource admission control function to determine what resources are available/can be granted on the location/path attributed to the request. This implies knowledge of the topology (including congestion point(s) and the current reservations) of a segment (if more than a single network element or link is handled by a unicast and/or multicast resource admission control function).

5) The optional capability of commencing data plane forwarding only after the resources admission control function has granted the requested resources, and affecting data plane forwarding if conditions change. The decision about the impact of resource admission control outcomes on the transport forwarding functions is part of the service provider / network operator policy. A service provider might decide to offer services on a best effort basis (without any resource guarantees) if the resource admission control function provides a negative result to a request.

6) The ability of the resource admission control function to inform the requesting entity about a negative outcome of a request.

5.1.1.4 Resource Admission Control Approaches

According to the base requirements outlined in clause 5.1.2.2 a multicast resource admission control function is closely linked to the managed resources in question. Typically access network segments together with aggregation network segments (ES 282 001 [2]) comprise multiple resources handled by transport Functional Entities, as well as the links connecting them. Two resource admission control approaches are identified for these segments:

- *Independent Resource Admission Control*: The resource admission control decision is handled by an independent resource admission control Functional Entity (FE), which controls resources within one or more segments.

- *Coordinated Resource Admission Control*: The resource admission control decision is handled by multiple resource admission control FEs that coordinate the admission control for resources to avoid uncontrolled overbooking. Communication between these FEs follows a hierarchical structure involving a top-tier resource admission control function and one or more lower-tier resource admission control functions.

Clause 6.2.2.1.3 provides further details and descriptions on the independent and coordinated resource admission control approaches.

NOTE: IP-Multicast has some embedded "in-band" signalling capabilities, allowing for simple distributed resource admission control mechanisms. Examples include administratively configured state limits for IP-Multicast state. It should be noted that the "in-band" mechanisms available in IP-Multicast are not sufficient to deploy per-user multicast policies (which would include the ability to identify the user and his bandwidth requirements). These "in-band" mechanisms will not be standardized as part of the present document.

5.1.1.5 Multicast Resource Admission Control in the Access Network Domain Transport Nodes

Support for Multicast in the Access Network domain requires that the Transport Network Nodes have multicast capabilities in order for these nodes to offer multicast based services such as IPTV. Moreover, these Transport Network nodes may require interfacing with the RACS for Admission Control and Resource Reservation Requests.

Table 1 describes the roles of the transport processing functions related to multicast based services.

Table 1: Multicast related Transport Functions

BTF	EFF	ECF	RCEF	x-RACF
EFF and ECF in the same transport node element	Packet Replication	Processing/Execution of Multicast Protocols	Enforcement of Multicast Traffic Policies	Policy evaluation of multicast policies
		Forwarding of events for policy evaluation	Forwarding of events for policy evaluation	

5.2   Charging

The RACS requirements for charging are restricted in Release 1 to providing support for offline charging by the RACS functions that can be located in different administrative domains: the SPDF, A-RACF and AF.

For push mode, the RACS functional entities, SPDF and A-RACF shall be capable of providing the following information for charging purposes:

- Charging Correlation Information (CCI).

- Request Type.

- Requestor Info.

- Subscriber Info.

- Service Priority.

- Media Description.

- Commit ID.

- Time Stamp.

- Reason.

The means to transfer this information is not standardized in the present document.

A Charging Correlation Information (CCI) is a globally unique identifier that may be generated by the SPDF if it was not provided by the AF. This identifier may also be forwarded to the A-RACF.

The Request Type may have the following values: Resource Reservation, Resource Modification and Resource Release.

The Subscriber Info represents the Subscriber-Id and the Globally Unique IP Address present in the request.

The Reason shall represent conditions such as successful, unsuccessful and abnormal conditions.

The charging capabilities in RACS for present document does not impose any additional charging requirements than those defined for previous releases.

The charging information for pull requests are not standardized in the present document.

5.3   QoS Management Functions in Fixed Access Networks

In order to define the RACS architecture it is necessary to identify the possible QoS management functions in fixed access networks. Those functions can be categorized according to their QoS control capabilities and business models. An abstraction is made here of the possible business models in the fixed environment.

To ensure QoS aware NGN service delivery, the following two architectures for dynamic QoS control are considered for RACS:

- **guaranteed QoS:** traffic delivery service with absolute numerical bounds on some or all of the QoS parameters, such as throughput, latency, jitter and loss.

NOTE 1: The bounds may be derived due to physical limits, or due to the enforcement of limits such as those encountered through mechanisms like rate policing. The bounds may result from designating a class of network performance objectives for packet transfer.

- **relative QoS:** traffic delivery service without absolute numerical bounds on the achieved bandwidth, packet delay or packet loss rates.

NOTE 2: The circumstances where certain classes of traffic are handled differently from other classes of traffic, and the classes achieve different levels of QoS, are described.

Support of QoS unaware ("Best Effort") networks as well as support of networks that have statically provisioned QoS differentiation does not require any RACS functionality.
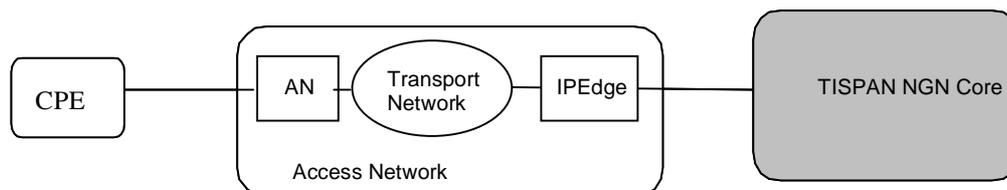
Figure 2: Access Network Model

The RACS architecture shall support both QoS control architecture models - guaranteed and relative - allowing the access provider to select the most suitable QoS architecture for their needs.

When relative QoS is used, the QoS differentiation shall be performed at the IP_Edge, e.g. compliant with the DiffServ Edge functionality defined in IETF specifications for Differentiated Services (RFC 2475 [4]). Moreover, RACS should take into account the ability of some CPN to provide QoS differentiation, e.g. by applying DiffServ marking, and take steps to allow this to have effect only where it is required by operator defined RACS local policies.

For guaranteed QoS control, enforcement of QoS admission control decisions (throughput control and traffic policing) shall be performed in the IP_Edge and may also be performed in the CPN and/or Access Node.

The RACS shall support the "proxy QoS reservation request with policy-push" as a QoS Push resource reservation mechanism, e.g. among others, the one shown in figure 3. In this case, the CPN does not itself support native application independent QoS signalling procedures. When a CPN invokes a specific service of an AF using the NGN signalling (e.g. SIP), the AF will issue a request to the RACS for QoS authorization (policy control) and resource reservation. The AF may extract implicit user requested QoS class from Service Request, e.g. by SIP SDP, based on operator's policy, and send the appropriate QoS class information to RACS.

RACS policy decisions are "pushed" to the policy enforcement point (IP_Edge) in the NGN access (e.g. xDSL).
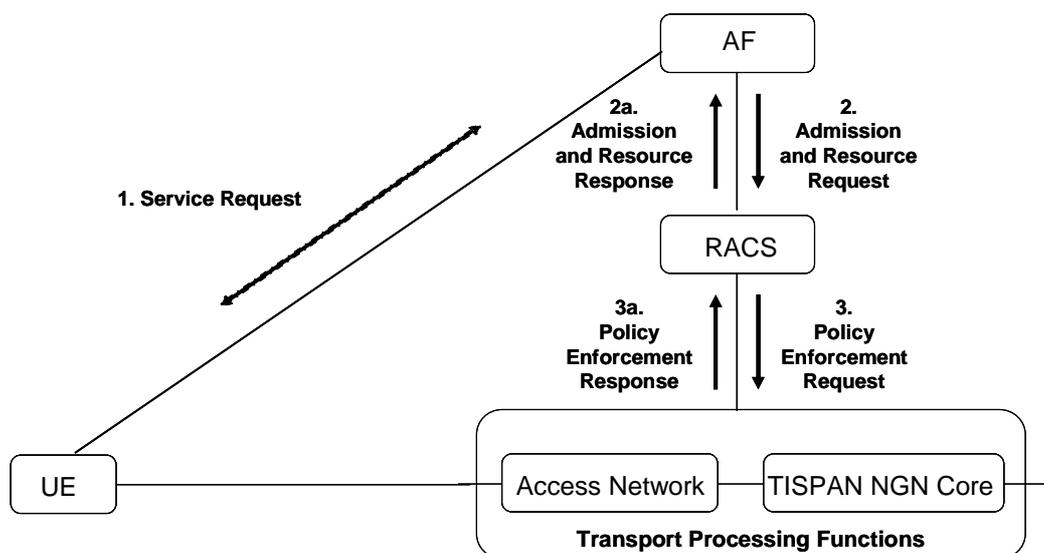
Figure 3: Example of proxy QoS with policy-push

In the example indicated in figure 3, and depending on its capabilities, the UE may add an indication of the QoS class in the service request.

NOTE 3: Besides the example depicted in figure 3, other "push" QoS resource reservation mechanism are possible.

The RACS also supports the QoS Pull resource reservation mechanism, e.g. the one depicted in figure 4. This "user requested QoS with policy-pull" mechanism requires that the UE is able to handle Layer 3 QoS signalling capability, and perform a QoS request for its own needs through the use of path-coupled signalling, e.g. RSVP. Similarly the UE may request a service which in turn may cause a QoS Request to be originated from a Transport Function resulting in a Policy Pull request.

The QoS request may be preceded by a previous authorization request, where an authorization token may be returned by RACS in order to perform a binding between the requested QoS for the media flow and the policy decision information to be enforced. This means that steps 1, 2, and 2a, indicated in figure 4 are optional as other binding mechanisms may be used.
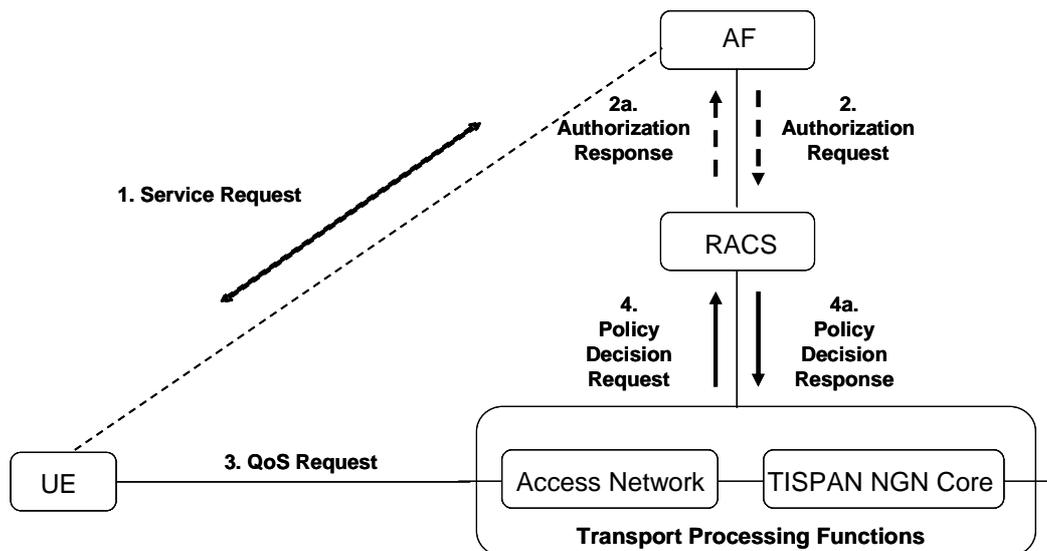
Figure 4: Example of User requested QoS with policy-pull

Please refer to annex F for more detailed information on these mechanisms.

5.4   Resource Control for Service Quality Downgrading

QoS downgrading involves the act of adjusting the QoS provided to an existing session (e.g. bandwidth and the time duration for using this bandwidth). An AF can request a QoS downgrade for a certain service without forcing it to terminate.

QoS downgrading may be required when a new incoming session should be admitted, and there is insufficient subscribed network resource for the new session. Moreover, according to the user service profile, the AF may decide to allow QoS downgrading for one or more existing sessions. As a result, the QoS level may be degraded in order to free resource for the new incoming session.

The RACS shall provide mechanisms to:

- allow the AF to express the desire to be informed in case the amount of resources controlled by RACS are insufficient to complete a request, but that it might be able to complete the request by downgrading QoS for a set of existing sessions allocated to this particular AF;

- inform the AF that a situation occurred where the amount of resources controlled by RACS are insufficient to complete a request, but that it might be able to complete the request by downgrading QoS for a set of existing sessions allocated to this particular AF.

In this case, the new incoming session and other existing sessions shall belong to the same subscriber.

NOTE: The mechanism is applicable for the access segment although other possible use cases are possible. These are not standardized in the present document.

6   RACS functional architecture definition

6.1   General

The overall functional architecture of the RACS is shown in figure 5.
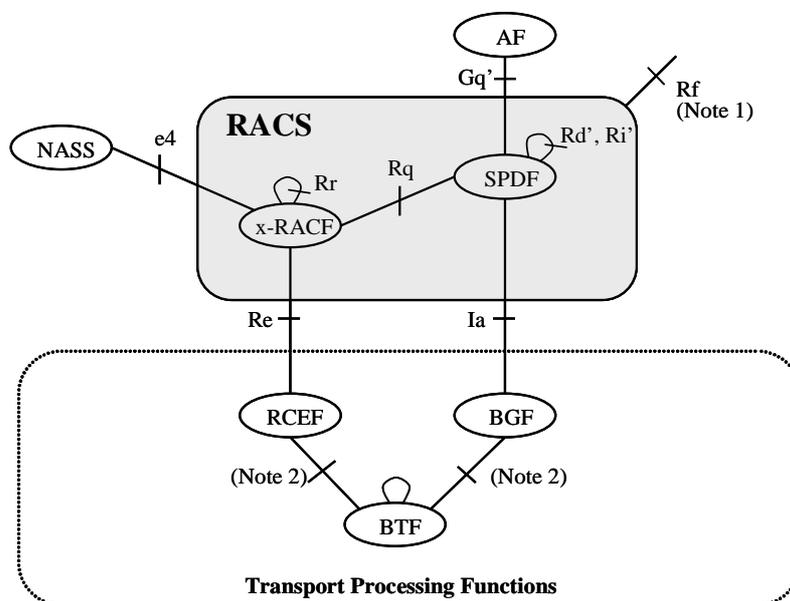
Figure 5: RACS Functional Architecture

NOTE 1:   The RACS has a Rf reference point in order to send the Charging Information directly to the Charging Functions for some cases, e.g. the pull mode. The Rf is only used for offline charging and is terminated on both x-RACF and SPDF.

NOTE 2:   The relationship between BTF and RCEF as well as BTF and BGF is considered to be an internal relationship within the same physical node and will not be standardized as part of the present document.

NOTE 3:   Besides the A-RACF and SPDF the present document addresses the aspects of the RCEF, BGF and AF that are associated to RACS. The overall functionality related to AF, RCEF and BGF is defined in ES 282 001 [2].

The NGN Service Layer encompasses an Application Function (AF), which offers services that require control of IP bearer resources. Examples of an AF are the P-CSCF and IBCF in the case of IMS. The AF maps the application layer QoS information, e.g. the P-CSCF maps parameters defined in SDP, into QoS request information to be sent via the Gq' reference point to the SPDF.

RACS shall support both Push and Pull QoS resource reservation mechanisms:

*   Push mode: RACS authorizes a reserve or a reserve-commit request from AF based on policy rules, performs admission control to requested resources and/or to the subscriber profile and, in case these operations are successful, RACS may instruct RCEF to enforce the policy and resource admission decision. In the case where the AF only issues a reserve request initially, this last step is triggered by a separate commit request from AF.

*   Pull mode: Upon reception of a reserve or reserve-commit request from RCEF, RACS performs admission control to requested resources and/or to the subscriber profile. In case the RCEF issues a reserve-commit request, RACS responds with the final policy and resource admission decision to instruct the enforcement. In case the RCEF instead issues a reserve request, the instructions for enforcement will be provided by RACS in the response to the consecutive commit request issued by RCEF.

The SPDF provides the AF with a single point of contact. Two functional specializations of x-RACF (generic Resource Admission Control Function) have been defined: the A-RACF, which is always in the access network, and the C-RACF, which is always in the core network. They both support the resource reservation methods as defined in clause 5.3. The x-RACF may receive requests from the SPDF, and in the case of A-RACF, from the RCEF or another A-RACF located in the same Operator Domain. Based on these requests and policy information stored in the x-RACF, the x-RACF may accept or reject these requests for the transport resources within its control.

Please refer to clauses 6.2.2.1.1 and 6.2.2.1.3 for further details on x-RACF specializations and their multiple instantiations, e.g. scope of the network topology view in terms of resources, and NGN layers where they may be found.

Each administrative domain shall have at least one SPDF.

There is only a single type of reference point between RACS instances in different administrative domains. This reference point is between SPDFs.

For resource and admission control the architecture provides a clear separation between layers that allows an application service to run over different access networks without impacting the application capabilities as long as the resources are available. Although x-RACF can be seen as a generic function, it may maintain different instances of resource models, depending on the different types of access.

The RACS (A-RACF) interacts with the Network Attachment Sub-System (NASS) via the e4 reference point.

The x-RACF has a Rf reference point in order to be allowed to send the Charging Information directly to the Charging Functions for some cases, e.g. the pull mode.

The SPDF also has a Rf reference point in order to be allowed to send the Charging Information directly to the Charging Functions for some other cases, e.g. the interconnection between RACS and the negotiation of the variation of the capacity of the quality during an active session.

The RCEF is a Functional Entity that is usually grouped into physical entities called IP_Edge Node/or Access Node, which and is accessed via the Re reference point. It is a logical element that belongs to the transport processing functions and enforces the traffic policies by means of which RACS can assure the use of the resources.

As far as the BGF Functional Entity is concerned, please refer to ES 282 001 [2] for definitions on where it is located.

Table 2 summarizes the services performed by the RCEF, C-BGF and I-BGF, under the control of the RACS.

Table 2: RACS Elementary Functions associated with RCEF, C-BGF and I-BGF

RCEF	C-BGF	I-BGF
Open/close gates	Open/close gates	Open/close gates
Packet marking	Packet marking	Packet marking
Resource allocation	Resource allocation (per flow)	Resource allocation (per flow)
	NAT	NAT
	Hosted NAT traversal	
Policing of down/uplink traffic	Policing of down/uplink traffic	Policing of down/uplink traffic
	Usage metering	Usage metering

Different BGF instances may implement different subsets of the services identified in Table 2 based on the operator's policy.

Unless stated explicitly, the remaining text of the present document refers to the term BGF for both C-BGF and I-BGF, regardless of its location in the network.

6.2   Functional elements

6.2.1   SPDF

6.2.1.1   SPDF main functions

The Service Policy Decision Function (SPDF) is a Functional Entity that acts as a final Policy Decision Point for Service-Based Policy control (SBP) for each administrative domain it resides in. It may also communicate with an interconnected SPDF located in an adjacent administrative domain for a reservation request.

The SPDF makes policy decisions by using service policy rules defined by the network operator. The most appropriate service based policy to be applied to a request from an AF or an interconnected SPDF is based on the combined meaning of the Requestor Name, Service Class, Service Priority, Reservation Class, or any other combination of these information elements contained in a transport control service request message received from the AF or the interconnected SPDF.

The SPDF hides the underlying network topology from applications and from interconnected SPDFs. This allows the SPDF to offer a common view to the AF (e.g. P-CSCF) and/or the interconnected SPDF regardless of the underlying network topology and particular access technology in use.

After having received transport control service requests from the AF or the interconnected SPDF, as well as after having chosen the service policy, authorization is then performed based on a process that involves the checking of the transport control service request against the service based policy.

If the outcome of the authorization is successful and one or more functional entities among A-RACF, BGF and interconnected SPDFs need to be interrogated to serve a request from an AF or an interconnected SPDF, the SPDF maps the QoS requirements and priority received in those transport control service requests into the parameters to be sent in requests to the A-RACF, to the BGF, to the interconnected SPDF, or any combination of those. This resource mediation process is performed according to the rules defined in the above mentioned selected service based policy.

The SPDF performs a coordination function between the AF, the A-RACF, the BGF, the interconnected SPDFs, or any combination of those as further described in clause 6.2.1.7.

Based on a discovery mechanism, the SPDF determines the appropriate entity or entities among A-RACF, BGF and interconnected SPDFs to interrogate in accordance with the required transport capabilities, and with the indication included in the transport control service request received from the AF or from an interconnected SPDF, along with Local Policies.

At the end of the process, the final decision is reported back to the entity that issued the request, i.e. an AF or an interconnected SPDF.

6.2.1.2   Summary of SPDF Elementary Functions

This clause contains a table where the above identified elementary functions for the SPDF have been shortly summarized.

In this table, descriptions related to technology dependent functions refer to functions that require specific knowledge of the link layer technology.

On the other hand, technology independent functions refer to functions that do not require that specific knowledge of the link layer technology because they are related to the IP level.

Table 3: RACS Elementary Functions associated with SPDF

Acronym	Function	Description
FDP	Final Decision Point	Makes the final admission decisions, including priority considerations, in terms of network resources and admission control, based on request from the AF or an interconnected SPDF.
SSBP	Selection of a service based policy	Choice of the most appropriate service based policy to be applied to the transport control service request based on information included in the transport control service request.
ACSR	Authorization based on contents of the service request	Checking between the selected service based policy and the contents of the transport control service request, in order to perform initial authorization if match occurs.
DSFE	Discovery of subsequent FE	Determination of the appropriate A-RACF, BGF and/or SPDF in accordance with the required transport capabilities, with the indication included in the transport control service request, and with local policies.
CMFE	Coordination of messages between FEs	Coordination function for messages exchanged between an AF, a BGF, an A-RACF and/or interconnected SPDF Fes.
NAPTC	NAPT control and NAT traversal	Controls network address translation for both near-end NA(P)T and far-end NA(P)T.
QMTI	QoS and Priority Mapping - Technology Independent	Maps the service QoS requirements and priority received from the AF or from the interconnected SPDF to network QoS parameters (e.g. Y.1541 class) and priority, see note 1.
GC	Gate Control	Controls the opening and closing of a gate, see note 1.
IPMC	IP Packet Marking Control	Decides on the packet marking and remarking of IP flows, see note 1.
RLC	Rate Limiting Control	Decides on the bandwidth limit of flows (e.g. for policing), see notes 1 and 2.
HSRP	Handling of service request priority	Ability to indicate a service priority level in the resource reservation request, see note 1.
NOTE 1: This Elementary Function is common to the SPDF and to the A-RACF.		
NOTE 2: In the case of A-RACF, this functionality may take the form of a parameter that belongs to a L3/L2 traffic policy (DITP).		

6.2.1.3 Reference points

The reference point between the AF and SPDF is Gq'. The Gq' enables the NGN Sub-Systems to interact with the Resource and Admission Control Sub-System (RACS) for authorization, resource reservation and Border Gateway Services (BGS).

The reference points between two SPDFs are Ri' and Rd'. They both convey information that is used to reach the desired network elements in the transfer layer.

The Ri' reference point is an inter-domain reference point, i.e. it is used when the AF can not communicate directly with the SPDF of a certain domain. In this case, a reachable SPDF forwards the information through the Ri' reference point towards another SPDF of a different domain to perform the resource request to the desired network element.

The Rd' reference point is an intra-domain reference point, i.e. it is used when the SPDF of a certain domain can not communicate directly with a specific underlying network element that is located in the same domain. In this case, the SPDF forwards the information through the Rd' reference point towards another SPDF of the same domain to perform the resource request to the desired network element.

The reference point between the SPDF and the A-RACF is Rq. The SPDF interacts with the A-RACF to ask for an admission control decision for the QoS resources required for the Application session via the Rq reference point. The authorization decision provided by the SPDF to the AF is dependent on the admission control decision taken by the A-RACF.

The reference point between the SPDF and the BGF is Ia. The SPDF interacts with the BGF to ask services as listed in Table 2. This reference point is used for communication between the SPDF and C-BGF and between the SPDF and I-BGF.

The SPDF shall be able to establish relationships with multiple A-RACFs. These A-RACFs can be all in the same or in different access networks. The SPDF shall have the ability to identify the correct A-RACF when a request is received from the AF.

The Gq' reference point constitutes an interdomain reference point as it allows that the AF and the SPDF are in different administrative domains.

In Release 1 inter-domain aspects are not explicitly addressed. The SPDF and the A-RACF may be located in different administrative domains, the Rq reference point may be an interdomain reference point.

For the present document, as each administrative domain shall have at least one SPDF, and the reference point between SPDFs is the only type of reference point between RACS instances in different administrative domains, the Rq reference point is always a intradomain reference point.

Use of the Rq reference point as an inter-domain reference point as described in R1 should be avoided.

NOTE: Backwards compatibility between implementations of both releases is always ensured as long as possible encryption of the Rq reference point performed by the Release 1 FEs for security reasons has an appropriate treatment by the present document FEs.

The SPDF also directly interfaces with the Charging Functions via the Rf reference point.

6.2.1.4   User profile

The SPDF does not require access to user profile information.

6.2.1.5   Priority

The AF or the interconnected SPDF can indicate a service priority level to the SPDF. In accordance, the SPDF has the ability to define a service priority level for the resource reservation request sent to the A-RACF. As an example, in the case of an emergency session, the AF or the interconnected SPDF may indicate to the SPDF that the resource is required for a Application priority session and, as a result, the SPDF indicates to the A-RACF a service priority for the requested resource.

6.2.1.6   Service request

Requests from the AF to the RACS over the Gq' reference point, or from an SPDF located in a different administrative domain to the RACS over the Ri' reference point, include information on the service required from RACS, an unique identifier for the requesting application, an unique identifier for the resource reservation session and an indication of the requested priority amongst others (see clause 6.3.1.3.1 for a complete list of information elements). It shall be possible for the AF or for an interconnected SPDF instance to request a different RACS service for each of the flows belonging to a single resource reservation session request.

The key information elements used by an AF or by an interconnected SPDF to specify the service requested from RACS are the Requestor Name and the Service Class (see definitions in clause 6.3.4.3). However, other parameters such as bandwidth also provide additional information about the service requested.

Service information is of local significance to the operators controlling the service and transfer layers respectively, and the definition of the actual values used is outside the scope of standardization.

By combining all the information received from the AF via Gq', or from an interconnected SPDF instance via Ri', with local operator policies, the SPDF can derive the following information:

- whether service is to be requested from the BGF, A-RACF, both or neither of them;

- whether service is to be requested from an SPDF located in a different administrative domain;

- transfer layer resources that shall be used for a particular resource reservation that may include transport network partition, interconnection type (where signalling-only interconnection types may not require the insertion of an I-BGF in the media path), and interconnect resources to be used (choosing the right I-BGF in the transport domain);

- traffic characteristics to be requested for individual media flows, including QoS parameters, which may be used by the SPDF to in turn request the appropriate filters or packet marking policies to be applied in the BGF and/or to describe to the A-RACF the resource being requested.

6.2.1.7   Coordination function

The SPDF maps requests received from an AF into a request sent to an A-RACF, a BGF, an interconnected SPDF located in a different administrative domain, or any combination of these Functional Entities.

Moreover, the SPDF also performs the coordination function for messages exchanged between an AF, BGF, A-RACF, an interconnected SPDF, or any combination of those.

A bundle identification, hereafter referred to as Resource Bundle-Id information, is received in every reply granting resources from the A-RACF. The SPDF shall be able to associate this Resource Bundle-Id to the resources reservation session during the existence of this resource reservation session.

In case failure conditions are affecting the A-RACF, the BGF, an interconnected SPDF, or any combination of those, the SPDF is capable of performing the necessary coordination for release of the impacted resources (e.g. an event reporting failure in the BGF is reported to the AF and any outstanding A-RACF resources shall also be released). The reference points between the A-RACF, BGF and SPDF, as well as an interconnected SPDF, shall be able to transport information indicating partial or complete failure of a BGF and/or an A-RACF.

The SPDF shall be able to handle reports of abnormal condition from the A-RACF specifying either an individual resource reservation session or a Resource Bundle-Id. In the latter case, all current resource reservation sessions associated to this bundle shall be released.

In addition, the SPDF can autonomously initiate a partial or total release of resources (e.g. administrative action in the SPDF).

The sequence used by SPDF to access the A-RACF, BGF and other SPDFs is a local decision in the SPDF, e.g. the SPDF is able to decide whether to access the A-RACF and then the BGF, or vice versa, or both in parallel. This is valid for request, modification and release. The implementation of this decision is out of the scope of the present document.

6.2.1.8   Charging

The SPDF shall be able to provide charging information for the Request/Modify/Release/Abort commands when necessary.

6.2.1.9   Deployment considerations

Due to the possible business roles in an access environment, the SPDF receiving the request from the AF may be either in the same administrative domain or in a different administrative domain from the terminating A-RACF.

The SPDF permits other instances besides IMS to request and control resources.

NOTE: As for any other functional entity, implementors may choose to combine the SPDF with the AF where this makes sense in the context of the business models, services and capabilities being supported (e.g. in the case of implementations supporting IMS services only). However, if this deployment option is adopted, there are some implications that should be taken into account:

- the service control/application Sub-System that hosts the AF and the SPDF in the RACS Sub-System can no longer belong to two different administrative domains;

- a SPDF (and associated transport network resources) can only serve the service control/application Sub-System that hosts the Application Function (AF) (e.g. an IMS-only NGN network).

6.2.1.10   Overload control

The SPDF provides bi-directional overload control mechanisms, which helps to limit the load on the A-RACF, SPDF, BGF or AF should any of these components experience overload. A full specification of this capability is left as an outstanding issue.

6.2.1.11   Discovery mechanism

The AF can obtain the RACS contact point from the NASS as a FQDN or IP address of the SPDF. Alternatively, in the absence of such a possibility, the AF may have other mechanisms, e.g. local configuration may be used.

The SPDF relies on local configuration to discover the contact points for the A-RACFs and the BGFs.

6.2.2   Generic Resource Admission Control Function

6.2.2.1   Main functions

The generic Resource Admission and Control Function (x-RACF) is a Functional Entity that acts as a Local Policy Decision Point (PDP) in terms of subscriber access admission control, as well as in terms of resource handling control. However, the final Policy Decision Point of the overall RACS framework is the SPDF.

The generic Resource Admission Control Function receives requests for QoS resources from the SPDF via the Rq reference point, indicating the desired QoS characteristics (e.g. bandwidth).

In Release 1, the Rq reference point may either be an interdomain or an intradomain reference point, whereas for the present document it can only be an intradomain reference point.

In Release 1, in interdomain scenarios, the generic Resource Admission Control Function shall authenticate the SPDF requesting resources. For intradomain scenarios, either in Release 1 or in the present document, the generic Resource Admission Control Function checks if the request matches the requestor's (operator SPDF) profile. Only validated requests for authenticated requesters shall be authorized and retained as input. For further details related to the interdomain and intradomain nature of the Rq reference point in Release 1 and in the present document, please refer to clause 6.3.1.1.

The generic Resource Admission Control Function shall indicate to the SPDF whether a request for resources is granted or not via the Rq reference point. When granting such requests, the generic Resource Admission Control Function may derive and install a L3/L2 traffic policy in the RCEF, which may include indications about the way how traffic control, e.g. gate control, packet marking, or rate limiting control, should be handled. This derivation process is preceded by the mapping of the network QoS parameters, either related to the L3, i.e. IP level that is usually associated with technology independent, or to the L2 that is usually associated with technology dependent, as well as by the inclusion of priority indications on the service and media requests related to specific parameters carried in the above mentioned L3/L2 traffic policies.

Besides the admission control, the resource reservation, and the derivation and installation of L3/L2 traffic policies processes, the generic Resource Admission Control Function may also be involved in aspects related to QoS handling, i.e. monitoring and report of transport resources, which may lead to the modification and enforcement of new L3/L2 traffic policies. In present document, these QoS aspects are only covered in informative annex E.

6.2.2.1.1 Specializations of x-RACF

Two functional specializations of the generic Resource Admission Control Function are defined in the present document: Access-RACF (A-RACF) and Core-RACF (C-RACF), which can be deployed in different network domains based on the operator's requirements. The main distinction between A-RACF and C-RACF is:

- The A-RACF checks the subscriber QoS profile obtained from the NASS in the context of resource admission control. The A-RACF is deployed in the access network domain, which may require the provisioning of the transport resources on a per subscriber basis.

- The C-RACF does not need to check the subscriber QoS profile in the context of resource admission control. The C-RACF is deployed in the core transport network domain, which may not provision the transport resources on a per subscriber basis.

The C-RACF specialization is not further standardized in the present document.

6.2.2.1.2 Reference points applicable to different specializations of x-RACF

Table 4 lists which reference points are applicable to the different specializations of x-RACF.

Table 4: Reference points per x-RACF specialization

Reference Point	Specialization of x-RACF	
	A-RACF	**C-RACF**
e4	applicable (see note 1)	see note 2
Re	applicable	see note 2
Rq	applicable (see note 1)	see note 2
Rf	applicable (see note 1)	see note 2
Rr	applicable	see note 2
NOTE 1: Restrictions for the applicability of this reference point apply when multiple instances of A-RACF are deployed within the same transport segment and/or the same service. See clause 6.2.2.1.3 for details.		
NOTE 2: The C-RACF is not further standardized in the present document.		

6.2.2.1.3 Multiple instantiations of x-RACF

Multiple instances of x-RACF are allowed for the same transport segment and/or service. One or more of those instances may be located within transport network elements (e.g. AN and/or IP_Edge).

An x-RACF instance may have a complete or partial view of the network topology and/or resources.

Each x-RACF instance may be involved in resource admission control for unicast services, multicast services, or both (e.g. in case network resources are to be shared between these services).

Coordination of admission control is achieved via the Rr reference point between x-RACF instances. This coordination may be needed to avoid uncontrolled overbooking, to reserve resources spanning multiple transport segments, or both. The Rr reference point is restricted to intradomain usage.

An x-RACF may coordinate resource admission control decisions on a per-request basis, or for multiple requests following a bulk resource coordination approach. The bulk resource coordination approach is used when an x-RACF makes resource admission control decisions independently without consulting other x-RACFs on a per-request basis and multiple x-RACFs are managing the same resources. The usage of those resources must then be coordinated between these instances through bulk resource reservation requests and/or bulk resource delegation. This coordination requires the x-RACFs to be aware of the current network topology and the associated available and allocated resources.

An x-RACF instance may coordinate admission control decisions to another x-RACF following one or more of the following procedures:

- As reservation requests arrive to an x-RACF, delegate them to another x-RACF to make the admission control decision for the reservation request (i.e. per-request coordination).

- Requesting bulk resources from another x-RACF for the purpose of performing admission control for arriving reservation requests without performing per-request coordination.

- Delegating the control of bulk resources to another x-RACF to perform admission control for arriving reservation requests without performing per-request coordination.

Please refer to clause 6.3.8.1.1 for the definition of the types of request and delegation models in the Rr reference point.

Instances of the x-RACF being involved in controlling the same transport resource, e.g. a resource represented by a specific ATM VP, shall be arranged in a tree structure. The top tier x-RACF in this structure is the one interacting with SPDF, and, when applicable, CLF and the Charging functions.

6.2.2.2   Summary of generic Resource Admission Control Function Elementary Functions

This clause contains a table where the above identified elementary functions for the generic Resource Admission Control Function have been shortly summarized. In addition, information on those elementary functions associated with the A-RACF and C-RACF instances is also indicated in two separated columns.

In this table, the descriptions related to technology dependent and to technology independent functions already indicated for Table 4 continue to be applicable.

Table 5: RACS Elementary Functions associated to generic Resource Admission Control Function

Acronym	x-RACF Elementary Function	Description	A-RACF	C-RACF see note 1
SSAP	Storage of subscriber access profile during attachment	Storage of the subscriber profile after subscriber attachment, including a QoS profile.	O see note 2	see note 1
NPAH R1	Network Policy Assembly Handling	Authentication and authorization of the FE requesting resources, and check if the request matches the subscriber access requestor's profile, e.g. guaranteeing that the total of the requests match the access capabilities.	M	see note 1
NPAH R2	Network Policy Assembly Handling	Authentication and authorization of the FE requesting resources, and check if the request matches the subscriber access requestor's profile, e.g. guaranteeing that the total of the requests match the access capabilities.	O see note 3	see note 1
ACP	Admission control process	Derivation of a QoS profile and check of the availability of resources for unicast and multicast services.	O see note 2	see note 1
RRP	Reservation of resources process	Resource reservation taking into account the resource management scheme used in the SPDF request, i.e. single-stage resource management, two-stage reserve-commit resource management, or authorize-reserve-commit resource management.	O see note 2	see note 1
DITP	Derivation and Installation of Traffic Policies	Derive and install of QoS parameters as part of L3/L2 traffic policies.	O	see note 1
QMTD	QoS and Priority Mapping - Technology Dependent	Mapping of the network QoS parameters to transport (technology-dependent) QoS parameters.	M	see note 1
TDDP	Technology Dependent Decision Point	Makes technology-dependent and resource-based admission decisions for unicast and multicast services.	M	see note 1

Acronym	x-RACF Elementary Function	Description	A-RACF	C-RACF see note 1
MITP	Modification and Installation of new Traffic Policies	Actions taken upon QoS handling process, e.g. by monitoring and controlling of access resources.	O	see note 1
HMRP	Handling of media request priority	Ability to handle the media priority received in the resource reservation request.	O see note 2	see note 1
QMTI	QoS and Priority Mapping - Technology Independent	Maps the service QoS requirements and priority received from the AF to network QoS parameters (e.g. Y.1541 class) and priority, see note 4.	O see note 2	see note 1
GC	Gate Control	Controls the opening and closing of a gate, see note 4.	M	see note 1
IPMC	IP Packet Marking Control	Decides on the packet marking and remarking of traffic flows, see note 4.	M	see note 1
RLC	Rate Limiting Control	Decides on the bandwidth limit of traffic flows (e.g. for policing), see notes 4 and 5.	M	see note 1
HSRP	Handling of service request priority	Ability to indicate a service priority level in the resource reservation request, see note 4.	O see note 2	see note 1
PPS	Policy based path selection	Ability to choose the best appropriate path for the requested service flow according to network policy, the requester class, the quality requirements and network resource status, and to indicate the selected path to the RCEF, see note 6.	O	see note 1

NOTE 1: The C-RACF is not further standardized in the present document.
NOTE 2: If multiple instances of A-RACF are being involved in controlling the same transport resource, the EFs marked with this note 2 are <u>all</u> mandatory for at least one of the A-RACF instances. This also ensures the backward compatibility of the present document with Release 1.
NOTE 3: The Rq reference point is intradomain for the present document.
NOTE 4: This Elementary Function is common to the SPDF and to the generic Resource Admission Control Function.
NOTE 5: In the case of generic Resource Admission Control Function, this functionality may take the form of a parameter that belongs to a L3/L2 traffic policy (DITP).
NOTE 6: The network policy maybe derived from service based policy or pre-defined by the network operators. The PPS should determine the appropriate (virtual) path (e.g. VPN)for the requested service flow based on the network policy, the requester class, the quality requirements and network resource status. Admission control should also be performed for the requested service flow. The sequence of admission control and policy-based path selection should be an implementation option. At last, the PPS should indicate to the RCEF the appropriate virtual path for the accepted service flow.

6.2.2.3   A-RACF

6.2.2.3.1   A-RACF main functions

The Access-Resource Admission and Control Function (A-RACF) is a functional instance of the generic Resource Admission Control Functional Entity (generic Resource Admission Control Function) that is deployed over access network domains. The main functions of A-RACF are the same as those indicated for the generic Resource Admission Control Function in Table 5 of clause 6.2.2.2.

6.2.2.3.2   Reference points

The A-RACF interfaces with the NASS via the e4 reference point.

The e4 reference point is used for Connectivity session Location and repository Function (CLF) in the Network Attachment Sub-System (NASS) to send network attachment information and the subscriber access profile information to the A-RACF.

The A-RACF also interfaces with the SPDF via the above mentioned Rq reference point, and with the RCEF via the Re reference point.

The Rr reference point is an intra-domain reference point between A-RACF instances. It is used to delegate and/or coordinate admission decisions between A-RACF instances that share responsibility for a given network segment.

The A-RACF also interfaces with the Charging Functions via the Rf reference point.

6.2.2.4   C-RACF

6.2.2.4.1   C-RACF main functions

The Core-Resource Admission and Control Function (C-RACF) is a functional specialization of the generic Resource Admission Control Functional Entity that resides in the core transport network domains. The main functions of C-RACF are the same as generic Resource Admission Control Function as described in clause 6.2.2.2. The elementary functions supported by C-RACF are a subset of the generic Resource Admission Control Function shown in Table 5.

The C-RACF is not further standardized in the present document.

6.2.2.5   Admission control process

6.2.2.5.1   A-RACF

The A-RACF performs admission control for the access and aggregation segment following a admission control procedure involving one or two steps depending on the operator's policy:

1)   **Subscriber access profile-based checking:** The A-RACF checks that the amount of requested bandwidth is compatible with the corresponding portion of the subscriber access profile, which may be received from the NASS over the e4 reference point, and the amount of bandwidth remaining in this envelope taking into account existing reservations.

2)   **Resource admission control:** If the admission control request references resources under the control of the particular A-RACF instance which received the request, this A-RACF instance verifies that the available resources are compatible with the requested resources taking into account existing reservations. Resource admission control performed by an A-RACF can involve correlating session information from multiple subscribers sharing the same resources. The resource request will include information which will allow the identification of the appropriate resource(s). Please refer to clause 6.2.2.1.3 for details on the procedures in case multiple A-RACF instances exist.

   NOTE 1: Step 1 and Step 2 may give different results in case of nomadism or in case resources are shared between multiple subscribers. The second step will typically involve checking transport resources in the access segment (e.g. bandwidth allocated to an ATM VC) and in the aggregation segment (e.g. bandwidth allocated to a VLAN or an ATM VP).

   NOTE 2: Further details on admission control scenarios are provided in annex C.

The NASS informs the A-RACF when a subscriber attaches to the network. The subscriber access profile received from NASS (ES 282 004 [5]) over the e4 reference point consists:

- Subscriber attachment info: Subscriber ID, Physical Access ID, Logical Access ID, Access Network Type and Globally Unique IP Address.

- QoS Profile Information (optional): Transport Service Class, UL Subscribed Bandwidth, DL Subscribed Bandwidth, Maximum Priority, Media Type and Requestor Name. The QoS Profile may contain one or more sets of information elements.

- Initial Gate Setting (optional): List of Allowed Destinations, UL Default Bandwidth, DL Default Bandwidth.

On the other hand, the SPDF provides the following information that is relevant to A-RACF procedures when it receives a request via the Rq reference point:

- Subscriber Id or IP address.

- Requestor Name/Service Class.

- Media Description.

- Service Priority.

The Physical Access ID, Logical Access ID and Access Network Type allows A-RACF to bind the Subscriber Id and/or its IP address to the topology information of the access and aggregation networks hosted in A-RACF.

The A-RACF uses the Initial Gate Setting, the capabilities of the elements in the data plane as well as access network policies, defined by the operator, to derive the initial traffic policies that must be installed in the RCEF.

When a resource request is received from the SPDF, based on the Subscriber Id and/or the IP address, the A-RACF identifies the subscriber access profile previously received from the NASS.

Local configuration shall determine the behaviour of the A-RACF if the QoS profile was not received from NASS.

The A-RACF first matches the Requestor Name in order to identify one or more QoS profile that applies to the request. In case more than one profile is identified, the A-RACF further matches the Media Type and Transport Service Class as received over Rq and in the QoS Profile.

A request over Rq may be denied if no information element set matches the request in accordance with local policies. In this process the Maximum Priority parameter (e4) is compared with the Media Priority parameter (Rq).

The A-RACF shall deny a request from the SPDF if it is not permitted by the selected QoS profile in accordance with local policies.

If the request is permitted by the QoS profile, the A-RACF shall verify whether it is compatible with the resources available in the access and aggregation segments.

An A-RACF instance may forward requests to other instances of A-RACF over the Rr reference point.

The request from the SPDF will be permitted only if all media can be accepted in all A-RACF instances. In A-RACF, a request can not be partially accepted. When granting such requests an A-RACF may install a traffic policy in the RCEF.

The A-RACF returns the result of the admission control process to the SPDF, which may include a Resource Bundle-Id representing the group to which the granted resource belongs.

NOTE 3:   The way the Resource Bundle-Id is defined is a local policy in the A-RACF. It represents a set of resources reservation sessions grouped together by A-RACF policies (e.g. represent the usage of a certain device in the transport network). The Resource Bundle-Id may represent a bundle of resources reservation session.

The A-RACF may perform overbooking admission control if it receives an indication to do so from the SPDF, and if normal admission control fails due to lack of resources on the Layer 2 resource for the transport service class concerned by the request. The A-RACF acts as follows:

- The A-RACF considers if resources are already reserved or committed by another Application session for the same Layer 2 resource.

- The A-RACF considers the sum of resources available on this Layer 2 resource plus the resources reserved or committed by any of this(ese) other Application (s) session(s) and verifies whether the requested resources do not exceed this amount.

- If it is the case, the admission control is granted provided that only one Application session commits the same resources at a time; otherwise the A-RACF shall deny the request.

6.2.2.5.2   C-RACF

The C-RACF is not further standardized in the present document.

6.2.2.6   Installation of policies

The following text is only applicable to the A-RACF specialization. The C-RACF is not further standardized in the present document.

Traffic policies installed in the RCEF may result in traffic conditioning mechanisms being applied to L2 and/or L3 in the transport data plane. The list below provides some examples of traffic conditioning mechanisms in RCEF that are installed on request from A-RACF by means of generic transport policies:

- pure L2 QoS mechanisms, e.g. VP/VC based for ATM networks, DLCI based for FR networks, or VLAN tag for Ethernet;

- intermediate L2/L3 QoS mechanisms, e.g. MPLS;

- pure L3 QoS mechanisms, e.g. DiffServ;

- L3 over L2 QoS mechanisms, e.g. DiffServ over ATM or FR;

- L3 over intermediate L2/L3, e.g. DiffServ and MPLS seamless integration.

In the context of the present document, A-RACF shall deal with both L2 and L3 policies. The use of L2 policy types by RCEF could be achieved by allocating a particular Id to each policy. In that case, RCEF would have to perform a certain policy based on its own interpretation of the L2 parameters, or of the L2 parameters combined with others, included in pre-defined/provisioned traffic policies. A-RACF could also explicitly specify the L2 traffic polices to RCEF.

As such, A-RACF shall be capable of:

- providing an explicit description of the traffic policies to be applied. This option is applicable to both L2 and L3 policies (e.g. DiffServ); and

- attaching a pre-defined traffic policy to the media flow(s). In this case the A-RACF provides a policy-id, which will be translated into specific traffic policies to be applied. This option is applicable to both L3 and L2 policies.

For guaranteed QoS, the A-RACF may enforce its admission control decision by setting L2/L3 QoS traffic policies in the RCEF via the Re reference point to police the subscriber traffic.

NOTE: The A-RACF may set QoS policies in the Access Node (AN) and/or the CPN but the mechanism to do so is outside the scope of the present document.

For relative QoS, the A-RACF "pushes", via the Re reference point, an IP QoS policy that updates dynamically the QoS differentiation parameters (e.g. DiffServ QoS parameters in the RCEF).

6.2.2.7   Charging

The following text is only applicable to the A-RACF instance. The C-RACF is not further standardized in the present document.

The A-RACF shall be able to provide charging information for the Request/Modify/Release/Abort commands when necessary.

6.2.2.8   Abnormal condition handling

The following text is only applicable to the A-RACF instance. The C-RACF is not further described in the present document as the extension to the core segment of the Transport Processing Functions sub-layer is not handled.

The A-RACF relinquishes all resource related to the affected resource reservation sessions. The A-RACF may also indicate when a bundle of resources are no longer available, if applicable.

The A-RACF may inform those other Functional Entities, if possible, which have been involved in the creation of the resource reservation.

6.2.2.9   Deployment considerations

The following text is only applicable to the A-RACF instance. The C-RACF is not further standardized in the present document.

The architecture allows multiples instances of A-RACF in the same access network. In this case, multiple A-RACF instances controlling the same resources shall operate in a coordinated manner according to procedures described in clause 6.2.2.1.3.

6.2.2.10   Overload control

The following text is only applicable to the A-RACF instance. The C-RACF is not further standardized in the present document.

The A-RACF may provide an overload control mechanism towards the SPDF, which helps to limit the load on the A-RACF should the A-RACF components experience overload. A full specification of this capability is left as an outstanding issue.

6.2.2.11   Discovery Mechanism

When multiple A-RACF instances are present and arranged in a hierarchical structure, the top tier A-RACF provides the e4 reference point and can identify lower tier A-RACFs based on the association between user location information (e.g. logical or physical access id acquired from NASS via e4) and the corresponding lower tier A-RACF id configured in the top tier A-RACF.

6.2.3   BGF

6.2.3.1   BGF main functions

The BGF is a packet-to-packet gateway for user plane media traffic. The BGF performs both policy enforcement functions and NAT functions under the control of the SPDF in each of the network segments: access, aggregation and core. An overview of the services provided by BGF is given in Table 2.

> NOTE: Static forwarding functions may be inserted in the IP path. How many functions are inserted and whether each function is acting on user plane media traffic, signalling traffic or both is a matter for each operator to decide. These functions are not visible to the RACS and are therefore outside the scope of the present document.

The BGF has a policy enforcement function that interacts through the Ia reference point with the SPDF and is under the control of the SPDF. The BGF operates on micro-flows, i.e. on individual flows of packets belonging to a particular application session. The BGF's policy enforcement function is a dynamic gate that can block individual flows or allow authorized flows to pass. For an admitted flow the SPDF instructs the BGF to open/close its gate for the particular flow, i.e. to allow the admitted flow to pass through the BGF.

Possible resources that are managed by the BGF includes the handling of a pool of IP addresses/ports and bit rate on the BGF reference points.

6.2.3.2   BGF parameters

Unidirectional micro-flows are specified by the SPDF towards the BGF in terms of a flow classifier including the standard 5-tuple (source IP address, destination IP address, source port, destination port, protocol). Elements of the 5-tuple that are unknown to the SPDF may be wild-carded by the SPDF in the instructions to the BGF.

Per admitted micro-flow, the SPDF may instruct the BGF to apply policies (e.g. traffic-conditioning filter) that limit the throughput of the flow to an admitted level indicated by the SPDF.

The usage of the BGF shall allow different combinations of parameters. As such:

- It must be possible to control the following services: address latching, NAT, QoS marking, bandwidth limiting and usage metering.

- It must be possible to provide media address and port information both towards and from the BGF for NAT control.

- It must be possible to provide mid-session updates related to NAT control and bandwidth policing over the reference point.

- It must be possible to indicate if RTP is used as media transport protocol, in which case the NAT must be able to establish both RTP and RTCP flows.

- It must be possible to provide an address independent media session identifier, since the address information may change during the media session.

6.2.3.3   Reference points

The reference point between the SPDF and the BGF is Ia.

6.2.3.4   Addressing latching

When a NAT device is located between a UE and the BGF, the remote media IP address/port information provided using signalling information (e.g. a SDP body in a SIP message) can not be used by the BGF to send media towards the user (instead, the media must be sent towards a specific IP address/port of the entity providing the NAT functionalities, reserved for the UE).

In the present document, address latching corresponds to determining the address on which the BGF listens for media on the local IP address/port the BGF has reserved for the remote UE as requested from SPDF. When media is received the BGF stores the IP address/port value from where the media was received (IP address/port of the entity providing the NAT functionality), and uses that information when forwarding media towards the UE. The NAT providing entity then forwards the media to the actual IP address/port of the UE.

6.2.3.5   Abnormal conditions handling

The BGF notifies the SPDF when it detects a network failure condition whereby it can no longer support the previously agreed services, and that will lead to the release of a previously allocated resources.

6.2.3.6   Overload control

The BGF may provide an overload control mechanism towards the SPDF, which helps to limit the load on the BGF should the BGF components experience overload. A full specification of this capability is left as an outstanding issue.

6.2.4   RCEF

6.2.4.1   RCEF main functions

When operating in the QoS Push mode, the Resource Control Enforcement Function (RCEF) performs policy enforcement functions for unicast and/or multicast after installation of traffic policies under the control of the x-RACF.

When operating in the QoS Pull mode, the Resource Control Enforcement Function (RCEF) also performs policy enforcement for unicast and/or multicast, after:

- having received a request from the BTF;

- having generated events, e.g. query for resources, which trigger a policy evaluation in the x-RACF based on the information received from the BTF;

- having received installation of traffic policies under the control of the x-RACF.

The RCEF is managed by the RACS through the Re reference point.

The RCEF is usually located in a Transport Network node Element, i.e. Access Nodes and/or IP-Edge nodes.

RCEFs may exist in the same Access Network Domain.

6.2.4.2   Reference points

The traffic policies for both unicast as well as multicast data are provided by the x-RACF to the RCEF through the Re reference point. Events which are to trigger a policy evaluation are sent by RCEF via the Re reference point to x-RACF.

RCEF may also interact with BTF to enforce policies which impact data forwarding behaviour, such as data replication for multicast traffic.

6.2.4.3   RCEF parameters

Unidirectional micro-flows are specified by the x-RACF towards the RCEF in terms of a flow classifier including the standard 5-tuple (source IP address, destination IP address, source port, destination port, protocol). Elements of the 5-tuple that are unknown to the x-RACF may be wild-carded by the x-RACF in the instructions to the SPDF.

It must be possible to provide mid-session updates over the Re reference point.

It must be possible to provide an address independent media session identifier, since the address information may change during the media session.

6.2.5   Application Function (AF)

6.2.5.1   AF main functions

This clause looks at requirements on Application Functions (AFs) related to controlling bearer resources. The AF is not a stand-alone functional entity of the NGN architecture. It is a convenient short cut to represent the functionality that exists in some Service Control Sub-Systems and Applications to interact with the RACS when the QoS "Push" Model is used.

The AF is expected to perform the operations when requesting resources following the push model, as defined in clause 6.1, indicated below.

The AF shall provide information to the SPDF to identify media flows to express the service expected from RACS and the bandwidth that needs to be authorized and allocated for those flows. Bandwidth requirements shall be complemented with class based service information indicating service expectations such as QoS characteristics, which transfer layer resources that should be used, and whether service from BGF, A-RACF, or both is requested. This class-based information may also capture predefined traffic characteristics. Resource priority requirements may also be supplied.

The AF shall indicate whether the media should be enabled (i.e. gate opened) when resources are allocated. Alternatively, the gate AF may request that the gate be opened later, after resources are committed.

The AF shall be capable of issuing reservation modify and release messages that contain the same reservation information as provided in reservation request and commit messages together. The AF shall further be capable of updating time limited reservations through reservation modify messages and through reservation refresh messages.

In the case where a NAT function is required, the AF shall request address-mapping information and shall do any modifications that may be required to address information within application signalling (e.g. SDP).

In the case where support of a hosted NAT is required, the AF shall request address latching, since the remote media IP address/port information provided within application signalling (e.g. SDP) cannot be used to send media towards the UE behind the NAT.

The AF shall provide overload control capabilities, which enable the AF to reduce its resource request rate when overload is detected within the RACS. Also, the AF may request that the RACS reduces its rate of notifications to the AF, in case of overload within the AF. A full specification is left as an outstanding issue.

The AF may be capable of operating in a mode of operation by means of which the AF request resources for media flows belonging to a single application session per resource request.

The AF may be capable of operating in any or all of the following modes of operation:

- the mode where a single resource reservation request per application session is issued by the AF;

- the mode of operation where multiple independent resource reservation requests per application session are issued either from a single or multiple AFs, where each independent request is intended to reserve a different set of resources within the network.

The AF is entitled to use Subscriber-Id and/or an IP address to identify to RACS the resource being requested. The decision of what information is provided to RACS depends on the type of application and it is outside of the scope of the present document.

When following the pull model as defined in clause 6.2.2.1.3, the AF is expected to operate as indicated below.

The AF may provide information to the SPDF to authorize consecutive reservation requests from transport functions. This information may include bandwidth requirements, indications of service expectations such as QoS characteristics, and which transfer layer resources that should be used.

6.2.5.2 Reference points

The Application Function (AF) interacts with the SPDF via the Gq' reference point. It makes requests for bearer resources and may receive notifications when resources are reserved and released.

6.2.5.3 Charging

The AF shall be able to provide charging information for the Request/Modify/Release/Abort commands when necessary.

6.2.5.4 Abnormal conditions handling

Abnormal conditions are reported by the SPDF indicating that the current reservations are no longer valid. The AF behaviour that follows is application dependent and the RACS does not make any assumption on that. The abnormal condition information is sent to the AF after all resource session and state information is cleared in RACS.

6.3 RACS reference points

6.3.1 Rq reference point (SPDF - A-RACF)

6.3.1.1 Functional requirements

The Rq reference point provides interaction between the SPDF and the A-RACF functional building blocks of the RACS architecture. The Rq requirements are classified in functional and non-functional elements.

The A-RACF provides facilities for topology-aware resource reservation, resource reservation tracking, and a resource-constraint-based admission control service that shall be addressed through the Rq reference point.

The Rq reference point is used for QoS resource reservation information exchange between the SPDF and the A-RACF. Via the Rq reference point the SPDF issues requests for resources in the access and aggregation networks, indicating IP QoS characteristics.

In Release 1 inter-domain aspects are not explicitly addressed. As the SPDF and the A-RACF may be located in different administrative domains, the Rq reference point may be an interdomain reference point.

For the present document, as each administrative domain shall have at least one SPDF, and the reference point between SPDFs is the only type of reference point between RACS instances in different administrative domains, the Rq reference point is always a intradomain reference point.

Use of the Rq reference point as an inter-domain reference point as described in R1 should be avoided.

NOTE: Backwards compatibility between implementations of both releases is always ensured as long as possible encryption of the Rq reference point performed by the Release 1 FEs for security reasons, has an appropriate treatment by the present document FEs.

Following functional requirements are directly derived from the role and position of the Rq reference point in the RACS.

6.3.1.1.1 Resource management mechanisms

The Rq reference point shall support a versatile set of resource management schemes, suitable for coping with all target deployment architectures, as stipulated and defined in the present document. In this context, the following resource management schemes must be supported:

- proxies resource reservation with "policy-push";

- support for all the scenarios defined in RACS functional architecture:

  - QoS request initiated by Application Function.

  - QoS request initiated by CPN through the application layer signalling with QoS negotiation extensions.

- flexibility for evolution in future NGN releases;

- the Rq reference point shall provide subsequent resource management models in support of these requirements:

  - Single-stage resource management model, providing resource management services in a mode where reserved resources are immediately available upon successful reservation.

  - Two-stage reserve-commit resource management model that can be leveraged in support of services that aim to support charging per service-invocation, and require as such service-theft-prevention solutions.

  - Authorize-reserve-commit resource management model, supporting service-based local policy control under coordination of a network-hosted application function.

6.3.1.1.2 Service model

The services provided for each of the resource reservation models shall offer the following capabilities:

- the service model shall allow resource reservation for an individual application session that can involve multiple media flows. A media flow may be uni-directional or bi-directional (combining in effect two uni-directional flows);

- the resource management model established through the Rq reference point shall support atomicity of resource management services at the level of an application session. This implies support for collective reservation, release, and modification of resource requirements for all the media flows that belong to the application session;

- a resource requirement budget can be established for each individual service flow of the application session;

- mid-session modification of previously established resource reservations shall be supported for individual service sessions in an atomic manner (e.g. in support of service session modifications that have to be accommodated on behalf of SIP re-invite). Atomicity shall be guaranteed, per mid-session modification, across all changes that are in order for the individual media flows of the session, including:

  - modification (increase or reduction) of resource requirements reserved on behalf of selected individual media flows;

  - release of resources previously reserved on behalf of a selected individual media flows;

  - creation of new resource reservation on behalf of new individual media flows that are added to the service session.

- collective release of all resources for an application session.

6.3.1.1.3   Duration semantics

In terms of duration semantics, the resource management model supported by the Rq reference point shall support both soft-state and hard-state resource management approaches along with the following functions:

- for both approaches Rq shall support facilities for explicit removal of previously established resource reservation;

- for both approaches Rq shall support facilities for explicit modification of previously established resource reservation;

- granularity of removal and modification facilities shall be at the level of individual flow reservations;

- Time Limited hard-state with update possibilities;

- Resource Modification Request primitive must be capable of carrying information needed to create reservation states. This means that all parameters provided in Reservation Request message must be possible to include in ReservationModify primitive. Thereby the A-RACF can rely on states kept in AF to support seamless fail over instead of replicating soft state reservations.

6.3.1.1.4   Audit and synchronization support

The only mechanism for synchronization over Rq supported in the present document implies the use of soft-state reservation.

The Rq does not support any audit mechanism in the present document.

6.3.1.1.5   Report facilities for unsolicited events

The Rq reference point shall support facilities for indicating, on a per request basis, relevant events such as revocation of established resource reservations.

6.3.1.2   Non-functional requirements

The Rq reference point shall support the non-functional requirements indicated in clauses 6.3.1.2.1 and 6.3.1.2.2.

6.3.1.2.1   Reliability requirements

The Rq reference point shall provide mechanisms to ensure reliability of all communication performed over the interface.

6.3.1.2.2   Security requirements

The security requirements for RACS are described in TS 187 001 [14].

6.3.1.3   Information exchanged over the Rq Reference Point

6.3.1.3.1   Resource Reservation Request

The resource reservation request message is used to request resources from the SPDF to the A-RACF. The SPDF knows the address of the A-RACF entity based on local configuration data. The Resource Request contains the following information elements:

Table 6: Resource Reservation Request - Information Elements

Resource Req (SPDF -> A-RACF)	
Application Function Identifier	Global unique Identifier for the application function instance.
Resource Reservation Session ID	The reference is a unique resource reservation session identifier in the scope of the Application Function Identifier.
Subscriber-ID (optional)	It identifies the subscriber attached to the access network (see note 1).
Globally Unique IP Address (optional)	Globally Unique address that corresponds to the UNI associated to the subscriber attached to the network (see note 1).
Assigned IP Address	The IP address [Ipv4 or Ipv6].
Address Realm	The addressing domain in which the IP address is significant (see note 2).
Requestor Name	Identifies the RACS client requesting the resources (e.g. name of a ASP or group of ASPs). This name corresponds to the Requestor Name in a QoS profile provided by NASS.
Service Class	Service class requested by the SPDF. It reflects the service relationship between the A_RACF and SPDF owners. The set of Service Classes that are offered to an SPDF is an administrative matter.
Service Priority (optional)	The priority associated to the service request that defines the handling precedence by the receiving entity.
Charging Correlation Information (CCI) (optional)	Globally unique identifier for charging correlation purposes.
Duration of Reservation (optional)	Duration of the reservation requested by the client.
Authorization package ID (optional)	Identifier of an authorization context for the session. In the case of a multicast reservation, the identified context provides information on the multicast channels allowed or not allowed during the session and their respective QoS requirements.
Media Description	The media description.
Media Type	The pre-defined type of the media for each flow (e.g. Video).
Media Id	Identifier for the specific media.
Media Priority (optional)	The priority associated to the media to be used in the admission control process in A-RACF.
Traffic Flow Parameters	The traffic flow description of the media.
Direction	Direction of the flow.
Flow Id	Identifier for the specific flow.
IP Addresses	Source and Destination IP addresses [Ipv4, Ipv6] and Address Realm that each address belongs to (see note 3).
Ports	Source and Destination Port Numbers (see note 4).
Protocol	Protocol Id (e.g. UDP, TCP).
Bandwidth	The maximum request bit rate.
Reservation Class (optional)	A particular index that identifies a set of traffic characteristics of the flow (e.g. burstiness and packet size).
Transport Service Class (optional)	Identifies the forwarding behaviour to be applied to the particular flow (see note 5).
Commit Id	Identify if request is to be committed.
Overbooking request indicator (optional)	Indicates that the A-RACF may process the resource request in overbooking mode.
NOTE 1: At least one of these two parameters - Subscriber-ID or Global Unique IP address - shall be provided.	
NOTE 2: It makes the assigned IP address unique, for example it can be a VPN-id.	
NOTE 3: An IP address prefix is supported.	
NOTE 4: Port Ranges are supported and can be defined by specifying the minimum and maximum value or by using a wildcard.	
NOTE 5: Transport Service Class is also part of QoS profile provided by NASS.	

6.3.1.3.2   Resource Modification Request

The resource modification request message is used to modify current resource allocation from the SPDF to the A-RACF. The address information necessary to contact the A-RACF may be received from AF or from an interconnected SPDF in the spdf-transparent-info (the SPDF may have other means to retrieve the A-RACF address). The Resource Mod message contains the following elements:

Table 7: Resource Modification Request - Information Elements

Resource Mod (SPDF -> A-RACF) (see note)		
Application Function Identifier	Global unique Identifier for the application function instance.	
Resource Reservation Session ID	The reference is a unique resource reservation session identifier in the scope of the Application Function (AF) Identifier.	
Requestor Name	Identifies the RACS client requesting the resources (e.g. name of a ASP or group of ASPs). This name corresponds to the Requestor Name in a QoS profile provided by NASS.	
Service Class	Service class requested by the SPDF. It reflects the service relationship between the A--RACF and SPDF owners. The set of Service Classes that are offered to an SPDF is an administrative matter.	
Duration of Reservation (optional)	Duration of the reservation requested by the client.	
Charging Correlation Information (optional)	Globally unique identifier for charging correlation purposes.	
Service Priority (optional)	The priority associated to a service request that defines the handling precedence by the receiving entity.	
Authorization package ID (optional)	Identifier of an authorization context for the session. In the case of a multicast reservation, the identified context provides information on the multicast channels allowed or not allowed during the session and their respective QoS requirements.	
Media Description	The media description.	
	Media Type	The pre-defined type of the media for each flow (e.g. Video).
	Media Id	Identifier for the specific media.
	Media Priority (optional)	The priority associated to the media to be used in the admission control process in A-RACF.
	Traffic Flow Parameters	The traffic flow description of the media.
	Direction	Direction of the flow.
	Flow Id	Identifier for the specific flow.
	IP Addresses	Source and Destination IP addresses [Ipv4, Ipv6] and Address Realm that each address belongs to.
	Ports	Source and Destination Port Numbers.
	Protocol	Protocol Id (e.g. UDP, TCP).
	Bandwidth	The maximum request bit rate.
	Reservation Class (optional)	A the particular index that identifies a set of traffic characteristics of the flow (e.g. burstiness and packet size).
	Transport Service Class (optional)	Identifies the forwarding behaviour to be applied to the particular flow.
Commit Id	Identify if request is to be committed.	
NOTE: Only the Bandwidth inside the Traffic Flow Parameter element can be modified.		

6.3.1.3.3   Resource Request/Modification Confirmation

The resource reservation confirmation message is used to acknowledge the resource reservation or modification by A-RACF. In case the request can not be fulfilled, the appropriate cause is returned to the SPDF. In case of an unsuccessful modification, the BGF also informs if the previous reservation was kept. The message contains the following elements:

Table 8: Resource Confirmation - Information Elements

Resource Mod/Req Cnf (A-RACF -> SPDF) (see note)	
Application Function Identifier	Global unique Identifier for the application function instance.
Resource Reservation Session ID	The reference is a unique resource reservation session identifier in the scope of the Application Function Identifier.
Resource Bundle-Id (optional)	Represents a set of resource reservation sessions grouped together by A-RACF policies. It shall be possible to represent a hierarchy of resources in the resource Bundle-Id associated to that particular RACS resource reservation session.
Duration of Reservation Granted (optional)	Duration of the reservation granted by A-RACF.
Overbooking confirmation indicator (optional)	Indicates that the reservation has been achieved by the A-RACF with overbooking.
Result	The result of the request.
NOTE : The optional parameters are not present in case of an unsuccessful result.	

6.3.1.3.4   Resource Release Request

The resource reservation release message is used by the SPDF to relinquish the resource reservation in A-RACF. A parameter indicates if acknowledgement is expected by the SPDF from the A-RACF. The message contains the following elements:

Table 9: Resource Release - Information Elements

Resource Rel (SPDF-> A-RACF)	
Application Function Identifier	Global unique Identifier for the application function instance.
Resource Reservation Session ID	The reference is a unique session identifier in the scope of the Application Function Identifier (see note).
NOTE: The presence of a wildcard in the session part of the reference indicates that all resources identified associated to the Application Function Identifier shall be released, otherwise only the specific session is released (it implies all media in the session).	

6.3.1.3.5   Abort Resource Reservation

The abort reservation message is used by the A_RACF to indicate to the SPDF that the resource previously reserved is lost. The message may transport an indication for more than one reservation. The message contains the following elements:

Table 10: Abort Reservation- Information Elements

Abort Res (A-RACF -> SPDF) (see note)	
Application Function Identifier	Global unique Identifier for the application function instance.
Resource Reservation Session ID	The reference is a unique Resource Reservation session identifier in the scope of the Application Function Identifier (see note).
Resource Bundle-Id (optional)	It represents a set of resource reservation sessions grouped together by A-RACF policies. It shall be possible to represent a hierarchy of resources in the resource Bundle-Id associated to that particular RACS resource reservation session.
Time Stamp	The time when the resources were lost.
Cause	The cause that lead to the lost of the reservation.
NOTE: A single message shall be able to carry multiples blocks.	

6.3.2   e4 reference point (A-RACF - NASS)

This is the reference point between the A-RACF and the Customer Location Function (CLF) of the network attachment Sub-System (NASS). The reference point e4 is described in ES 282 004 [5].

6.3.3   Ia Reference Point (SPDF - BGF)

This is the reference point between the SPDF and the BGF. This reference point is internal to the administrative domain. The following requirements apply to the reference point.

6.3.3.1   Functional Requirements

The functional requirements for the Ia reference point are presented below in itemized lists.

6.3.3.1.1   Control of NAT, Hosted NAT traversal and Gating

1)   Request of the NAT binding (two terminations, each containing an IP address, port and IP version) to receive and transmit the media flows; information about the allocated bindings must be returned to the requestor.

2)   Indicate, in the NAT binding request, the remote source and destination media parameters for each media flow, including possible wildcarding of specific media parameters (in case the information is not known by the controlling node).

3)   Indicate, in the NAT binding request, the IP address/port latching for specific terminations (if the information cannot be retrieved from signalling data, the data is known to be incorrect, etc.).

4)   Indicate, in the NAT binding request, the media transport protocol (RTP, T.38, MSRP etc.) for each media flow in order for the BGF to be able to perform protocol specific functions (e.g. dual-port reservation for RTP/RTCP, proper statistics collection, etc.).

5)   Indicate, in the NAT binding request, if the media flow is uni- or bi-directional (in case of uni-directional, also indicate the specific direction).

6)   Request mid-session modification of media parameters, including a possible request for new IP address/port latching.

6.3.3.1.2   Transport Protocol Type Policing

1)   Request L4 protocol type policing.

2)   Request mid-session modification of L4 protocol type policing.

6.3.3.1.3   Bandwidth control

1)   Request allocation of bandwidth resources needed for a specific media flow.

2)   Indicate, in the bandwidth allocation request, the bandwidth policing information.

3)   Request mid-session bandwidth modification.

6.3.3.1.4   QoS marking

1)   Indicate QoS marking values (e.g. DiffServ/DSCP) for each egress media flow.

6.3.3.1.5   Usage metering and statistics reporting

Report media flow specific usage metering information (octets of sent data, etc.), when flow is released and during mid-session, if requested.

6.3.3.1.6   Resource state synchronization

Given that resource state synchronization is a required function in order to recover from different failure scenarios, the reference point shall allow:

1)   Reporting of BGF state change (due to rebooting, network failure, HW failure, etc.)

2)   Requesting and Reporting of the current BGF resource state.

6.3.3.2   Non-Functional Requirements

The Ia reference point shall support the following non-functional requirements.

6.3.3.2.1   Reliability requirements

The Ia reference point shall provide a mechanism to guarantee reliability of all communication performed over the reference point.

6.3.3.2.2   Security requirements

The security requirements for RACS are described in TS 187 001 [14].

6.3.3.3   Information exchanged over the Ia Reference Point

The information elements for the Ia reference point are not described in the present document. Further information is available in the Stage 3 documentation.

6.3.4   Gq' Reference Point (AF - SPDF)

6.3.4.1   Functional Requirements

The Gq' reference point allows the AF to request resources from the RACS. Since the SPDF functional entity can only request policy enforcement from other elements in the RACS, the resource reservations performed over Gq' will result, if authorized by the SPDF, in derivative resource reservations and/or service requests over the reference points associated with the SPDF, i.e. Rq, Ia, Rd', and/or Ri'.

Functional requirements over Gq' are therefore a combination of the requirements over the Rq, Ia, Rd', and Ri' reference points, described in later clauses. However, it should be noted that the Gq' reference point is not a simple aggregation of functions resulting in separate information flows for Rq-related, Ia-related, Rd'-related, and Ri'-related requests; the Gq' reference point also allows for reservations relevant to Rq, Ia, Rd' and Ri', to be requested by AFs as a single atomic request, which the SPDF can then split into separate requests and coordinate accordingly depending on the service requested (see clause 6.2.1.7 on the SPDF coordination).

6.3.4.2   Non-Functional Requirements

Non-functional requirements for the Gq' reference point on reliability and security are the same as those defined for the Rq reference point in clause 6.3.1.2.

6.3.4.3   Information exchanged over the Gq' Reference Point

Resource reservation requests over Gq' shall be expressed using the same information elements as those over the Rq and Ia (see clauses 6.3.1 and 6.3.3 above), with the exceptions listed in Table 11.

Table 11: Information Elements with specific meaning in Gq'

Service Class	Service class requested by the AF. It reflects the service relationship between the AF and SPDF owners. The set of Service Classes that are offered to an AF is an administrative matter.
Resource Bundle-Id	Not transported over Gq'.

NOTE: Information elements exchanged over Gq' are described here as equivalent to those over Rq and Ia. However, the actual values given to these parameters at service execution may be different across each of these reference points, depending on mappings performed by the SPDF to requests coming from Application Functions according to the operator's local policies.

6.3.5   Ri' Reference Point (SPDF-SPDF inter-domain)

6.3.5.1   Functional Requirements

The Ri' Reference Point allows provides a means for interaction between two SPDF in different operators domains.

The Ri' Reference Point allows the SPDF in one Originating Domain to trigger Admission Control in the Interconnected Domain. The Ri' Reference Point further allows the Interconnected Domain to communicate the Result of the Admission Control in the Interconnected Domain back to the Originating Domain.

The Ri' Reference Point is the single point of contact to a given Domain, hiding the details of the Topology and Functional Entities within that given Domain.

6.3.5.1.1   Resource management mechanisms

The Ri' Reference Point shall support the same resource management schemes as defined for the Rq and Gq' reference point (see clause 6.3.1.1.1).

6.3.5.1.2   Service model

The services provided for each of the resource reservation models shall offer the following capabilities:

- The service model shall allow resource reservation for an individual application session that can involve multiple media flows. A media flow may be uni-directional or bi-directional (combining in effect two uni-directional flows).

- The resource management model established through the Ri' Reference Point supports a granularity of resource management services at the level of:

    - originating and destination interconnected domains in both directions;

    - application functions.

This model applies to the initial reservation, to the modification, and to the release request.

In the case of the AF granularity, the Ri' reference point is used when an AF can not communicate directly with the RACS of a certain domain but requires reservation of resources in this domain. The RACS in the originating domain relays the AF requests through the Ri' reference point towards the RACS in the destination domain.

- A resource requirement budget can be established for each individual service flow of the Application Session.

- Mid-session modification of previously established resource reservations shall be supported for individual service sessions, i.e. the following mechanisms must be supported:

    - Modification (increase or reduction) of resource requirements reserved on behalf of selected individual media flows.

    - Release of resources previously reserved on behalf of a selected individual media flows.

    - Creation of new resource reservation on behalf of new individual media flows that are added to the service session.

6.3.5.1.3 Duration semantics

In terms of duration semantics, the resource management model supported by the Ri' reference point shall support both soft-state and hard-state resource management approaches along with the following functions:

- For both approaches Ri' shall support facilities for explicit removal of previously established resource reservation.

- For both approaches Ri' shall support facilities for explicit modification of previously established resource reservation.

- The same granularity levels than those described in clause 6.3.5.1.2 shall be available for both approaches.

6.3.5.1.4 Audit and Synchronization support

Audit and Synchronization mechanisms on the Ri' reference point shall be aligned with those offered on the Gq' reference point.

6.3.5.1.5 Report facilities for unsolicited events

The Ri' Reference Point shall support facilities for indicating relevant events such as revocation of established resource reservations.

6.3.5.2 Non-Functional Requirements

6.3.5.2.1 Reliability requirements

The Ri' reference point shall provide mechanisms to ensure reliability of all communication performed over the reference point.

6.3.5.2.2 Security requirements

The security requirements for RACS are described in TS 187 001 [14].

6.3.5.3 Information exchanged over the Ri' Reference Point

The information exchange over the Ri' reference point is not standardized in the present document.

6.3.6 Rd' Reference Point (SPDF-SPDF intra-domain)

The Rd' reference point is not standardized in the present document.

6.3.7   Re Reference Point (A-RACF - RCEF)

6.3.7.1   Functional Requirements

The RCEF entity ensures facilities for the enforcement of L2/L3 traffic policies defined by the access network provider that are communicated by the A-RACF through the Re reference point.

The Re reference point is used for controlling the L2/L3 traffic policies performed in the transport plane, as requested by the resource management mechanisms, i.e. gating, packet marking, traffic policing and mid-session updates functionalities.

According to the common approach adopted, the RACS reference points present functional and non-functional requirements.

In clauses 6.3.7.1.1.1 to 6.3.7.1.1.4, the functional requirements for the Re reference point will be described.

6.3.7.1.1   Policy Enforcement Management

6.3.7.1.1.1   Installation of Policies

After successful authorization of QoS resources, the Re reference point shall allow the A-RACF to install traffic policies in RCEF, in order to enable traffic conditioning in the transport plane.

The installation of a new policy to a particular flow or a group of flows may or may not result in the replacement of a policy previously installed. A confirmation for this request is also required.

In the context of the present document, A-RACF shall deal with both L2 and L3 policies. The use of L2 policy types by RCEF could be achieved by allocating a particular Id to each policy. In that case RCEF would have to perform a certain policy based on its own interpretation of the L2 parameters, or of the L2 parameters combined with others, included in pre-defined/provisioned traffic policies. A-RACF could also explicitly specify the L2 traffic polices to RCEF.

As such, A-RACF shall be capable of:

- providing an explicit description of the traffic policies to be applied. This option is applicable to both L2 and L3 policies (e.g. DiffServ); and

- attaching a pre-defined traffic policy to the media flow(s). In this case the A-RACF provides a policy-id, which will be translated into specific traffic policies to be applied. This option is applicable to both L3 and L2 policies.

In addition, the A-RACF shall be capable either:

- to provide an explicit description of the policies to be applied;

- attach a pre-defined policy of RCEF to the media flow(s). In this case the A-RACF provides a policy-id to the RCEF, which is capable of translating the policy-id into specific policies to be applied.

The specific controls that may be requested are indicated in clauses 6.3.7.1.1.1.1 to 6.3.7.1.1.1.3.

6.3.7.1.1.1.1   Gating

This functionality is performed by the RCEF in the transport plane. The decision of applying Gate Control is dependent on the request that indicates if the associated gate should be opened or closed, as well as on local policies stored in the A-RACF. This command allows the A-RACF to enable or disable IP flows.

6.3.7.1.1.1.2   Packet marking

This functionality is usually associated with the appliance of QoS differentiation mechanisms involving the DiffServ Edge Function.

Where the associated parameters for the DiffServ Edge Function, i.e. classifiers, meters, packet handling actions, may be statically or dynamically configured on the RCEF.

6.3.7.1.1.1.3   Traffic policing

This functionality shall consist of the inspection of each packet performed by the RCEF in order to enforce the decision of the A-RACF. This inspection shall lead to a packet handling action, in terms of packets matching or not the classification, which will result in packets being forwarded or silently discarded.

6.3.7.1.1.2   Removal of Policies

This mechanism shall be initiated by the A-RACF. Upon reception of this message, the RCEF shall release all the resources associated with an existing traffic policy.

6.3.7.1.1.3   Revoke of policies indication

This mechanism shall be initiated by the RCEF every time an external event occurs denoting that the access information is no longer valid. The RCEF shall notify the A-RACF accordingly, and shall release all the resources associated with an existing reservation.

6.3.7.1.1.4   Audit and synchronization support

Not standardized in the present document.

6.3.7.2   Non-functional requirements

6.3.7.2.1   Reliability requirements

Not standardized in the present document.

6.3.7.2.2   Security requirements

The security requirements for RACS are described in TS 187 001 [14].

6.3.7.3   Information exchanged over the Re Reference Point

The information elements for the Re reference point are not described in the present document. Further information is available in the Stage 3 documentation.

6.3.8   Rr Reference Point (x-RACF - x-RACF intra-domain)

6.3.8.1   Functional Requirements

The Rr reference point is used for QoS resource reservation between x-RACF instances of RACS within a single administrative domain. The Rr reference point allows one x-RACF to delegate resource admission responsibility of performing admission control to another x-RACF.

6.3.8.1.1   Overall features

The following overall features shall be supported by the Rr reference point:

- resource admission control shall be applicable for unicast service, multicast service, or both;

- modification of an existing reservation shall be possible, e.g. increase or decrease of an aggregate/bulk reservation.

6.3.8.1.1.1   Types of request

The following types of request shall be supported by the Rr reference point:

- per-request level, which is coupled to reservation requests arriving over Rq or Re, and is only applicable to the unicast service, NOT to the multicast service;

- aggregate level, which is decoupled from reservation requests arriving over Rq or Re. Aggregate level delegation requests are independent from application triggers although they may result from processing of the application level requests.

6.3.8.1.1.2   Delegation Models

The delegation of the responsibility of performing admission control can be initiated either by the x-RACF to which this responsibility is delegated, or by the x-RACF that delegates the responsibility. Delegation instructions shall include admission decision criteria derived from the applicable subset of the user access profile and/or applicable access network policies. The admission decision criteria specifies the parameters used to decide if a particular reservation request can be accepted.

The following delegation models shall be supported by the Rr reference point:

- Request model, where one x-RACF instance solicits the resource reservation (e.g. initial reservation, modification) to another x-RACF instance that is responsible for admission control for those resources within that network segment. The request model can operate with per-request level or aggregate level requests.

- Offering model, where one x-RACF instance offers an aggregate/bulk amount of resources to another x-RACF instance which thereby becomes responsible for admission control to those resources. The offering model is only applicable for aggregate level requests.

6.3.8.1.2   Resource management mechanisms

The Rr Reference Point shall support the following resource management schemes:

- Delegation and interaction of resource admission control and reservation between x-RACF instances.

- Support for all the scenarios defined in RACS functional architecture:

  - QoS request initiated by Application Function;

  - QoS request initiated by CPN through the application layer signalling with QoS negotiation extensions;

  - QoS Request initiated by Transport Processing Functions.

- The Rr reference point shall support subsequent resource management models in support of these requirements:

  - Single-stage resource management model, providing resource management services in a mode where reserved resources are immediately available upon successful reservation.

  - Two-stage reserve-commit resource management model that can be leveraged in support of services that aim to support charging per service-invocation, and require as such service-theft-prevention solutions.

  - Authorize-reserve-commit resource management model, supporting service-based local policy control under coordination of a network-hosted application function.

6.3.8.1.3   Service model

The services provided for each of the resource reservation models shall offer the following capabilities:

- The service model shall allow resource reservation for one or several media flows. The media flows may be part of an application session that can involve multiple media flows. A media flow may be uni-directional or bi-directional (combining in effect two uni-directional flows).

- The resource management model established through the Rr reference point shall support collective reservation, release, and modification of resource requirements for a group of media flows. This group of media flows may for example be associated with an application session.

- A resource requirement budget can be established for each individual service flow.

- Mid-session modification of previously established resource reservations shall be supported for individual service sessions, i.e. the following mechanisms must be supported:

  - Modification (increase or reduction) of resource requirements reserved on behalf of selected individual media flows.

  - Release of resources previously reserved on behalf of a selected individual media flows.

  - Creation of new resource reservation on behalf of new individual media flows that are added to the service session.

6.3.8.1.4   Duration semantics

In terms of duration semantics, the resource management model supported by the Rr reference point shall support both soft-state and hard-state resource management approaches along with the following functions:

- For both approaches the Rr Reference Point shall support facilities for explicit removal of previously established resource reservation.

- For both approaches the Rr Reference Point shall support facilities for explicit modification of previously established resource reservation.

- The same granularity levels than those described in clause 6.3.8.1.2 shall be available for the soft-state and hard-state approaches.

- Resource Modification Request primitive must be capable of carrying information needed to create reservation states. This means that it must be possible to include all parameters of the Reservation Request in the Modification Request. The x-RACF can rely on states kept in AF to support seamless fail over instead of replicating soft state reservations.

6.3.8.1.5   Audit and Synchronization support

Audit and Synchronization mechanisms on the Rr Reference Point shall be aligned with those offered on the Rq Reference Point.

6.3.8.1.6   Report facilities for unsolicited events

The Rr Reference Point shall support facilities for indicating relevant events such as revocation of established resource reservations.

6.3.8.2   Non-Functional Requirements

6.3.8.2.1   Reliability requirements

The Rr reference point shall provide mechanisms to ensure reliability of all communication performed over the Reference Point.

6.3.8.2.2   Security requirements

The security requirements for RACS are described in TS 187 001 [14].

6.3.8.3   Information exchanged over the Rr Reference Point

6.3.8.3.1   Resource Reservation Request

The resource reservation request message is used to request resources sent from one x-RACF (e.g. in a central location) to another x-RACF (e.g. in AN). The originating x-RACF can obtain the location information of another x-RACF based on configuration or derive it from the resource mapping. This message is intended for the support of Request model. The Resource Request contains the following information elements:

Table 12: Resource Reservation Request - Information Elements

Resource Req (Originating x-RACF -> Terminating x-RACF)	
Request Originating Function Identifier	Global unique Identifier for the Request Originating Function instance.
Resource Reservation Session ID	The reference is a unique resource reservation session identifier in the scope of the Request Originating Function Identifier.
Subscriber-ID (optional)	It identifies the subscriber attached to the access network (see note 1).
Globally Unique IP Address (optional)	Globally Unique address that corresponds to the UNI associated to the subscriber attached to the network (see note 1).
Assigned IP Address	The IP address [Ipv4 or Ipv6].
Address Realm	The addressing domain in which the IP address is significant (see note 2).
Requestor Name (Optional)	Identifies the RACS client requesting the resources (e.g. name of a ASP or group of ASPs). This name corresponds to the Requestor Name in a QoS profile provided by NASS.
Service Class (Optional)	Service class requested by the RACS client.
Service Priority (optional)	The priority associated to the service request that defines the handling precedence by the receiving entity.
Charging Correlation Information (CCI) (optional)	Globally unique identifier for charging correlation purposes.
Duration of Reservation (optional)	Duration of the reservation requested by the client.
Physical Access ID (Optional)	The identifier of the physical access to which the user equipment is connected.
Logical Access ID (Optional)	The identifier of the logical access used by the attached user equipment. In the xDSL case, the Logical Access ID may explicitly contain the identifier of VP and/or VC carrying the traffic.
Media Description (Conditional, see note 6)	The media description.
Media Type	The pre-defined type of the media for each flow (e.g. Video).
Media Id	Identifier for the specific media.
Media Priority (optional)	The priority associated to the media to be used in the admission control process in terminating x-RACF.
Traffic Flow Parameters	The traffic flow description of the media.

Resource Req (Originating x-RACF -> Terminating x-RACF)		
	Direction	Direction of the flow.
	Flow Id	Identifier for the specific flow.
	IP Addresses	Source and Destination IP addresses [Ipv4, Ipv6] and Address Realm that each address belongs to (see note 3).
	Ports	Source and Destination Port Numbers (see note 4).
	Protocol	Protocol Id (e.g. UDP, TCP).
	Bandwidth	The maximum request bit rate.
	Reservation Class (optional) (see note 5)	A particular index that identifies a set of traffic characteristics of the flow (e.g. burstiness and packet size).
	Transport Service Class (optional) (see note 5)	A particular index that Identifies the forwarding behaviour to be applied to the particular flow.
Bulk Reservation Description (Conditional, see note 6)		The description of a bulk reservation.
	Direction of the bulk reservation (Optional)	Direction of the requested bulk resources.
	Physical Access ID (Optional, see note 8)	The identifier of the physical access to which the user equipment is connected.
	Logical Access ID (Optional, see note 8)	The identifier of the logical access used by the attached user equipment. In the xDSL case, the Logical Access ID may explicitly contain the identifier of VP and/or VC carrying the traffic.
	Physical Aggregation ID (Optional, see note 8)	The identifier of the physical resource in the aggregation network to which the bulk resource is processed.
	Logical Aggregation ID (Optional, see note 8)	The identifier of the logical resource in the aggregation network to which the bulk reservation is processed.
	Bandwidth	The maximum requested data rate.
	Reservation Class (optional)	A particular index that identifies a set of traffic characteristics of the requested resources (e.g. burstiness and packet size).
	Transport Service Class (optional)	Identifies the forwarding behaviour to be applied to requested resources.
Commit Id (Optional)		Identify if request is to be committed.
Overbooking request indicator (optional, see note 7)		Indicates that the TERMINATING x-RACF may process the reservation request in overbooking mode.
NOTE 1: These two parameters - Subscriber-ID or Global Unique IP address - may not be needed unless per user checking is required. NOTE 2: It makes the assigned IP address unique, for example it can be a VPN-id. NOTE 3: An IP address prefix is supported. NOTE 4: Port Ranges are supported and can be defined by specifying the minimum and maximum value or by using a wildcard. NOTE 5: Transport Service Class is also part of QoS profile provided by NASS. NOTE 6: Dependent on the granularity of requested resources, either Media Description or Bulk Reservation Description shall be present. NOTE 7: The Overbooking Request Indicator is only applicable to per flow request as optional parameter. NOTE 8: Either physical/logical access Ids or physical/logical aggregation connection Ids may be present in the bulk resource reservation.		

6.3.8.3.2   Resource Modification Request

The resource modification request message is used to modify current resource allocation from originating x-RACF to terminating x-RACF. This message is intended for the support of Request model. The Resource Mod message contains the following elements:

Table 13: Resource Modification Request - Information Elements

Resource Mod (Originating x-RACF -> Terminating x-RACF) (see note)	
Request Originating Function Identifier	Global unique Identifier for the Request Originating function instance.
Resource Reservation Session ID	The reference is a unique resource reservation session identifier in the scope of the Request Originating Function Identifier.
Requestor Name (*Optional*)	Identifies the RACS client requesting the resources (e.g. name of a ASP or group of ASPs). This name corresponds to the Requestor Name in a QoS profile provided by NASS.
Service Class (*Optional*)	Service class requested by the RACS client.
Charging Correlation Information (optional)	Globally unique identifier for charging correlation purposes.

Resource Mod (Originating x-RACF -> Terminating x-RACF) (see note)	
Service Priority (optional)	The priority associated to a service request that defines the handling precedence by the receiving entity.
Duration of Reservation (optional)	Duration of the reservation requested by the client.
Physical Access ID (Optional)	The identifier of the physical access to which the user equipment is connected.
Logical Access ID (Optional)	The identifier of the logical access used by the attached user equipment. In the xDSL case, the Logical Access ID may explicitly contain the identifier of the port, VP and/or VC carrying the traffic.
Media Description (Conditional)	The media description.
Media Type	The pre-defined type of the media for each flow (e.g. Video).
Media Id	Identifier for the specific media.
Media Priority (optional)	The priority associated to the media to be used in the admission control process in terminating x-RACF.
Traffic Flow Parameters	The traffic flow description of the media.
Direction	Direction of the flow.
Flow Id	Identifier for the specific flow.
IP Addresses	Source and Destination IP addresses [Ipv4, Ipv6] and Address Realm that each address belongs to (see note 3)
Ports	Source and Destination Port Numbers (see note 4).
Protocol	Protocol Id (e.g. UDP, TCP).
Bandwidth	The maximum request bit rate.
Reservation Class (optional)	A particular index that identifies a set of traffic characteristics of the flow (e.g. burstiness and packet size).
Transport Service Class (optional)	A particular index that Identifies the forwarding behaviour to be applied to the particular flow.
Bulk Reservation Description (Conditional)	The description of bulk reservations.
Direction of the requested bulk resources (Optional)	Direction of the requested bulk resources.
Physical Access ID (Optional)	The identifier of the physical access to which the user equipment is connected.
Logical Access ID (Optional)	The identifier of the logical access used by the attached user equipment. In the xDSL case, the Logical Access ID may explicitly contain the identifier of VP and/or VC carrying the traffic.
Physical Aggregation ID (Optional)	The identifier of the physical resource in the aggregation network to which the bulk reservation is processed.
Logical Aggregation ID (Optional)	The identifier of the logical resource in the aggregation network to which the bulk reservation is processed.
Bandwidth	The maximum requested data rate.
Reservation Class (optional)	A particular index that identifies a set of traffic characteristics of the requested resources (e.g. burstiness and packet size).
Transport Service Class (optional)	Identifies the forwarding behaviour to be applied to requested resources.
Commit Id	Identify if request is to be committed.
NOTE: Only the Bandwidth inside the Traffic Flow Parameter element can be modified.	

6.3.8.3.3   Resource Request/Modification Confirmation

The resource reservation confirmation message is used to acknowledge the resource reservation or modification. In case the request can not be fulfilled, the appropriate cause is returned to the originating x-RACF. In case of an unsuccessful modification, the terminating x-RACF also informs if the previous reservation was kept. The message contains the following elements:

Table 14: Resource Confirmation - Information Elements

Resource Mod/Req Cnf (Terminating x-RACF -> Originating x-RACF) (see note)	
Request Originating Function Identifier	Global unique Identifier for the Request Originating function instance.
Resource Reservation Session ID	The reference is a unique resource reservation session identifier in the scope of the Request Originating Function Identifier.
Duration of Reservation Granted (optional)	Duration of the reservation granted by TERMINATING x-RACF.
Overbooking confirmation indicator (optional)	Indicates that the terminating x-RACF may process the resource request in overbooking mode.
Result	The result of the request.
NOTE: The optional parameters are not present in case of an unsuccessful result.	

6.3.8.3.4   Resource Release Request

The resource reservation release message is used by the Originating x-RACF to relinquish the resource reservation in Terminating x-RACF. A parameter indicates if acknowledgement is expected by the Originating x-RACF from the Terminating x-RACF. The message contains the following elements:

Table 15: Resource Release - Information Elements

Resource Rel (Originating x-RACF-> Terminating x-RACF)	
Request Originating Function Identifier	Global unique Identifier for the Request Originating function instance.
Resource Reservation Session ID (see note)	The reference is a unique session identifier in the scope of the Request Originating Function Identifier (see note).
NOTE : The presence of a wildcard in the session part of the reference indicates that all resources identified associated to the Request Originating Function Identifier shall be released, otherwise only the specific session is released (it implies all media in the session).	

6.3.8.3.5   Abort Resource Reservation

The abort reservation message is used by the terminating x-RACF to indicate to the Originating x-RACF that the resource previously reserved is lost. The message may transport an indication for more than one reservation. The message contains the following elements:

Table 16: Abort Reservation- Information Elements

Abort Res (Terminating x-RACF -> Originating x-RACF) (see note)	
Request Originating Function Identifier	Global unique Identifier for the Request Originating function instance.
Resource Reservation Session ID	The reference is a unique Resource Reservation session identifier in the scope of the Request Originating Function Identifier (see note).
Time Stamp	The time when the resources were lost.
Cause	The cause that lead to the lost of the reservation.
NOTE: A single message shall be able to carry multiples blocks.	

6.3.8.3.6   Resource Allocation Request

The resource allocation request message is used to increase or decrease current resource allocation that is sent from one x-RACF (e.g. in a central location) to another x-RACF (e.g. in AN) or from x-RACF (e.g. in AN) to x-RACF (e.g. in a central location) for Offering model. The Resource Alloc message contains the following elements:

Table 17: Resource Allocation Request- Information Elements

Request Alloc (x-RACF <-> x-RACF) (see note 3)	
Request Originating Function Identifier	Global unique Identifier for the Request Originating function instance.
Resource Reservation Session ID	The reference is a unique resource reservation session identifier in the scope of the Request Originating Function Identifier.
Requestor Name *(Optional)*	Identifies the RACS client requesting the resources (e.g. name of a ASP or group of ASPs). This name corresponds to the Requestor Name in a QoS profile provided by NASS.
Service Class *(Optional)*	Service class requested by the RACS client.
Service Priority (optional)	The priority associated to a service request that defines the handling precedence by the receiving entity.
Subscriber-ID (conditional)	It identifies the subscriber attached to the access network (see note 1).
Globally Unique IP Address (conditional)	Globally Unique address that corresponds to the UNI associated to the subscriber attached to the network (see note 1).
Assigned IP Address	The IP address [Ipv4 or Ipv6].
Address Realm	The addressing domain in which the IP address is significant (see note 2).
Charging Correlation Information (CCI) (optional)	Globally unique identifier for charging correlation purposes.
Duration of Reservation (optional)	Duration of the reservation requested by the requestor.
Bulk Reservation Description (conditional)	The description of bulk reservations.
Direction of the requested bulk resources (Optional)	Direction of the requested bulk resources.
Physical Access ID (Optional)	The identifier of the physical access to which the user equipment is connected.
Logical Access ID (Optional)	The identifier of the logical access used by the attached user equipment. In the xDSL case, the Logical Access ID may explicitly contain the identifier of VP and/or VC carrying the traffic.
Physical Aggregation ID (Optional)	The identifier of the physical connection in the aggregation network to which the bulk resource is processed.
Logical Aggregation ID (Optional)	The identifier of the logical connection in the aggregation network to which the bulk resource is processed.
Bandwidth	The maximum requested data rate.
Reservation Class (optional)	A particular index that identifies a set of traffic characteristics of the request resources (e.g. burstiness and packet size).
Transport Service Class (optional)	Identifies the forwarding behaviour to be applied to particular request resources.
NOTE 1: At least one of these parameters (Subscriber-ID, Global Unique IP Address) shall be provided when the request is performed on a per subscription basis. NOTE 2: It makes the assigned IP address unique, for example it can be a VPN-id. NOTE 3: This message is mainly used for requesting the change of bulk resources when dedicated resources are allocated to difference services e.g. multicast.	

ETSI

6.3.8.3.7 Resource Allocation Confirmation

The resource allocation request message is used to confirm resource allocation for Offering model. The Resource Alloc conf message contains the following elements:

Table 18: Resource Allocation Conf- Information Elements

Resource Alloc Cnf (x-RACF <-> x-RACF) (see note 3)	
Request Originating Function Identifier	Global unique Identifier for the Request Originating function instance.
Resource Reservation Session ID	The reference is a unique Resource Reservation session identifier in the scope of the Request Originating Function Identifier (see note 1).
Duration of Reservation Granted (optional)	Duration of the reservation granted by the server.
Result	The result of the request.
NOTE 1: At least one of these parameters (Subscriber-ID, Global Unique IP Address) shall be provided when the request is performed on a per subscription basis.	
NOTE 2: It makes the assigned IP address unique, for example it can be a VPN-id.	
NOTE 3: The optional parameters are not present in case of an unsuccessful result.	

6.4 RACS Flows: Interaction Procedures

This clause describes the RACS interactions involved within the sub-procedure blocks for Authorize QoS Resources, Resource Reservation with Service-based Policy, Resource Modification, Resource Commit, Resource Release, Report Event and Abort Reservation indicated by the BGF and the A-RACF, Indication of Bearer Release, Resource Reservation Modification. These procedures are utilized to provide Service based Policy for session-based services and Border Gate Function (BGF).

> NOTE: In the following scenarios, the sequence used by SPDF to access the A-RACF and BGF is a local decision in the SPDF meaning that the SPDF is able to decide whether to access A-RACF and then BGF, or vice versa, or both in parallel (depending on the input from the AF). This is valid for request, modification and release flows.

6.4.1 Subscriber Attaches to the Access Network

The NASS is responsible for notifying the A-RACF when a subscriber attaches to the network. The NASS provides to A-RACF an association between Subscriber ID/IP address, the bearer used in the access network and additional subscriber access information.

Figure 6 presents the associated procedure:
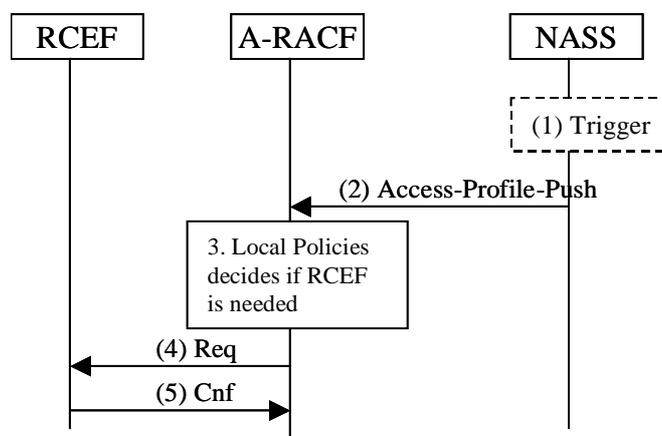
Figure 6: Subscriber attaches to the access network

1) The NASS accepts a request from a user equipment device to obtain bearer resources to attach to the access network or a modification on a subscriber's access profile that has been previously "pushed" to the RACS by NASS occurs.

2) The NASS sends Access-Profile-Push to inform A-RACF. When multiple A-RACF instances are present in the form of hierarchical structure, the NASS interacts with the top tier A-RACF instance as the single point of contact for Access-Profile-Push.

3) Based on Local Policies in the A-RACF and the information received from the NASS, the A-RACF decides if any traffic policy need to be installed, changed or removed. The application of the new local policies will apply to new SPDF requests whereas the current reservations are optionally handled according to previous local policies.

4) The A-RACF requests the RCEF to install traffic policies (depending on step 3). When multiple A-RACF instances are present in the form of hierarchical structure, the A-RACF may interact with co-located RCEF to install traffic policies.

5) The RCEF confirms the installation of the traffic policies (depending on step 4).

6.4.2   Request Resource

6.4.2.1   Request Resource by using the push mode

This clause provides the flows for resource reservation request from the AF towards the SPDF. Based on SPDF policies, the SPDF decides to contact the A_RACF, BGF or both.
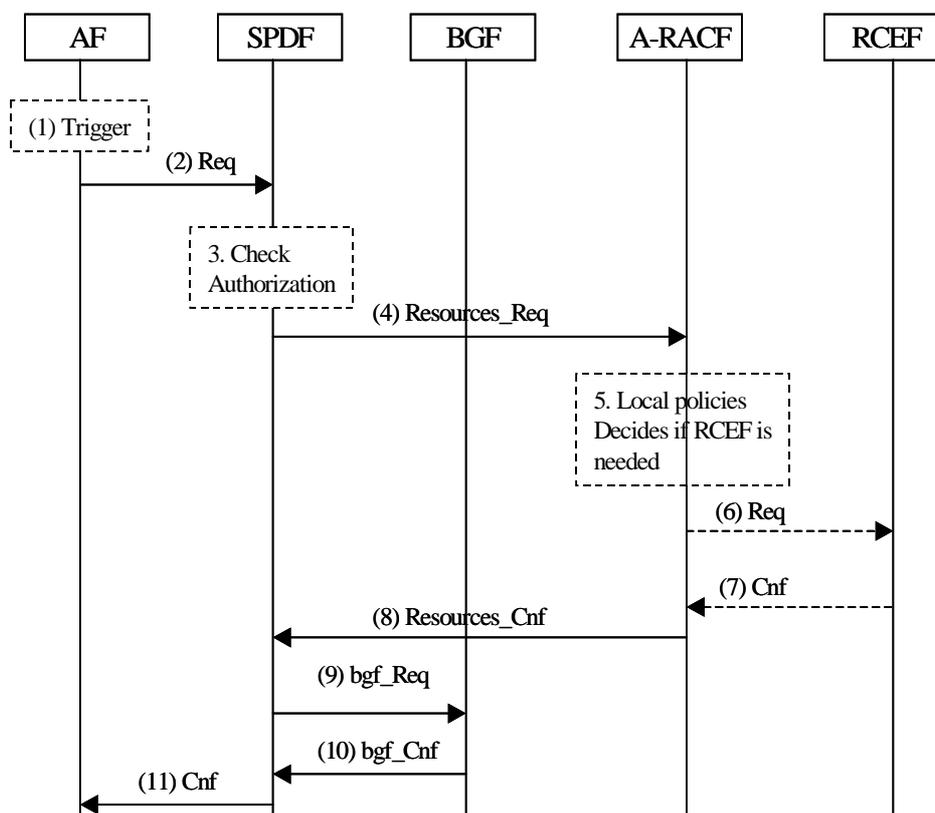
Figure 7: Request resource (Push Mode)

1) An AF session initiation message is received from UE, generated in AF itself, or another AF. The AF identifies that this session requires resources in the transport network in order to support the associated media flows.

2) The AF sends a unicast or multicast service request information to the SPDF.

3) The SPDF authorizes the request. This process consists of verifying if the required resources for the AF session, present in the service request, are consistent with operator policy rules defined in the SPDF for that particular AF.

4)   In case the service is authorized, the SPDF determines how to serve the request. It may be required to send Resources-Req to allocated resources of the A-RACF and/or bgf-Req request to BGF. When multiple A-RACF instances are present in the form of hierarchical structure, the SPDF contacts the top tier A-RACF instance as the single point of contact for resource admission control. The SPDF uses the local policies and the parameters in the request in order to take the decision. Therefore, steps 5) to 8) and/or 9) and 10) may not be performed depending on the SPDF decision.

5)   The A-RACF maps the request from SPDF into the internal network topology. The A-RACF performs authorization and admission control based on access network policies. The A-RACF also decides if there are traffic policies to be installed in the RCEF. When multiple A-RACF instances are present in the form of hierarchical structure, the top tier A-RACF instance forwards the request to other A-RACF instances in case those instances are in control of resources referenced in the request (i.e. the top tier A-RACF has delegated resources to other A-RACF instances). In this case the top tier A-RACF makes the final admission decision based on the results of resource admission from all other instances.

6)   The A-RACF evaluates the availability and, if successful, reserves resources and requests the RCEF to install the traffic policies to be applied to the associated flows (depending on step 5). When multiple A-RACF instances are present in the form of hierarchical structure, the A-RACF may interact with co-located RCEF to install traffic policies.

7)   The RCEF confirms the installation of the traffic policies (depending on step 6). For multicast services, traffic policies authorize the delivery of the multicast flow(s). Multicast replication follows as needed.

8)   The A-RACF sends Resource-Cnf to inform the SPDF if the resources are reserved.

9)   The SPDF has determined that serving this request requires sending a request to the appropriate BGF and therefore the SPDF sends a bgf_Req to the BGF.

10)   The BGF performs the requested service (e.g. allocates the necessary resources to insert a RTP relay function) and confirms the operation to the SPDF.

11)   The SPDF forwards the result to the AF.

NOTE: The multicast replication process is handled by the transport processing functions. RACS only indicates in the traffic policy whether the requested flow by a user is authorized. If the requested flow is authorized, the transport processing functions will replicate it when required.

6.4.2.2   Request Resource by using the pull mode

The flow diagram for this procedure is not standardized in the present document.

6.4.2.2.1   Admission control using pull mode when only one x-RACF is involved in managing the same resources

The procedure described in this clause is used for performing admission control using pull mode (e.g. the admission control is triggered from the network).

This procedure is applicable when only one x-RACF is exclusively involved in managing given resources.

BTF　　　　　RCEF　　　　x-RACF

(1) Trigger

(2a) Request (optional)

(2b) Request

(3) Request

(4) Adm Ctrl

(5) Policy

(6) Response

(7) Request (optional)

(8) Trigger Response
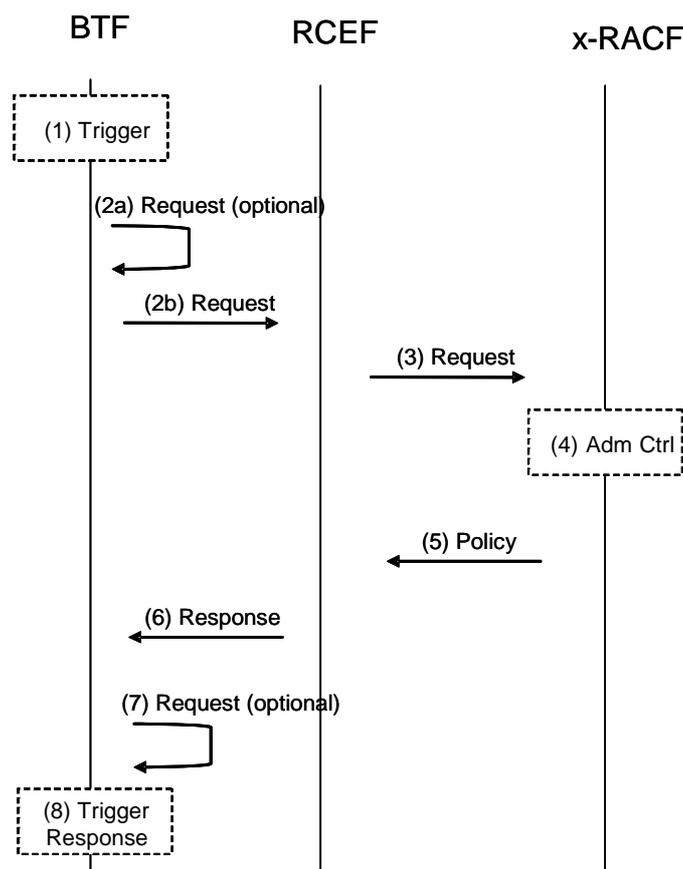
Figure 8: Admission control using pull mode
when only one x-RACF is involved in managing the same resources

1) The BTF receives a trigger for requesting access to resources. This trigger may come, for example, from a CND or from another BTF.

2a) Optionally the BTF forwards the request to another BTF. This usually happens when the BTF is not co-located with an RCEF capable of interacting with an x-RACF.

2b) The BTF forwards the request to the RCEF.

3) The RCEF builds a reservation request and sends it to the x-RACF.

4) The x-RACF performs the admission control; this applies to the network segment and the associated resources which it has responsibility for (e.g. for a x-RACF instance deployed in the AN, the admission control may only be for the access segment while for another x-RACF instance deployed on a platform separate form any traffic forwarding device may perform the admission control for both the access and aggregation segments).

5) The x-RACF enforces the appropriate policy in the RCEF.

6) The RCEF sends to the BTF the response to its request.

7) Optionally the BTF forwards the request to another BTF. This allows for further admission control processes applying other network segments (e.g. after performing admission control in the access segment, admission control in the aggregation segment may be needed as well).

8) Depending on the type of trigger received in the first place by the BTF, the BTF may optionally send a response to that trigger.

NOTE 1: The standardization of steps 2a, 2b, 6 and 7 is outside the scope of the present document.

NOTE 2: Steps 3 and 5 are to be considered as Re interactions when RCEF and x-RACF are located in different nodes. If RCEF and x-RACF are co-located, the standardization of these interaction is outside of the scope of the present document.

6.4.2.2.2   Admission control using pull mode when multiple x-RACFs are involved in managing the same resources

The procedure described in this clause is used for performing admission control in pull mode (e.g. the admission control is triggered from the network).

This procedure is applicable when multiple x-RACFs are involved in managing the same resources.
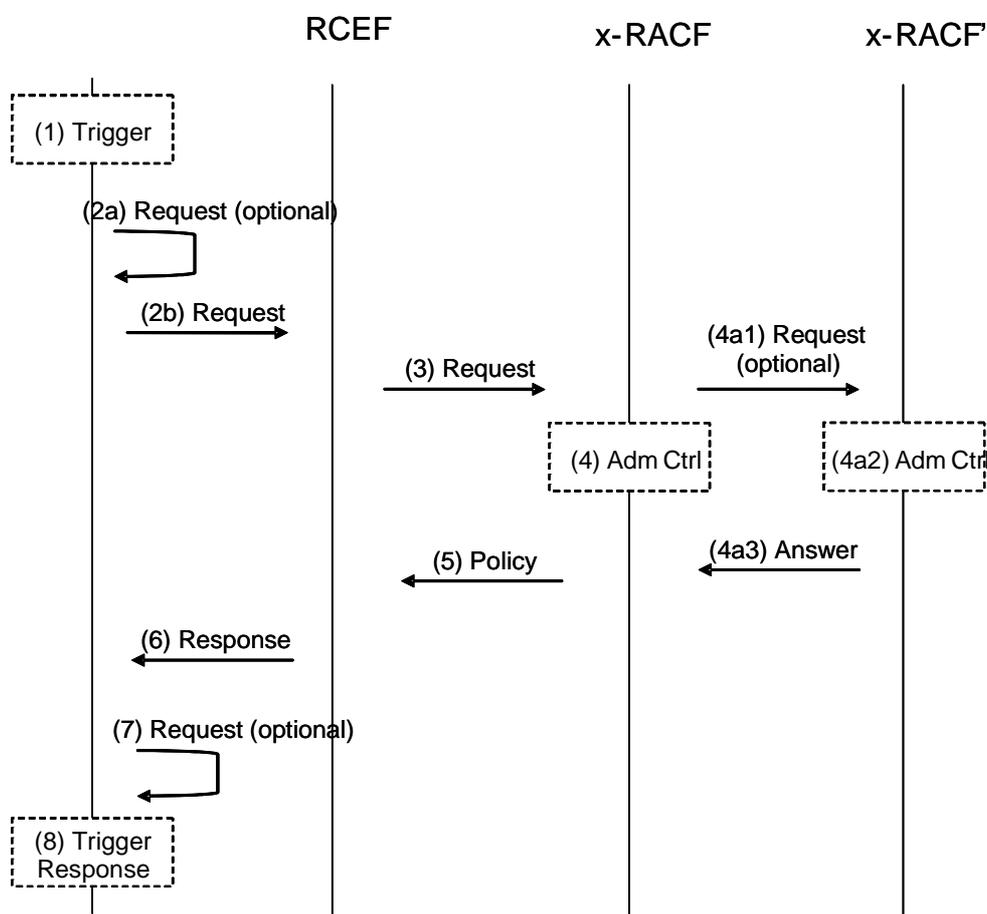
**Figure 9: Admission control using pull mode
when multiple x-RACFs are involved in managing the same resources**

1)   The BTF receives a trigger for requesting resources. This trigger may come, for example, from a CND or from another BTF.

2a)   Optionally the BTF forwards the request to another BTF. This usually happens when the BTF is not co-located with an RCEF capable of interacting with an x-RACF.

2b)   The BTF forwards the request to the RCEF.

3)   The RCEF builds a reservation request and sends it to the x-RACF.

4)   The x-RACF performs the admission control; this applies to the network segment and the associated resources which it has responsibility for (e.g. for a x-RACF instance deployed in the AN, the admission control may only be for the access segment while for another x-RACF instance deployed on a platform separate form any traffic forwarding device may perform the admission control for both the access and aggregation segments).

4a)   The x-RACF may interact with another x-RACF' (prime). The interaction (4a1) then triggers an admission control decision in x-RACF' (4a2) followed by an answer to the interaction request (4a3). This step may be decoupled from reservation requests arriving to the first x-RACF from the RCEF.

5)   The x-RACF enforces the appropriate policy in the RCEF.

6)   The RCEF sends to the BTF the response to its request.

7) Optionally the BTF forwards the request to another BTF. This allows for further admission control processes applying other network segments (e.g. after performing admission control in the access segment, admission control in the aggregation segment may be needed as well).

8) Depending on the type of trigger received in the first place by the BTF, the BTF may optionally send a response to that trigger.

NOTE 1: The standardization of steps 2a, 2b, 6 and 7 is outside the scope of the present document.

NOTE 2: Steps 3 and 5 are to be considered as Re interactions when RCEF and x-RACF are located in different nodes. If RCEF and x-RACF are co-located, the standardization of these interaction is outside of the scope of the present document.

6.4.3 Request Resource Wholesale/Retail Scenario

6.4.3.1 Request Resource with access to the A-RACF in the retail domain

This clause provides the flows for resource reservation request for wholesale/nomadism scenario. In this network deployment option, the NCP performs its own Admission Control decisions related to the access user profile and the available resources on the access network segment (ES 282 001 [2]). The NANP performs Admission Control decisions based on the NCP's profile and available resources over the aggregation network segment.

Based on SPDF(R) policies, the SPDF(R) wants to establish contact with the BGF(R), the A-RACF(R) and contacts the SPDF(W) in the wholesale NANP. Based on SPDF(W) policies, the SPDF(W) decides to contact the A-RACF(W) in the wholesale network, replies to the SPDF(R) which then establishes contact with the BGF(R).

Figure 10: Request Resource wholesale/nomadism with access to A-RACF in the retail domain

1) An AF session initiation message is received or generated in AF. The AF identifies that this session requires resources in the transport network in order to support the associated media flows.

2) The AF sends a service request to the SPDF(R).

3) The SPDF(R) authorizes the request. This process consists of verifying if the required resources for the AF session, present in the service request, are consistent with operator policy rules defined in the SPDF(R) for that particular AF. It may be required to send resource request to allocated resources of the A-RACF(R). The SPDF(R) uses the local policies and the parameters in the request in order to take the decision. Therefore, steps 12) to 13) may not be performed depending on the SPDF(R) decision.

4) As the SPDF(R) does not own the resources in the transport network, the service request is sent further to the SPDF(W).

5) The SPDF(W) authorizes the request. This process consists of verifying if the required resources for the SPDF(R) session, present in the service request, are consistent with operator policy rules defined in the SPDF(W) for that particular SPDF(R).

6) In case the service is authorized, the SPDF(W) determines how to serve the request. It may be required to send resource request to allocated resources of the A-RACF(W). The SPDF(W) uses the local policies and the parameters in the request in order to take the decision. Therefore, steps 7) to 10) may not be performed depending on the SPDF(W) decision. When multiple A-RACF instances are present in the form of hierarchical structure, the SPDF contacts the top tier A-RACF(W) instance being the single point of contact for policy and resource admission control.

7) The A-RACF(W) maps the request from SPDF(W) into the internal network topology. The A-RACF(W) performs authorization and admission control based on access network policies. The A-RACF(W) also decides if there are traffic policies to be installed in the RCEF. When multiple A-RACF instances are present in the form of hierarchical structure, the top tier A-RACF(W) instance forwards the request to other instances in case those instances are in control of resources referenced in the request (i.e. the top tier A-RACF(W) has delegated resources to other A-RACF instances). In this case the top tier A-RACF(W) makes the final admission decision based on the results of resource admission from all instances.

8) The A-RACF(W) requests the RCEF to install the traffic policies to be applied to the associated flows (depending on step 7). When multiple A-RACF instances are present in the form of hierarchical structure, the A-RACF(W) may interact with co-located RCEF to install traffic policies.

9) The RCEF confirms the installation of the traffic policies (depending on step 8).

10) The A-RACF(W) sends resource confirmation to inform the SPDF(W) if the resources are reserved.

11) The SPDF(W) sends the result of the resource reservation to the SPDF(R).

12) The SPDF(R) sends resources request to allocated resources of the A-RACF(R). When multiple A-RACF instances are present in the form of hierarchical structure, the top tier A-RACF(R) instance forwards the request to other instances in case those instances are in control of resources referenced in the request (i.e. the top tier A-RACF(R) has delegated resources to other A-RACF instances). In this case the top tier A-RACF(R) makes the final admission decision based on the results of resource admission from all instances.

13) The A-RACF(R) confirms the operation to the SPDF(R).

14) The SPDF(R) determines that whether this service request requires sending a request to the appropriate BGF(R). Therefore, steps 14) and 15) may not be performed depending on the SPDF(R) decision.

15) The BGF(R) performs the requested service (e.g. allocates the necessary resources to insert a RTP relay function) and confirms the operation to the SPDF.

16) The SPDF(R) forwards the result to the AF.

6.4.3.2   Request Resource without access to the A-RACF in the retail domain

This clause provides the flows for resource reservation request from the AF towards the SPDF(R) in the retail network when there is no NAT in the NANP network. Based on SPDF(R) policies, the SPDF(R) wants to establish contact with the BGF, and contacts the SPDF(W) in the wholesale NANP. Based on SPDF(W) policies, the SPDF(W) decides to contact the A-RACF in the wholesale network, replies to the SPDF(R) which then establishes contact with the BGF(R).
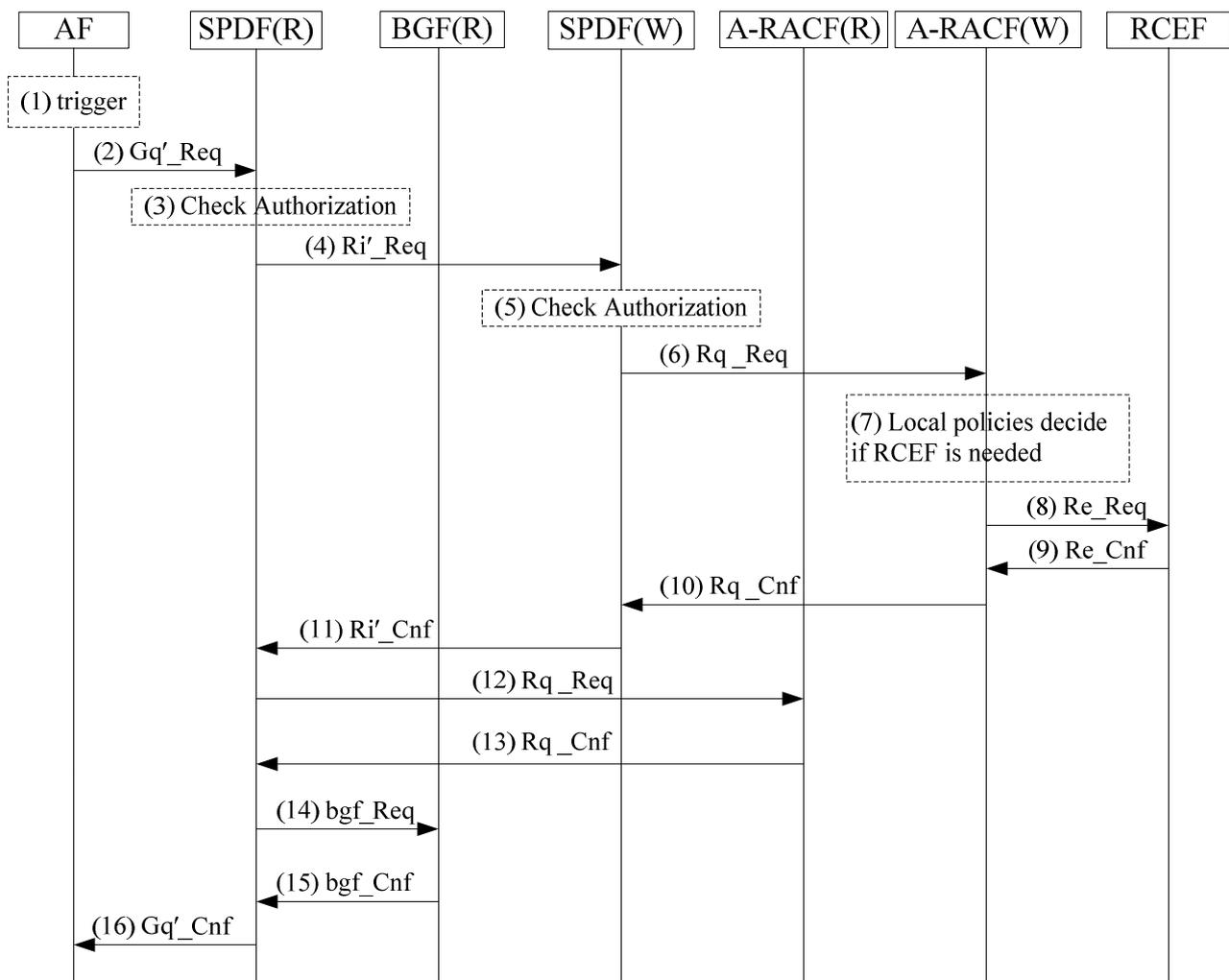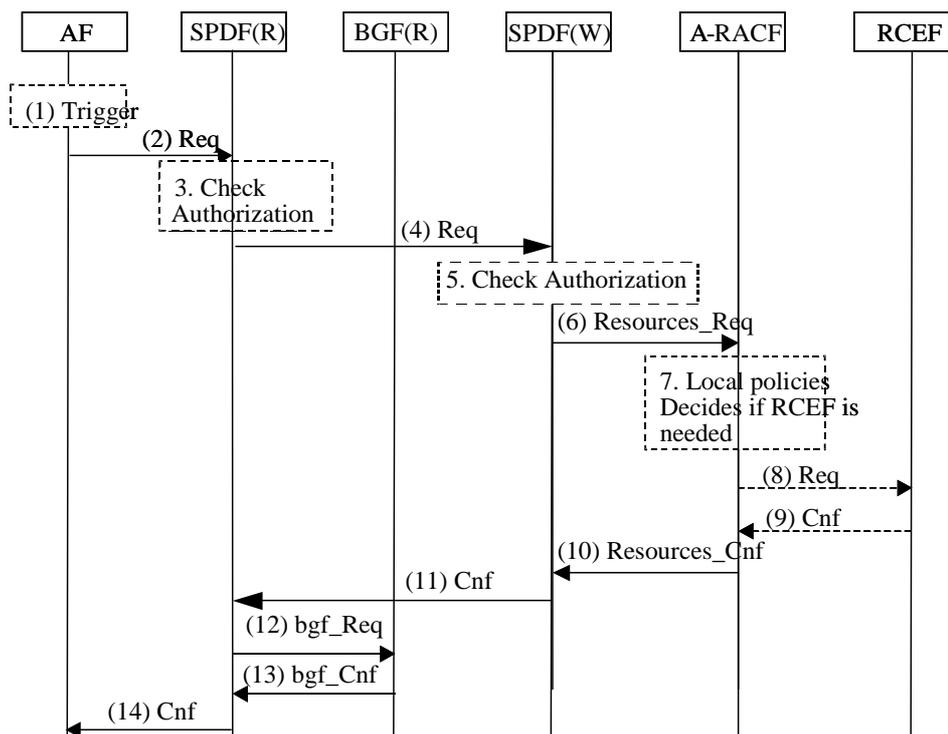
Figure 11: Request resource wholesale without access to A-RACF in the retail domain
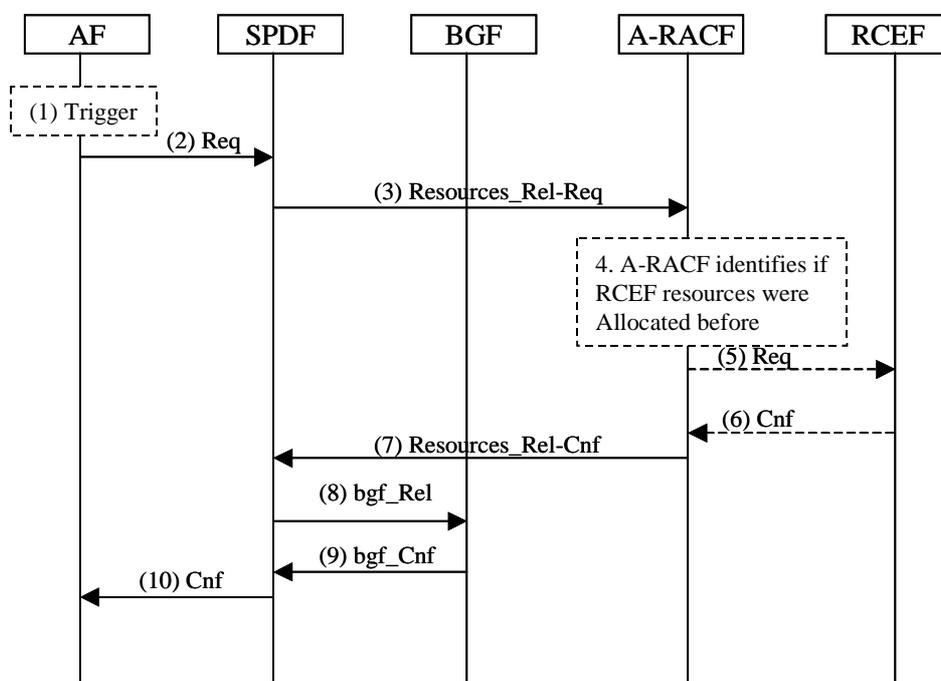
1)   An AF session initiation message is received or generated in AF. The AF identifies that this session requires resources in the transport network in order to support the associated media flows.

2)   The AF sends a service request to the SPDF(R).

3)   The SPDF(R) authorizes the request. This process consists of verifying if the required resources for the AF session, present in the service request, are consistent with operator policy rules defined in the SPDF(R) for that particular AF.

4)   As the SPDF(R) does not own the resources in the transport network, the service request is sent further to the SPDF(W).

5)   The SPDF(W) authorizes the request. This process consists of verifying if the required resources for the SPDF(R) session, present in the service request, are consistent with operator policy rules defined in the SPDF(R) for that particular SPDF(R).

6)   In case the service is authorized, the SPDF(W) determines how to serve the request. It may be required to send Resources-Req to allocated resources of the A-RACF. The SPDF(W) uses the local policies and the parameters in the request in order to take the decision. Therefore, steps 7) to 10) may not be performed depending on the SPDF(W) decision. When multiple A-RACF instances are present in the form of hierarchical structure, the SPDF contacts the top tier A-RACF instance being the single point of contact for policy and resource admission control.

7)   The A-RACF maps the request from SPDF(W) into the internal network topology. The A-RACF performs authorization and admission control based on access network policies. The A-RACF also decides if there are traffic policies to be installed in the RCEF. When multiple A-RACF instances are present in the form of hierarchical structure, the top tier A-RACF instance forwards the request to other instances in case those instances are in control of resources referenced in the request (i.e. the top tier A-RACF has delegated resources to other A-RACF instances). In this case the top tier A-RACF makes the final admission decision based on the results of resource admission from all instances.

8)   The A-RACF requests the RCEF to install the traffic policies to be applied to the associated flows (depending on step 7). When multiple A-RACF instances are present in the form of hierarchical structure, the A-RACF may interact with co-located RCEF to install traffic policies.

9)   The RCEF confirms the installation of the traffic policies (depending on step 8).

10)   The A-RACF sends Resource-Cnf to inform the SPDF(W) if the resources are reserved.

11)   The SPDF(W) sends the result of the resource reservation to the SPDF(R).

12)   The SPDF(R) determines that whether this service request requires sending a request to the appropriate BGF. Therefore, steps 12) and 13) may not be performed depending on the SPDF(R) decision.

13)   The BGF performs the requested service (e.g. allocates the necessary resources to insert a RTP relay function) and confirms the operation to the SPDF.

14)   The SPDF forwards the result to the AF.

6.4.4   Release Resource

6.4.4.1   Release Resource Request by using the push mode

This clause provides the flows for resource release in A-RACF as well as a service termination in the Border Gateway Function (BGF).

Figure 12: Release resource by using the push mode

1)   An AF session release message is received or generated in AF. The AF identifies that the associated resources shall be released.

2)   The AF sends a request to the SPDF to relinquish the resources previously allocated.

3)   The SPDF determines that serving this request requires sending a Resources-Rel to A-RACF and/or to request the termination of the BGF service (s). Steps 4) to 7) and/or 8) to 9) may not be performed. When multiple A-RACF instances are present in the form of hierarchical structure, the SPDF contacts the top tier A-RACF instance for resource release operations.

4)   The A-RACF releases all associated resources. The A_RACF checks if there are traffic policies to be removed from the RCEF. When multiple A-RACF instances are present in the form of hierarchical structure and are involved in reserving resources for the original reservation request from the AF, the top tier A-RACF instance forwards the request to other A-RACF instances to request the resource release.

5)   The A-RACF requests the RCEF to remove the associated traffic policies (depending on 4). When multiple A-RACF instances are present in the form of hierarchical structure, the A-RACF may interact with co-located RCEF to remove the associated traffic policies.

6)   The RCEF confirms the removal of the traffic policies (depending on 5).

7)   The A-RACF informs the SPDF that the resources were relinquished.

8)   The SPDF determines that a release request is to be sent to the appropriate BGF.

9)   The BGF terminates the service (s) and confirms the operation to the SPDF.

10)   The SPDF forwards the result to the AF.

6.4.4.2   Release Resource Request by using the pull mode

6.4.4.2.1   Resource Release using pull mode when only one x-RACF is involved in managing the same resources

The procedure described in this clause is used for release the resource after performing admission control using pull mode (e.g. the admission control is triggered from the network).

This procedure is applicable when only one x-RACF is exclusively involved in managing given resources.
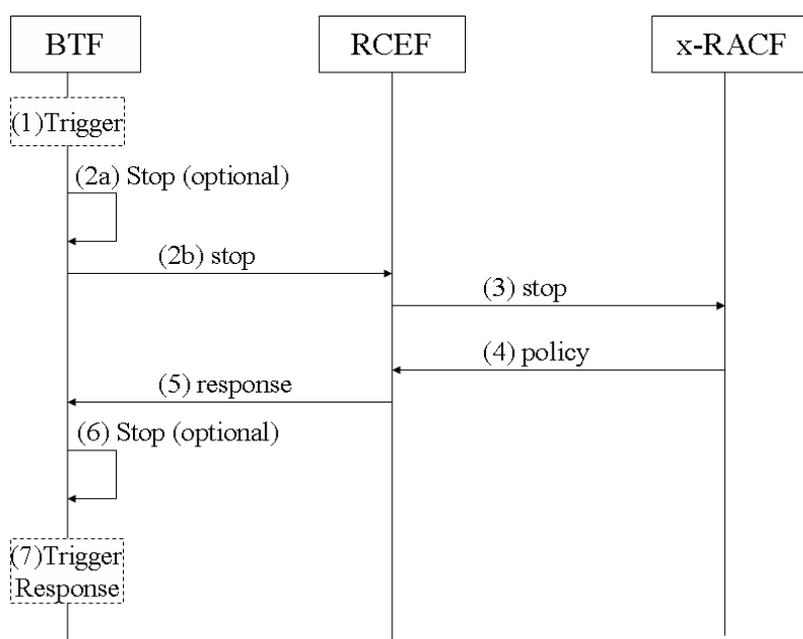
Figure 13: Resource Release using pull mode
when only one x-RACF is involved in managing the same resources

1)   The BTF receives or generates a trigger for stopping access to resources. This trigger may come, for example, from a CND or from another BTF.

2a)   Optionally the BTF forwards the request to another BTF. This usually happens when the BTF is not co-located with an RCEF capable of interacting with an x-RACF.

2b)   The BTF forwards the request to the RCEF.

3)   The RCEF builds a multicast stop request and sends it to the x-RACF. The x-RACF performs the resource reclaim; this applies to the network segment and the associated resources which it has responsibility for (e.g. for a x-RACF instance deployed in the AN, the resource reclaim may only be for the access segment while for another x-RACF instance deployed on a platform separate form any traffic forwarding device may perform the resource reclaim for both the access and aggregation segments).

4)   The x-RACF enforces the appropriate policy in the RCEF.

5) The RCEF sends to the BTF the response to its request.

6) BTF stops multicast replication. Optionally the BTF forwards the stop request to another BTF. This allows for further resource reclaim processes applying other network segments (e.g. after performing resource reclaim in the access segment, resource reclaim in the aggregation segment may be needed as well).

7) Depending on the type of trigger received in the first place by the BTF, the BTF may optionally send a response to that trigger.

NOTE 1: The standardization of steps 2a, 2b, 6 and 7 is outside the scope of the present document.

NOTE 2: Steps 3 and 4 are to be considered as Re interactions when RCEF and x-RACF are located in different nodes. If RCEF and x-RACF are co-located, the standardization of these interactions is outside of the scope of the present document.

6.4.4.2.2 Resource release using pull mode when multiple x-RACFs are involved in managing the same resources

The procedure described in this clause is used for release after performing admission control in pull mode (e.g. the admission control is triggered from the network).

This procedure is applicable when multiple x-RACFs are involved in managing the same resources.
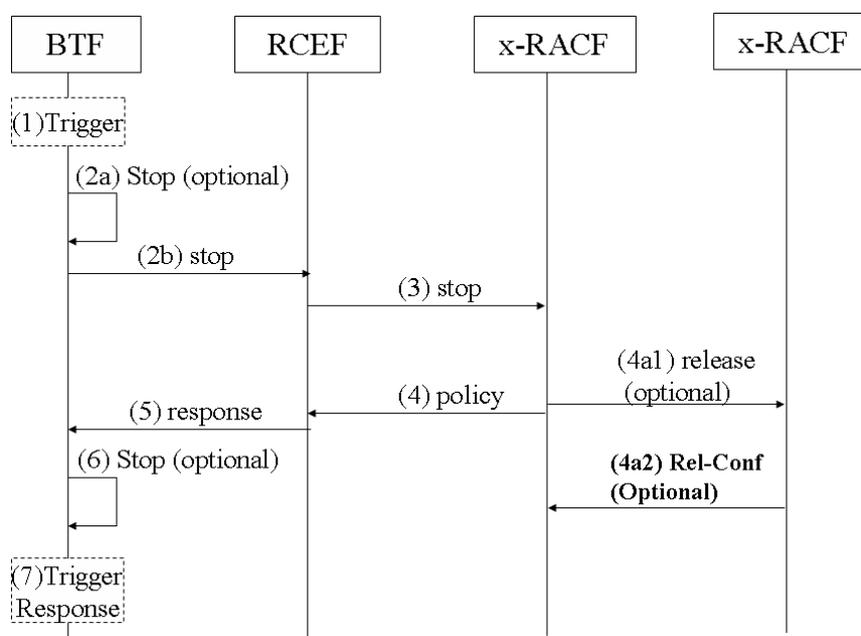
**Figure 14: Resource Release using pull mode
when multiple x-RACFs are involved in managing the same resources**

1) The BTF receives or generates a trigger for stopping multicast. This trigger may come, for example, from a CND or from another BTF.

2a) Optionally the BTF forwards the request to another BTF. This usually happens when the BTF is not co-located with an RCEF capable of interacting with an x-RACF.

2b) The BTF forwards the request to the RCEF.

3) The RCEF builds a stop request and sends it to the x-RACF. The x-RACF reclaims the resource; this applies to the network segment and the associated resources which it has responsibility for (e.g. for a x-RACF instance deployed in the AN, the resource reclaim may only be for the access segment while for another x-RACF instance deployed on a platform separate form any traffic forwarding device may perform the resource reclaim for both the access and aggregation segments).

4a) The x-RACF may interact with another x-RACF' (prime). Based on the release policies (the policies may be timeout triggered, or release at once, some portion of the resource) saved in the x-RACF, when the policy matched, with the interaction (4a1) release the additional resource allocated by X-RACF', then triggers an resource reclaim in x-RACF' followed by an answer to the interaction request (4a2). 4a1 can be carried at any time due to the release policies. And how much resource released for some time or once is based on the release policy.

5) The x-RACF enforces the appropriate policy in the RCEF.

6) The RCEF sends to the BTF the response to its request.

7) BTF stops multicast replication. Optionally the BTF forwards the stop request to another BTF. This allows for further resource reclaim processes applying other network segments (e.g. after performing resource reclaim in the access segment, resource reclaim in the aggregation segment may be needed as well).

8) Depending on the type of trigger received in the first place by the BTF, the BTF may optionally send a response to that trigger.

NOTE 1: The standardization of steps 2a, 2b, 6 and 7 is outside the scope of the present document.

NOTE 2: Steps 3 and 5 are to be considered as Re interactions when RCEF and x-RACF are located in different nodes. If RCEF and x-RACF are co-located, the standardization of these interactions is outside of the scope of the present document.

6.4.5 Commit Resources procedure

This procedure is triggered by an AF session signalling message received at the AF, or an internal action at the AF. The "Commit Resources" procedure is optional and is only needed if the AF had previously ordered the SPDF to reserve resources without a commit.

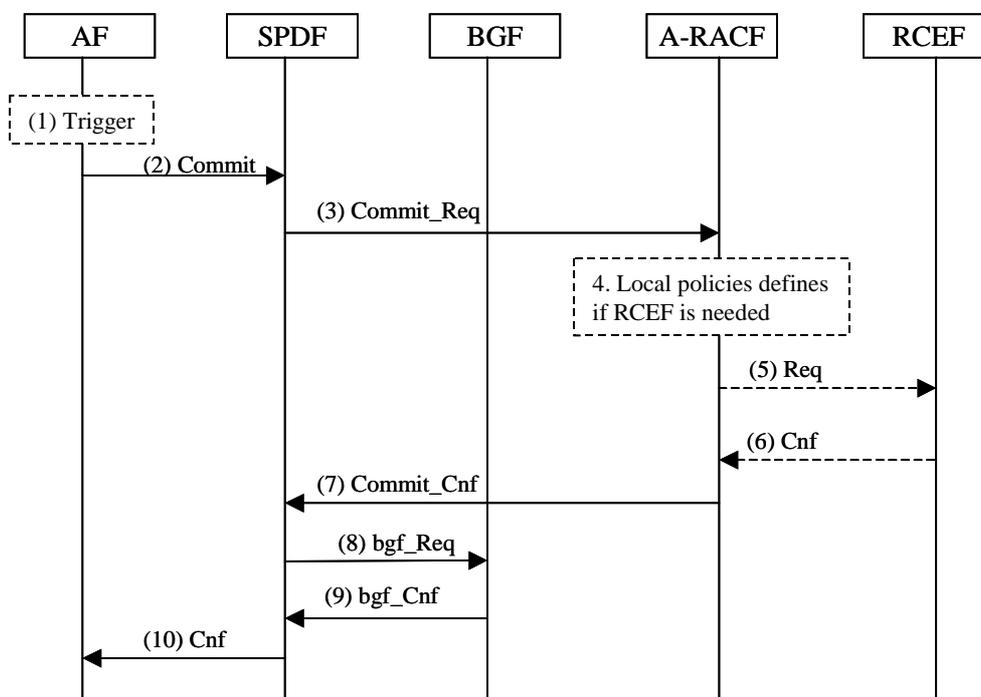The decision where the commit is ultimately performed is based on the SPDF policies.

Figure 15: Commitment of resources

1) An AF session signalling message is received at the AF, or an internal action at the AF triggers the need to enable the transport of the media flow in the access network associated with the application.

2) The Application Function (AF) sends a Commit request to the SPDF.

3) The SPDF sends a Commit-Req message to the A-RACF and/or to the BGF to open the "gate". The decision is based on local policies. Whether steps 4) to 7) and 8) and 9) are executed is dependent on this decision. When multiple A-RACF instances are present in the form of hierarchical structure, the SPDF contacts the top tier A-RACF instance for resource commitment operations.

4) The A-RACF receives the Commit-Req message. One possible decision of A-RACF is to explicitly open the "gate" in the transport network. This corresponds to the installation of a particular traffic policy in the RCEF. When multiple A-RACF instances are present in the form of hierarchical structure, the top tier A-RACF instance forwards the request to other A-RACF instances to request the resource commitment in case those instances are in control of resources referenced in the request (i.e. the top tier A-RACF has delegated resources to other A-RACF instances).

5) The A-RACF sends a request to install the traffic policies in the RCEF (depending on 4). When multiple A-RACF instances are present in the form of hierarchical structure, the A-RACF may interact with co-located RCEF to install traffic policies.

6) The RCEF reports to the A-RACF the installation of the traffic policies (depending on 5).

7) The A-RACF reports to the SPDF that the Commit-Req was successfully performed.

8) The SPDF may also (or alternatively) need to perform gate control at the BGF. In such a case the BGF sends a bgf_Req to the BGF.

9) The BGF reports to the SPDF that the action was performed.

10) The SPDF reports to the AF that the Commit was performed.

6.4.6 Resource Modification Request

6.4.6.1 Resource Modification Request by using the push mode

This procedure is used when the AF session signalling decides to modify the AF session by using the push mode. An update of a previous reservation is requested from the SPDF.

The following figure is applicable to both access sides of a session establishment.
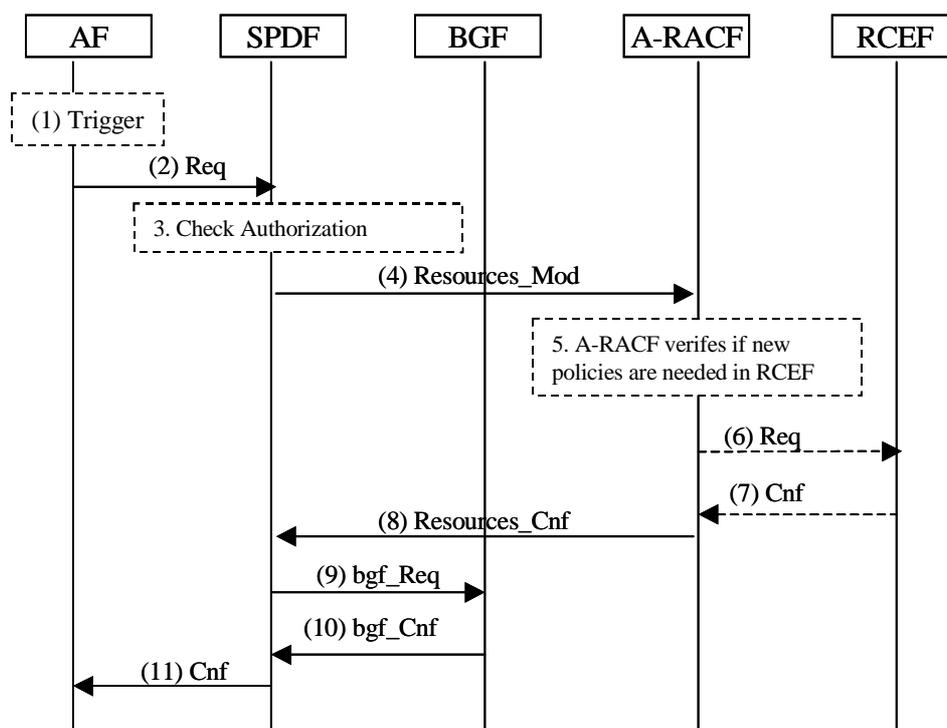
Figure 16: Resource Modification Request by using the push mode

1)   An AF session modification results in the need to change the existing resource reservation.

2)   The AF sends the service request information to the SPDF.

3)   The SPDF shall authorize the request with the modified parameters. This authorization consists of verifying if the modified QoS resources for the AF session, present in the session description, are consistent with the operator policy rules defined in the SPDF. The SPDF determines if serving this request requires sending a Resources-Req to A-RACF and/or bgf-Req request for BGF service(s). Whether steps 4) to 8) and/or 9) and 10) are executed is dependent on this decision.

4)   The SPDF has determined that serving this request requires sending a Resources-Mod message to the A-RACF. When multiple A-RACF instances are present in the form of hierarchical structure, the SPDF contacts the top tier A-RACF instance for resource modification operations.

5)   The A-RACF performs admission control based on access network policies with the new QoS parameters. When multiple A-RACF instances are present in the form of hierarchical structure and are involved in reserving resources for the original reservation request from the AF, the top tier A-RACF instance forwards the request to other instances to request the resource modification.

6)   The A-RACF may request the RCEF to modify the installed traffic policies that are applied to the associated resource reservation session flows. When multiple A-RACF instances are present in the form of hierarchical structure, the A-RACF(W) may interact with co-located RCEF to install traffic policies.

7)   The RCEF confirms the modification of the traffic policies (depending on 6).

8)   The A-RACF informs the SPDF that the resources requested are reserved.

9)   The SPDF checks if there are also service (s) to be modified in BGF. If yes, a bgf-req is sent to the BGF.

10)   The BGF modifies the service (s) and confirms the operation to the SPDF.

11)   The SPDF sends the confirmation to the AF.

6.4.6.2 Resource Modification Request by using the pull mode

This procedure is used when the AF session signalling decides to modify the AF session by using the pull mode. An update of a previous reservation is requested from the SPDF.

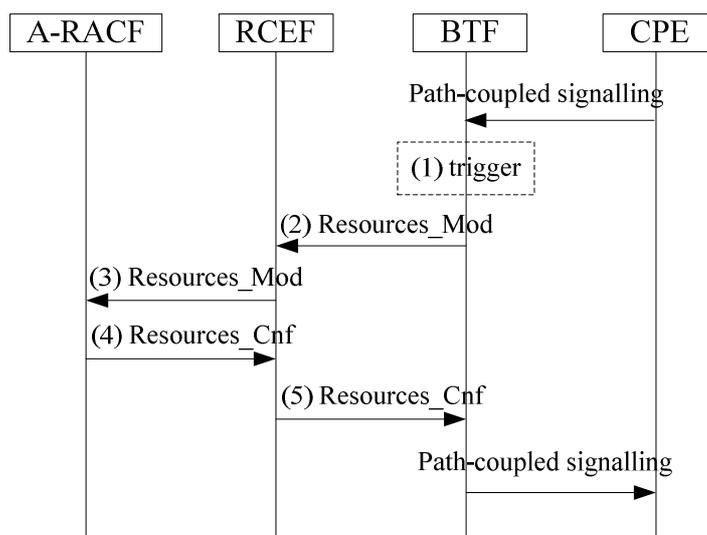The following figure is applicable to both access sides of a session establishment.

Figure 17: Resources Modification Request by using the pull mode

1)   The resource modification request is usually triggered by a request indicated through the signalling from the CPN to modify the authorized resource for the given flow.

2)   The BTF transfers the resource modification request to the RCEF.

3)   The RCEF forwards the request to the A-RACF.

4)   The A-RACF checks the authorization and admission control based on access network policies with the new QoS parameters. The A-RACF may request the RCEF to modify the installed traffic policies. The A-RACF sends the response information to the RCEF.

5)   The RCEF sends the response to the BTF.

6.4.7   RACS Retrieves Access Profile from NASS

When A-RACF processes a resource reservation request received from the SPDF, the user's access profile may not be available.

Depending on Local Policies, the A-RACF may "pull" the Access-Profile from the NASS. This procedure is also applicable to the A-RACF recovery via data synchronization with NASS.

Figure 18 presents the associated procedure:
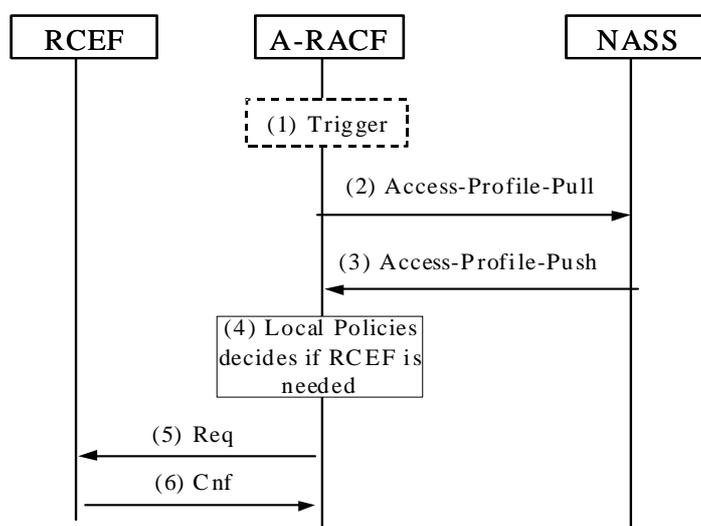
Figure 18: Access Profile Retrieval

1)   This trigger represents the situations where the A-RACF needs the subscriber's access profile and this information is not locally available.

2)   The A-RACF sends Access-Profile-Pull message to the NASS for retrieving Access Profile Information. When multiple A-RACF instances are present in the form of hierarchical structure, the top tier A-RACF instance sends Access-Profile-Pull message to the NASS.

3)   The NASS sends the subscriber associated access profile to the A-RACF using Access-Profile-Push message.

4)   Based on the local policies of A-RACF and the information received from the NASS, the A-RACF decides if any traffic policy needs to be installed in the RCEF.

5)   The A-RACF requests the RCEF to install the appropriate traffic policies to be applied (depending on step 4). When multiple A-RACF instances are present in the form of hierarchical structure, the A-RACF may interact with co-located RCEF to install traffic policies.

6)   The RCEF confirms the installation of the traffic policies.

6.4.8   Subscriber Detaches from the access network

This procedure presents the flows for the case where the NASS notifies the A-RACF that a certain binding is no longer valid.

NOTE: A similar flow can also represent an internal event in the A-RACF, for example a management decision. In this case the message from the NASS to the A-RACF is not present.

The A-RACF sends a notification towards the AF that the resource reservation is revoked and all associated resources are released.
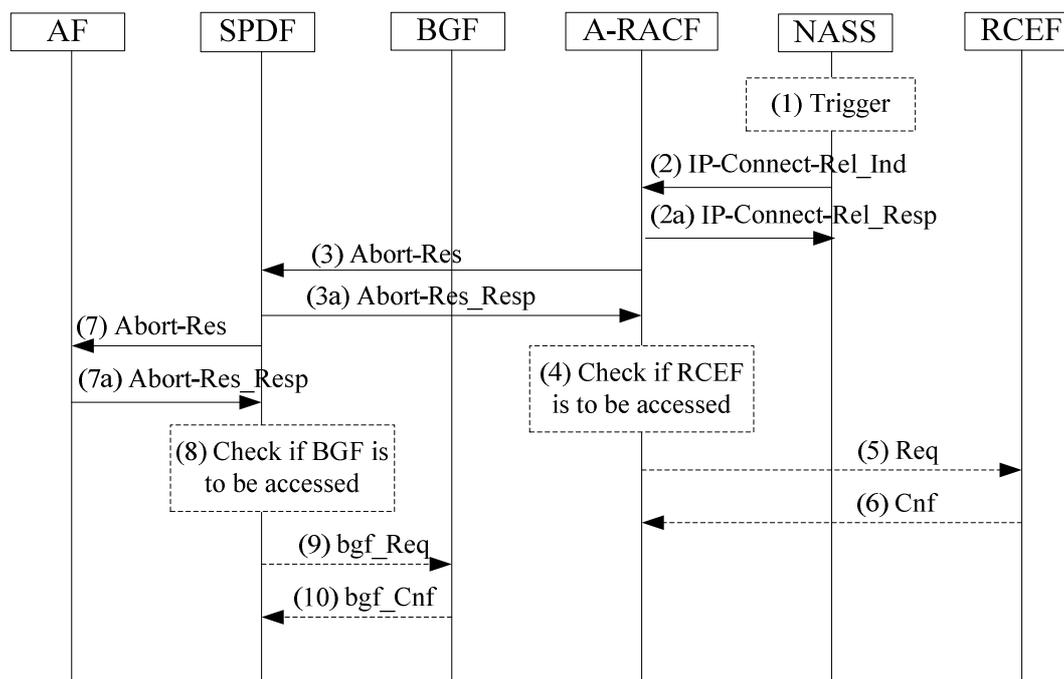
Figure 19: Subscriber detachment

1) The NASS decides that a bearer path is to be released (e.g. the end user equipment sends a release request for the bearer path to NASS).

2) The NASS informs the A-RACF that the access information is no longer valid by sending an IP-Connectivity-Release-Indication. When multiple A-RACF instances are present in the form of hierarchical structure, the NASS sends an IP-Connectivity-Release-Indication to the top tier A-RACF.

2a) The A-RACF responds to the NASS.

3) The A-RACF needs to relinquish all resources associated to the IP address/Subscriber-Id. In case there are still outstanding reservations, the A-RACF also notifies the SPDF. When multiple A-RACF instances are present in the form of hierarchical structure, the top tier A-RACF instance needs to notify other A-RACF instances to check if outstanding reservations exist.

3a) The SPDF responds to the A-RACF.

4) The A-RACF checks if there are resources to be released in the RCEF. Whether steps 5) and 6) are executed is dependent on this decision. When multiple A-RACF instances are present in the form of hierarchical structure, the A-RACF may interact with the co-located RCEF in step 5) and 6).

5) The A-RACF sends a request to the RCEF for the removal of existing policies.

6) The RCEF confirms the removal of existing policies.

7) The SPDF reports to the AF that the existing reservation was revoked.

7a) The AF responds to the SPDF.

8) The SPDF checks if there are resources to be released in the BGF. The execution of steps 9) and 10) are depending on this decision.

9) The SPDF sends a request to the BGF for the removal of allocated resources.

10) The BGF confirms the removal of allocated resources.

6.4.9 Abnormal event from the RCEF

This procedure is used when the A-RACF receives an indication from the RCEF that a certain traffic policy can no longer be sustained. The A-RACF sends a notification towards the AF that the resource reservation was revoked and all associated resources are released.

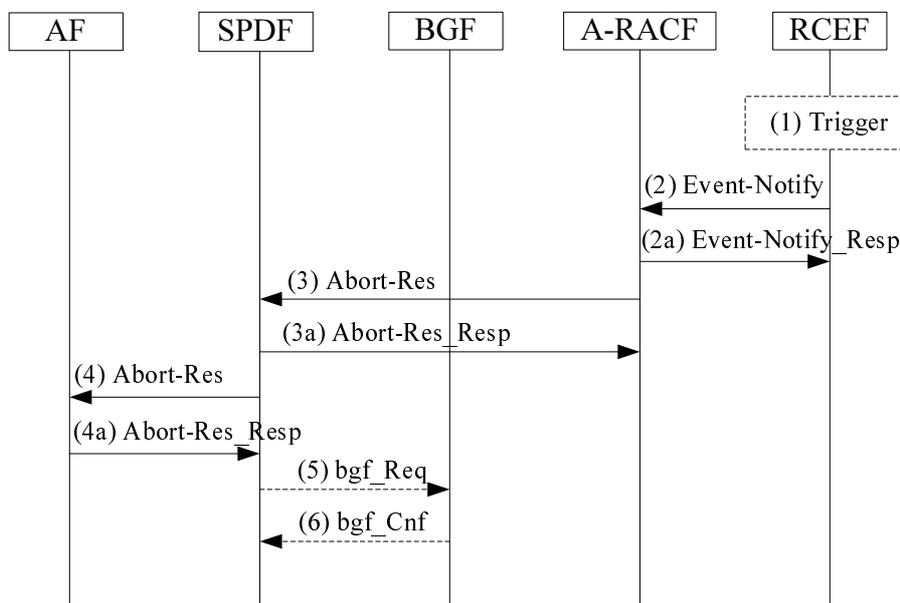Figure 20 presents the associated procedure:

Figure 20: Abnormal event reported by the RCEF

1)   The RCEF decides that it can no longer support the previously installed traffic policies (e.g. problem in the reference point).

2)   The RCEF informs A-RACF that the traffic policies can no longer be applied via an Event-Notify. When multiple A-RACF instances are present in the form of hierarchical structure, the RCEF may interact with co-located A-RACF via an event-notify. This co-located A-RACF also informs the top tier A-RACF.

2a)   The A-RACF sends the response to the RCEF.

3)   The A-RACF needs to relinquish all associated resources. In case there are outstanding reservations, the A-RACF notifies the SPDF by sending Abort-Res. When multiple A-RACF instances are present in the form of hierarchical structure, the top tier A-RACF instance notifies the SPDF based on the results of all A-RACF instances.

3a)   The SPDF sends the response to the A-RACF.

4)   The SPDF reports to the AF that the resources were lost by sending Abort-Res.

4a)   The AF responds to the SPDF.

5)   The SPDF checks if there are resources to be released in the BGF. If yes, the SPDF sends a request to the BGF for the removal of allocated resources.

6)   The BGF confirms the removal of allocated resources.

6.4.10 Report of BGF Events

The BGF is capable of providing dynamic information about the traffic associated to certain media. As such, applications can request RACS to be notified about certain events, for example the level of traffic usage or media activity.

In the scenario the event is reported to the AF as previously requested.
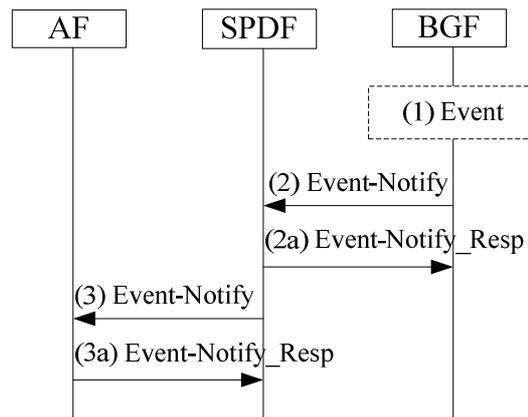
Figure 21: Report of BGF events

1)   The BGF identifies a certain traffic condition needs to be reported in accordance with a service previously requested by the SPDF.

2)   The BGF sends the event notification to the SPDF.

2a)   The SPDF sends the response to the BGF.

3)   The SPDF forwards the event notification to the respective AF.

3a)   The AF responds to the SPDF.

6.4.11   Indication of a BGF Service Failure (Autonomous Release of BGF)

The BGF notifies the SPDF when it detects a condition that leads to the release of previously allocated resources.

Figure 22 presents the particular case where the A-RACF is accessed.
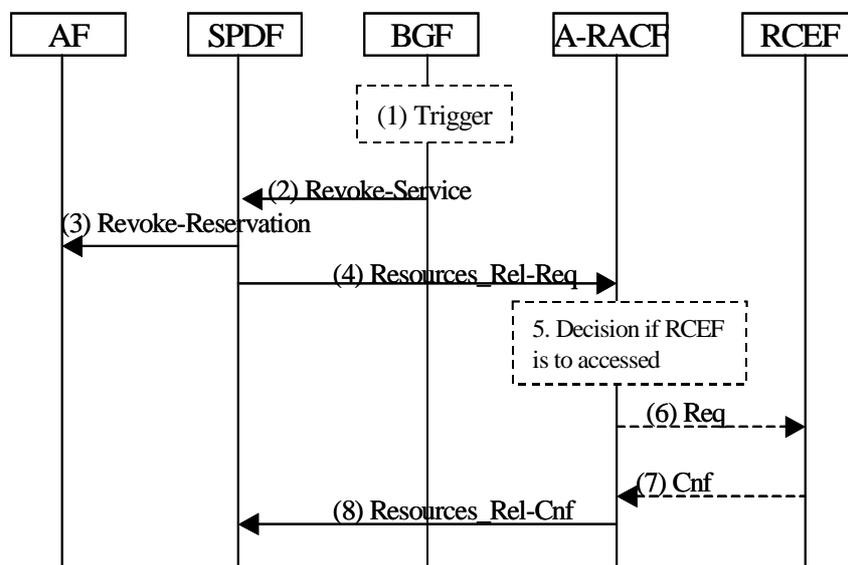
Figure 22: BGF service failure

1)   The BGF detects a failure that affects an existing service (e.g. reference point failure).

2)   The BGF informs the SPDF that the policies can no longer be applied via Revoke-Service. The SPDF verifies that there are resources to be released in A-RACF. Whether steps 4) to 7) are executed is dependent on this decision.

3)   The SPDF reports to the AF that the resources of the resource reservation were revoked.

4) The SPDF requests the A-RACF to release the associated resources (depending on step 2). When multiple A-RACF instances are present in the form of hierarchical structure, the SPDF contacts the top tier A-RACF instance for resource modification operations.

5) The A-RACF needs to relinquish all resources associated to the associated resource reservation session. The A-RACF checks if there are traffic policies to be removed in the RCEF. When multiple A-RACF instances are present in the form of hierarchical structure and are involved in reserving resources for the original reservation request from the AF, the top tier A-RACF instance forwards the request to other A-RACF instances to request the resource release.

6) The A-RACF contacts the RCEF (depending on step 5). When multiple A-RACF instances are present in the form of hierarchical structure, the A-RACF may interact with co-located RCEF to remove the associated traffic policies.

7) The RCEF replies to the A-RACF.

8) The A-RACF replies to the SPDF with information that the resources are released.

Annex A (informative):
Binding Information in RACS, NASS and AF

The example here described uses a xDSL access line to illustrate the use of Subscriber-Id and @IP as binding information. The PPP and DCHP methods are used in a multi-VC environment to illustrate some capabilities offered by the NGN access. It is not the purpose of this annex to limit any other deployment. The same example could also illustrate the Ethernet case by replacing VCs by VLANs.

In this example, "Customer C" has a contract with Access Service Provider S to provide a broadband service.

Figure A.1 gives an example of the usage of the NASS/RACS/AF binding identities. This is a particular implementation that does not preclude other mappings.
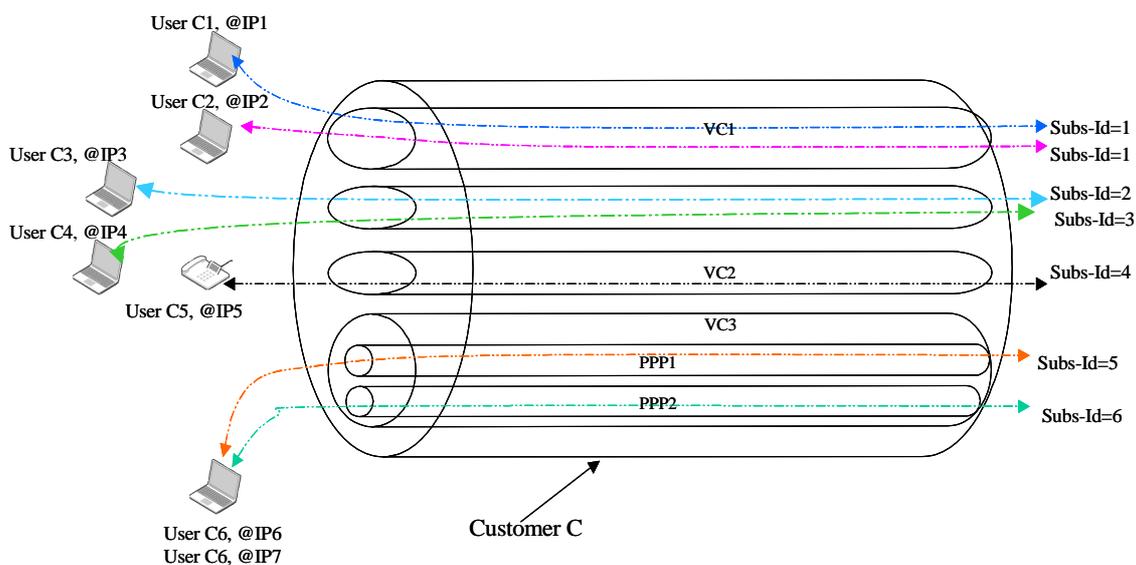
Figure A.1: Example of use of NASS/RACS/AF binding identities

The following consideration applies to the architecture model applied in the access network. It is a particular implementation to illustrate the possibilities of address mapping in NASS.

- Subscriber-ID and or @IP identifies the service bearer resource granted by the network to UE. In the case of PPP, it may identify the bearer (PPP tunnel) that is granted to the end user when the attachment procedure is finished. In case of DHCP, it is expected that Subscriber-ID is derived from the identity of the Client C.

- When an UE attaches to the network , NASS sends to the A-RACF the Subscriber-ID associated to this bearer together with the respective @IP. Different PPP sessions can share the same VC which results that every PPP session may have a different Subscriber-ID, even though those PPP session are over the same VC in the last mile (it does not precludes that the same Subscriber-Id is used). The model allows to the same UE to start multiple PPP sessions.

- When the AF queries the Location of the user to NASS, the AF obtains the same Subscriber-ID as the one sent before by NASS to A-RACF.

- The AF can use the @IP and/or Subscriber-ID to reserve resources from RACS. The SPDF does not modify these parameter.

Annex B (informative):
Policy nomenclature for RACS

This annex contains tutorial information on generic policy nomenclature as a basis for the work on RACS.

B.1   Overview

The main motivation leveraging policies within a system is to support dynamic adaptability of behaviour by changing policy without recoding or stopping a system. This also implies that it should be possible to dynamically update the policy rules interpreted by distributed entities to modify their behaviour. RACS, as a system which processes events, is an example of a generic policy control Sub-System. This clause outlines key terms related to policy and policy control. Additional details can be found e.g. in RFC 3198 [9] ("Terminology for Policy-Based Management") and RFC 2753 [10] and which outlines "a Framework for Policy-based Admission Control", including definitions for terms like Policy Enforcement Points (PEP) and Policy Decision Points (PDP), which are evolved towards a more granular definition of policy here. Other industry fora such as the DSL-Forum also define policy control frameworks (see DSL-Forum [11]).

B.2   Policy Terminology

B.2.1   Policy

A policy is a set of rules which governs the choices in behaviour of a system. A policy is comprised of conditions and actions, where conditions are evaluated when triggered by an event. A policy is attached to a target and in the context of a target, if a condition evaluates to true, then the associated actions are executed. A system that supports the execution of policies exposes methods to provision, update and delete these policies. Further, it provides methods to activate and deactivate policies against the targets of policy supported by the system. The execution of policies may result in the provisioning or activation of policies on interconnected systems. This is known as policy delegation.

B.2.2   Conditions

A condition in its most general form is any expression that can evaluate to true or false. A condition is often referred to as a match criterion (i.e. if a specific criterion is met/matched, then the associated action(s) will execute).

B.2.3   Actions

Actions within a policy are generally domain specific. For example, there could be some actions that are applicable to executing a security related policy and there could be some actions that are applicable to executing a QoS/bandwidth-management policy (e.g. guaranteeing minimum rate or low latency behaviour).

B.2.4   Events

As noted earlier, the notion of an event provides the trigger for evaluating a condition. In some contexts the trigger mechanism for evaluating a condition (i.e. an event) can be implicit and thus an explicit event cannot be observed. For example, when a policy applies to traffic traversing a network device (e.g. a traffic policing feature is applied to traffic identified by a certain 5-tuple), the condition is typically some match criterion based on the value(s) of some field(s) in a packet and the implicit triggering event is the arrival of a packet (i.e. the condition is evaluated on each packet at the time of arrival of the packet). In other contexts, however, it is important to have an explicit event to trigger the evaluation of a condition because in the absence of such a trigger there is no basis for knowing when to evaluate the condition.

B.3   Types of Policy

B.3.1   Authorization Policy

Authorization policies define what services or resources a subject (i.e. user or management agent) can access (see also Damianou, N. et. al [12]) and which actions a subject can perform. One differentiates between positive authorization policies, which specify sets of permitted actions, and negative authorization policies, which correspondingly define forbidden actions. If one or more active authorization policies are in scope for the received request, these policies are executed and any associated actions conditionally invoked. Policy processing entities commonly allow for explicit provisioning and storage of authorization policies as manageable entities.

Within RACS, SPDF as well as A-RACF are examples of entities which implement authorization policies. When an authorization request is received by either SPDF or A-RACF, the SPDF or A-RACF will determine and execute all applicable policies.

B.3.2   Obligation Policy

Obligation policies are event-triggered condition-action rules [12]. Obligation policies allow for performing a wide range of management-type of actions such as the allocation of bandwidth resources for a particular flow or the release of certain resources in case of failure scenarios (e.g. abnormal condition or overload condition event reported from BGF to SPDF). Actions within an obligation policy can include sub-obligation policies which must be processed locally or remotely. Sub-obligation policies can be activated as an action of the containing policy or can be embedded conditions/actions that are executed within the scope of an event processed by the containing policy.

B.3.3   Traffic Policy

> NOTE: See definition in clause 3.1.

B.3.4   Control Policy

Policies for which the execution trigger is an explicit control-plane event (e.g. a signalling event, a timer expiry event, etc.), and for which the action(s) does not entail the processing of a forwarded data packet, are known as control policies.

Annex C (informative):
Admission control scenarios

This annex contains tutorial information on admission control scenarios in order to better understand the third bullet item indicated in clause 6.2.2.5.1 of A-RACF Functional Entity.

C.1 Example of the handling of Connection Oriented network in the aggregation segment

The example described hereinafter constitutes a scenario that shows how A-RACF performs resource admission control in Connection Oriented network types.

In the broadband access network, the Network Access Provider performs the pre-provision of the network by creating logical channels (e.g. VP/VC, VLAN, MPLS LSP) between the AN and the IP_Edge by allocating bandwidth to these channels in advance based on network policy, making use of e.g. NMS , remote login or local configuration. All the logical channel information and related bandwidth parameter are stored or reported to A-RACF. Each logical channel bears a transport class so that every AN-IP_Edge pair has a full set of channels to connect each other. This information is used by the AN and by the IP_Edge to perform QoS flow classification and mapping to L2 logical channels. When AN has not the ability to do flow classification, the CPN can be considered instead to perform the L3 to L2 mapping, and in that case the policy can be provisioned by NMS or by other controller.

Also, both the AN and the IP_Edge may perform DiffServ QoS policy control and other Layer 2 switches located between the AN and the IP_Edge may either also perform DiffServ control or just do cross connection. These layer 2 switches, even though may have the DiffServ capability, may not perform bandwidth control, i.e. they may just schedule packets by transport priority, e.g. SP- strict priority. The bandwidth control is only performed at edge node (AN, IP_Edge) to permit flexible change of network policy. Moreover, the Layer 2 switches mainly perform Layer 2 connection data packets forwarding, and can be un-touched after the system has been setup.

After having received a QoS request from the AF, via the SPDF, and user's profile has been verified and passed, the A-RACF first selects an appropriate channel considering user's location information, transport class and IP_Edge selection information. The A-RACF subsequently evaluates whether to accept the outstanding request by comparing free quota associated to this channel and the requested quota, as well as by checking all the pre-provisioned access network policies Imposed by physical topology resource restriction. The A-RACF may dynamically derive and install L2/L3 traffic policies to the AN and the IP_Edge in order to authorize more or less bandwidth to an explicit transport class. The action is triggered by event notification, as indicated in access network policies or by resource usage status. Depending on the provider's choice, the control signalling granularity between the A-RACF and the transport processing functions can be transport class based or flow based.

Annex D (informative):
Network deployment scenarios

The TISPAN NGN architecture does not define business models but needs to support multiple network deployment scenarios in order to accommodate current as well future business models in industry. This annex provides a summary of the network deployment scenarios supported by RACS R2, which have been used to derive architectural requirements.

D.1 Resource control scenarios according to distribution of Service-based Policy Decision and Admission Control Functions

D.1.1 Single NGN operator performs Service-based Policy Decision and Admission Control Functions

D.1.1.1 Scenario Overview

This network deployment scenario supports the model where a single operator plays both the NGN Access Network and NGN Connectivity Provider roles and therefore performs all Service-based Policy Decision and Admission Control functions required.

Figure D.1 depicts this network deployment scenario.
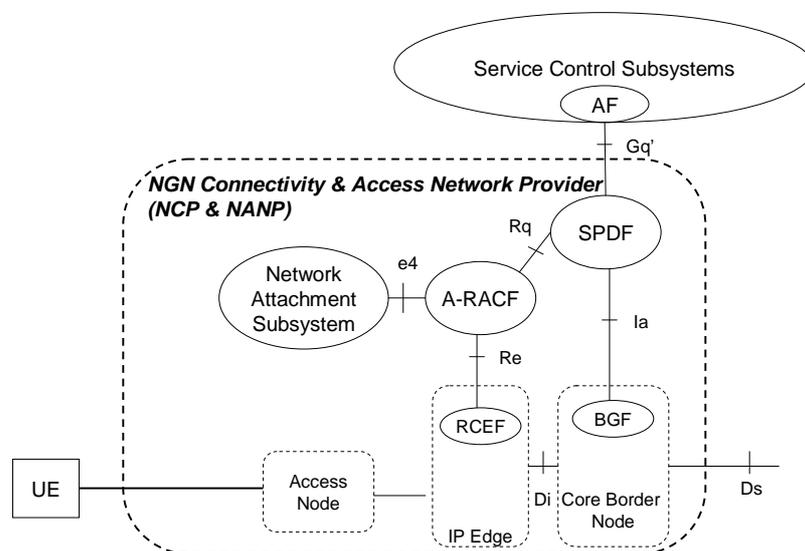
Figure D.1: Single NGN operator performs Service-based Policy Decision and Admission Control Functions

D.1.1.2 Business Need

This scenario is currently implemented in multiple NGN operators' networks.

D.1.1.3 Mapping to TISPAN Architecture: RACS requirements

This scenario was already supported in TISPAN RACS R1 and therefore does not impose any additional requirements to the TISPAN RACS R2 architecture.

D.1.1.4 Technical Analysis

D.1.1.4.1 Functional Element Analysis

No new functional elements are required.

D.1.1.4.2 Elementary Functions Analysis

No new or modified elementary functions are required.

D.1.1.4.3 Reference Point Analysis

No new reference points are required.

D.1.2 Service-based Policy Decision function handled in two domains

D.1.2.1 Scenario Overview

This network deployment scenario supports the model where two different operators play the roles of NGN Access Network Provider and NGN Connectivity Provider.

In this scenario the NGN Connectivity Provider performs some Service-based policy control itself in order to police requests from different application functions but relies on the NGN Access Network Provider to perform all Admission Control functions including:

- Admission Control based on access user profile.

- Admission Control based on available resources over the last mile (access network segment, ES 282 001 [2]).

- Admission Control based on SP profile.

- Admission Control based on available resources over the aggregation network segment.

It should be noted that the NGN Access Network Provider also performs some Service-based policy control itself in order to police requests coming from different NGN Connectivity Providers.

The figure below depicts this network deployment scenario.

Figure D.2: Service-based Policy Decision Function handled in two domains

NOTE: The distribution of NASS functional elements across these two domains is outside the scope of the present document. More detail can be found in ES 282 004 [5].

D.1.2.2 Business Need

This scenario is one possible way in which NGN operators are considering implementing wholesale and nomadism business models.

D.1.2.3 Mapping to TISPAN Architecture: RACS requirements

This scenario requires support for inter-SPDF communication so that RACS functions related to access and aggregation networks can be distributed across domains. The inter-SPDF communication required by this scenario is limited to delegation of Admission Control decisions across access and aggregations networks.

D.1.2.4 Technical Analysis

D.1.2.4.1 Functional Element Analysis

No new functional elements are required. However, SPDF is now required to communicate to adjacent SPDFs via the reference point Ri'.

D.1.2.4.2 Elementary Functions Analysis

No new elementary functions are required.

D.1.2.4.3 Reference Point Analysis

The new reference point Ri' as specified in clause 6.3.5 is required.

It should be noted that the use of Ri' in TISPAN RACS R2 is limited to the access-network related scenarios described in this annex. Ri' does not provide support for core-to-core interconnect scenarios where coordination of admission control decisions over separate core transport networks may be required.

D.1.3   Service-based Policy Decision and Admission Control functions distributed across two domains

D.1.3.1   Scenario Overview

This network deployment scenario supports the model where two different operators play the roles of NGN Access Network Provider and NGN Connectivity Provider.

In this network deployment option, the NCP performs its own Admission Control decisions related to the access user profile and the available resources on the access network segment, ES 282 001 [2]. The NANP performs Admission Control decisions based on the NCP's profile and available resources over the aggregation network segment.

Figure D.3 depicts this network deployment scenario.

Figure D.3: Service-based Policy Decision and Admission Control functions distributed across two domains

NOTE: The distribution of NASS functional elements across these two domains is outside the scope of the present document. More detail can be found in ES 282 004 [5].

D.1.3.2   Business Need

This scenario is one possible way in which NGN operators are considering implementing wholesale and nomadism business models.

D.1.3.3   Mapping to TISPAN Architecture: RACS requirements

This scenario requires support for inter-SPDF communication so that RACS functions related to access and aggregation networks can be distributed across domains. The inter-SPDF communication required by this scenario is limited to delegation of Admission Control decisions across access and aggregation networks.

D.1.3.4 Technical Analysis

D.1.3.4.1   Functional Element Analysis

No new functional elements are required. However, SPDF is now required to communicate to adjacent SPDFs via the reference point Ri' and to perform coordination of requests/responses via Ri' (from adjacent SPDFs) and requests/responses via Rq (from local A-RACF) belonging to a single resource reservation request over Gq'.

D.1.3.4.2   Elementary Functions Analysis

No new elementary functions are required.

D.1.3.4.3   Reference Point Analysis

It should be noted that the use of Ri' in TISPAN RACS R2 is limited to the access-network related scenarios described in this annex. Ri' does not provide support for core-to-core interconnect scenarios where coordination of admission control decisions over separate core transport networks may be required.

D.2   Resource control scenarios for Multicast and Unicast

This clause outlines a number of deployment scenarios for the RACS if Unicast and Multicast admission control are both required. Deployment scenarios are understood as different options on how an operator chooses to instantiate functional entities of RACS as well as related functional entities in physical devices. These scenarios are optional and depend on the deployment context of the network operator.

D.2.1   Independent scenario - Unicast and Multicast admission control are separated

D.2.1.1 Scenario Overview

For the "Independent Scenario", separate (and independent) instances of x-RACF are deployed for Unicast and for multicast. In this deployment scenario, resources are administratively split across unicast and multicast. x-RACF instance(s) handling Unicast and the x-RACF instances handling Multicast operate independently from each other and thus do not require any communication between them. Thus resources need to be partitioned across Unicast and Multicast.

> NOTE: For illustration purposes, there could for example be a single instance of x-RACF for unicast and multiple instances of x-RACF for multicast, geographically distributed for enhanced multicast admission control scalability. In this deployment scenario, resources are administratively split across unicast and multicast.

D.2.1.2 Business Need

Not applicable.

D.2.1.3 Mapping to TISPAN Architecture: RACS requirements

The "Independent Scenario" does not require any additional functional elements for the TISPAN Architecture. It requires that RACS functions and transport functions related to RACS are supporting Multicast (this includes e.g. support of Multicast in x-RACF and RCEF).

D.2.1.4 Technical Analysis

D.2.1.4.1 Functional Element Analysis

No new functional elements are required, though existing RACS functions (x-RACF and SPDF) as well as related transport functions (e.g. RCEF) need to be multicast aware.

D.2.1.4.2 Elementary Functions Analysis

Those elementary functions impacted by multicast need to be extended to support multicast as well.

D.2.1.4.3 Reference Point Analysis

No new reference points are required.

D.2.2 Synchronized Scenario

D.2.2.1 Scenario Overview

Similar to the "Independent Scenario", Unicast and Multicast admission control are handled by different instances of x-RACF. Different from the "Independent Scenario", the different instances of x-RACF cooperate with each other in the "Synchronized Scenario". The x-RACF instance(s) handling Unicast communicate(s) with the x-RACF instances handling Multicast in order to synchronize their view on resource utilization and availability. Therefore resources can be shared across Unicast and Multicast. Information exchange across x-RACF instances is required. The synchronization between x-RACF instances can be achieved at various granularity allowing different trade-offs between the level of synchronization overhead and the efficiency of resource sharing across Unicast and Multicast.

> NOTE: For illustration purposes, there could for example be a single instance of x-RACF for Unicast and Multiple instances of x-RACF for multicast, geographically distributed for enhanced multicast admission control scalability.

D.2.2.2 Business Need

Not applicable.

D.2.2.3 Mapping to TISPAN Architecture: RACS requirements

The "Synchronized Scenario" does not require any additional functional elements for the TISPAN Architecture. It requires that RACS functions and transport functions related to RACS are supporting multicast (this includes e.g. support of multicast in x-RACF and RCEF). Given that different instances of x-RACF need to synchronize their state, a new x-RACF - x-RACF reference point is required.

D.2.2.4 Technical Analysis

D.2.2.4.1 Functional Element Analysis

No new functional elements are required, though existing RACS functions (x-RACF and SPDF) as well as related transport functions (e.g. RCEF) need to be multicast aware. The different instances of x-RACF handling Multicast and Unicast need to be able to cooperate/synchronize with each other (see also clause D.2.2.4.3 on the requirement of a new x-RACF - x-RACF reference point).

D.2.2.4.2 Elementary Functions Analysis

Those elementary functions impacted by multicast need to be extended to support multicast as well.

D.2.2.4.3   Reference Point Analysis

A new reference point x-RACF - x-RACF is required.

D.2.3   Integrated scenario - Integrated Unicast and Multicast Admission Control

D.2.3.1   Scenario Overview

The "Integrated scenario" describes a deployment where both multicast and Unicast admission control are jointly managed by the same single or multiple instance(s) of x-RACF. For the "Integrated Scenario", x-RACF will typically be a functional instance of A-RACF, given that both - unicast and multicast admission control are handled by the x-RACF instance. If multiple instances of x-RACF are deployed a particular resource is only handled by a instance of x-RACF, i.e. resources are never controlled by more than a single instance of x-RACF. In this deployment scenario, each instance of x-RACF handles both Unicast and Multicast. It allows sharing of resource across Unicast and Multicast. No communication is needed between x-RACF instance(s).

> NOTE: The scenario relies on the use of the same x- RACF instance for both Unicast and Multicast. For illustration purposes, there could for example be multiple instances of x-RACF geographically distributed. Resources are completely shared across Unicast and Multicast.

D.2.3.2   Business Need

Not applicable.

D.2.3.3   Mapping to TISPAN Architecture: RACS requirements

The "Independent Scenario" does not require any additional functional elements for the TISPAN Architecture. It requires that RACS functions and transport functions related to RACS are jointly supporting Multicast and Unicast (this includes e.g. support of multicast in x-RACF and RCEF).

D.2.3.4   Technical Analysis

D.2.3.4.1   Functional Element Analysis

No new functional elements are required, though existing RACS functions (x-RACF and SPDF) as well as related transport functions (e.g. RCEF) need to be multicast aware.

D.2.3.4.2   Elementary Functions Analysis

Those elementary functions impacted by multicast need to be extended to support multicast as well.

D.2.3.4.3   Reference Point Analysis

No new reference points are required.

D.3   Resource control scenario for Metro Network

D.3.1   Scenario Overview

This network deployment scenario supports the Admission Control functions and resource control in metro network.

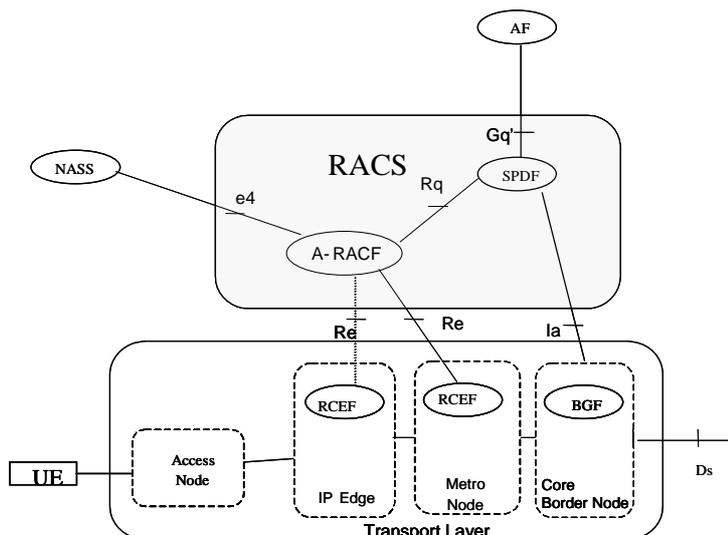Figure D.4 depicts this network deployment scenario.

Figure D.4: Resource Control Functions for Metro Network

D.3.2   Business Need

This scenario is currently implemented in many NGN operators' networks which have metro networks.

D.3.3   Mapping to TISPAN Architecture: RACS requirements

This metro controlling scenario does not require any additional functional elements for the TISPAN Architecture. However, the following extensions are needed for metro control.

- Metro Network resource control functions should be evaluated for inclusion into x-RACF.

- RCEFs are deployed to the metro nodes for resource controlling.

- x-RACF communicates with RCEFs in metro nodes through the Re reference point.

D.3.4   Technical Analysis

D.3.4.1   Functional Element Analysis

No new functional elements are required. But some function extensions in x-RACF and RCEF are required for metro controlling.

The function extensions for metro control are not standardized within the present document.

D.3.4.2   Elementary Functions Analysis

No new or modified elementary functions are required.

D.3.4.3   Reference Point Analysis

The Re reference point is used by RACS for controlling metro nodes, and it may need extension for metro control.

This issue is not standardized within the present document.

Annex E (informative):
Topology and Resource Management Use Cases and Elementary Functions

This annex contains tutorial information on use cases for Topology and Resource Management and related Elementary Function definitions as indicated in requirement of clause *4.2.2.6 Topology and Resource Information Retrieval*, item 33.

E.1   Topology and Resource Management Use Cases

E.1.1   Initial RACS Startup

When a RACS is deployed for the first time, it must load relevant topology and resource data from external systems in the carrier network. This use case is illustrated by the following scenario:
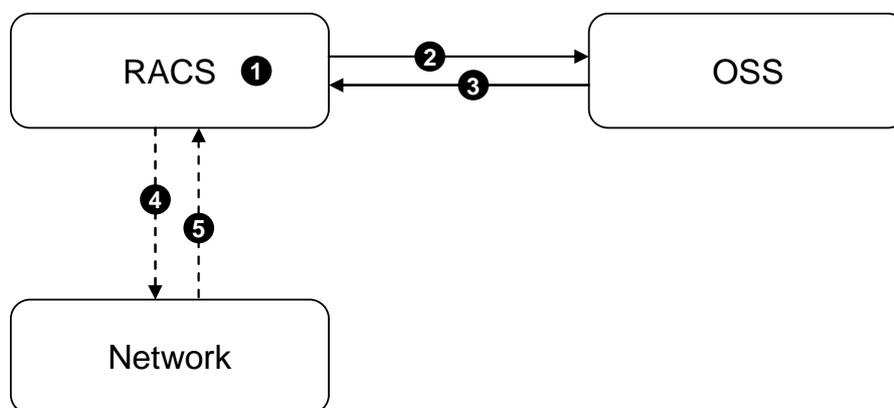
Figure E.1: Initial RACS startup

Key:

1.   RACS is started.

2.   RACS contacts OSS requesting topology and resource data.

3.   OSS sends current topology and resource data to RACS.

4.   RACS initiates a network auto-discovery procedure based on data received from OSS, as represented in the next clause [optional].

5.   RACS receives auto-discovered configuration data from network, as represented in the next clause [optional].

E.1.2   Network Auto-Discovery

The RACS may be capable of auto-discovering some or all of its element and topology information. Auto-Discovery may be a singular activity (e.g. the operator clicks a button asking for RACS to auto-discover the topology) or it may be an ongoing activity (e.g. the RACS periodically initiates re-discovery procedures to update its internal knowledge of the network). In either case, auto-discovery relies on the ability of the RACS to query specific network elements and systems to obtain element and topology information. The procedure, which may be applicable to several situations including the one indicated in the first use case, is represented below:
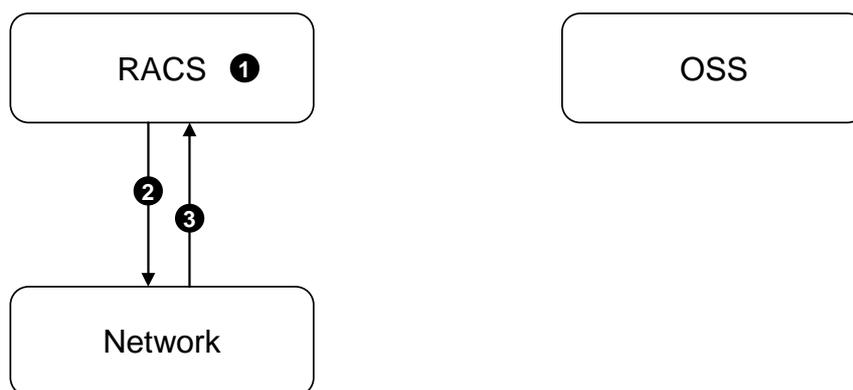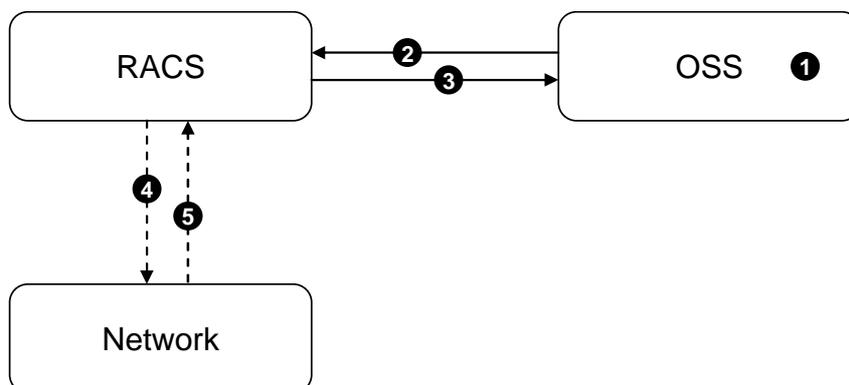
Figure E.2: Network auto-discovery procedure

Key:

1. RACS determines that it needs to auto-discover network data.

2. RACS initiates auto-discovery procedure based on local data.

3. RACS receives auto-discovered configuration data from network.

E.1.3   Managing Network Elements

NGN network operators will periodically add new network elements to their network to scale subscriber and service capabilities. As new network elements are added, the RACS must be made aware of their presence. This situation is represented in figure E.3:

**Figure E.3: Managing network elements**

Key:

1. A network element is added / modified / removed from OSS.

2. OSS notifies RACS of the change.

3. RACS confirms change receipt.

4. RACS initiates a network auto-discovery procedure based on data received from OSS, see clause E.1.2 [optional].

5. RACS receives auto-discovered configuration data from network, see clause E.1.2 [optional].

E.1.4   Managing Network Topology

NGN network operators will update network topology to reflect changes in the existing network configuration as well as during roll-out of new network elements. As the network topology is updated, the RACS must be made aware of the changes. Changes may occur in the topology of the network (e.g. an AN is connected to a new IP_Edge device) or the resource associated with that topology (e.g. the VP capacity between an IP_Edge and AN is changed). This use case may be represented as follows:
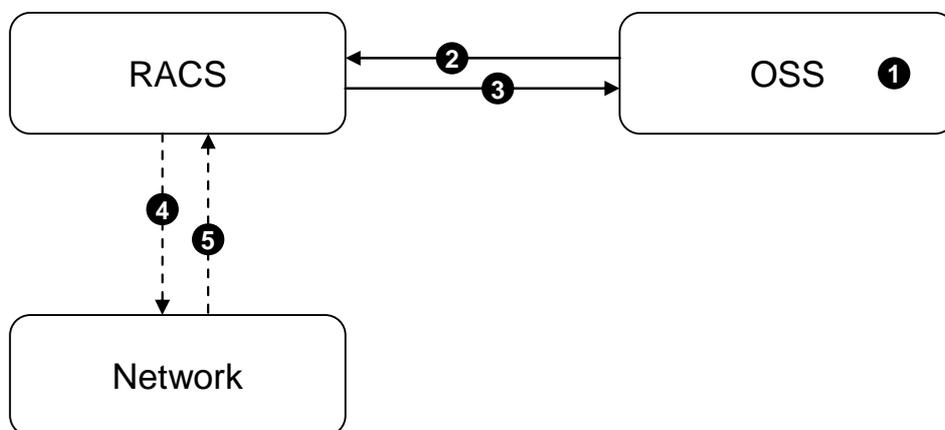
Figure E.4: Managing network topology

Key:

1.   A network link is added / modified / removed from OSS.

2.   OSS notifies RACS of the change.

3.   RACS confirms change receipt.

4.   RACS initiates a network auto-discovery procedure based on data received from OSS, see E.1.2 [optional].

5.   RACS receives auto-discovered configuration data from network, see clause E.1.2 [optional].

E.1.5   Real-Time Monitoring

Events within the network may temporarily change the element and topology information needed by RACS. As opposed to provisioning and auto-discovery, monitoring deals with temporary changes to the network such as the transient failure/restart of a network link or element. The RACS notification of that change may be performed directly or through the OSS system.

E.1.5.1   Real-time Monitoring (Network Integration)

In this case, RACS is directly notified by the network and may perform a network auto-discovery procedure.
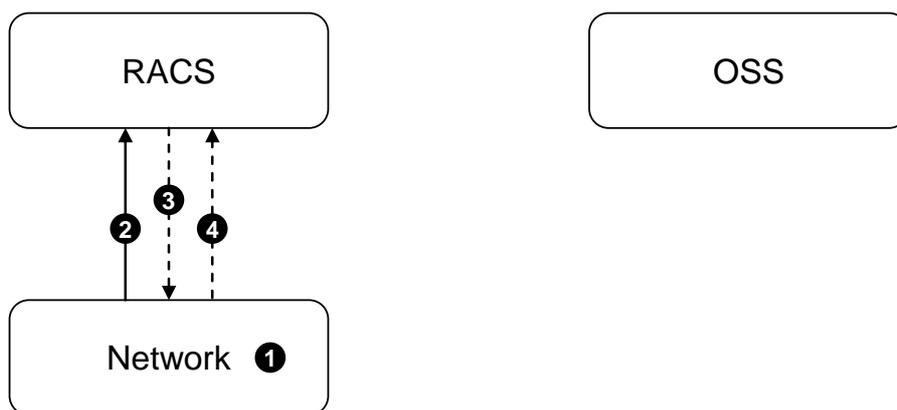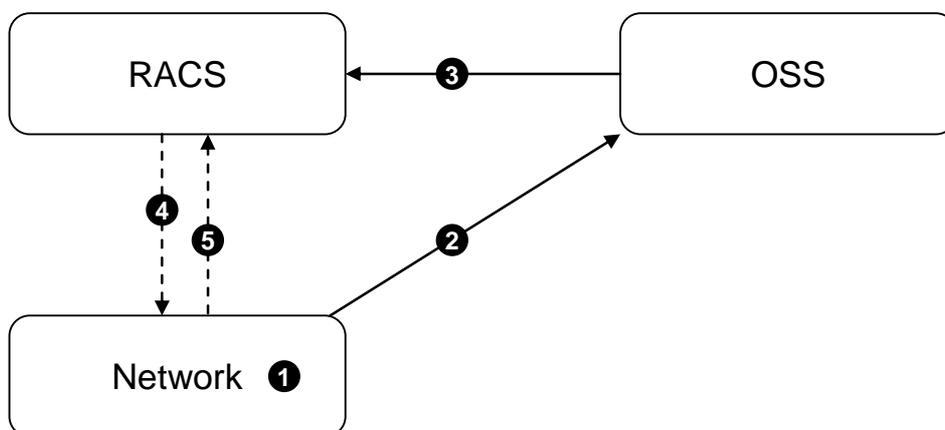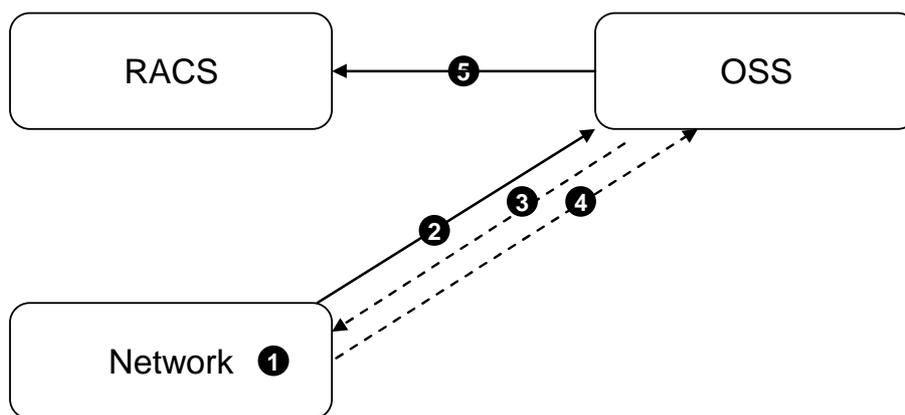
Figure E.5: Real-time monitoring performed by network integration

Key:

1. An event occurs within the network that modifies the state of one or more network resources.

2. Network notifies RACS that state has been updated.

3. RACS initiates a network auto-discovery procedure based on data received from network, see clause E.1.2 [optional].

4. RACS receives auto-discovered configuration data from network, see clause E.1.2 [optional].

E.1.5.2   Real-time Monitoring (OSS Integration)

In this case, RACS is notified through the OSS and may perform a network auto-discovery procedure.

Figure E.6: Real-time monitoring performed by OSS integration

Key:

1. An event occurs within the network that modifies the state of one or more network resources.

2. Network notifies OSS of event.

3. OSS notifies RACS that state of network has been updated.

4. RACS initiates a network auto-discovery procedure based on data received from network, see clause E.1.2 [optional].

5. RACS receives auto-discovered configuration data from network, see clause E.1.2 [optional].

E.1.5.3   OSS-based Monitoring

In this case, RACS is notified through the OSS, which interrogates the network to obtain further information.

Figure E.7: Real-time OSS-based monitoring

Key:

1. An event occurs within the network that modifies the state of one or more network resources.

2. Network notifies OSS of event.

3. OSS requests additional information about current state of network.

4. OSS receives additional information about current state of network.

5. OSS notifies RACS that state of network has been updated.

E.1.6   Just-In-Time Information Pull

When RACS is processing a Multimedia Authorization request, it may not have the topology information required to process the decision. The RACS can asynchronously load additional topology data from the OSS in order to continue processing the request. The following diagram illustrates this use case:
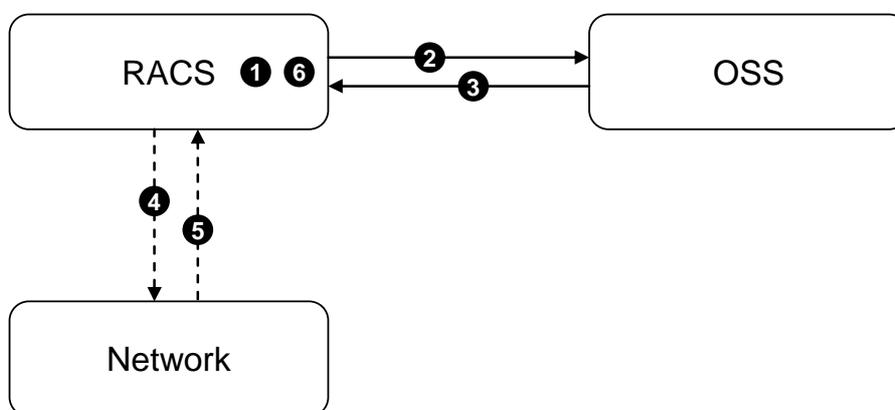
Figure E.8: Just in time information pull

Key:

1. RACS is processing a Multimedia Authorization request but determines that it is lacking information to process the request.

2. RACS contacts OSS requesting topology and resource data.

3. OSS sends current topology and resource data to RACS.

4. RACS initiates a network auto-discovery procedure based on data received from OSS, see E.1.2 [optional].

5. RACS receives auto-discovered configuration data from network, see E.1.2 [optional].

6. RACS continues processing the Multimedia Authorization request.

E.2 Topology and Resource Management Elementary Functions

This clause describes the Elementary Functions that may be considered as associated with the above mentioned use cases for Topology and Resource Management. These Elementary Functions may be applicable to x-RACF or other RACS Functional Entities, e.g. the Provisioning EF is also applicable to the SPDF.

E.2.1 Provisioning Elementary Function

The Provisioning EF provides facilities for an external system to inform the RACS of static element and network topology data. The Provisioning EF may operate in Pull or Push mode. When operating in Pull mode, the RACS will contact an external system to request a download of static element and topology data. When operating in Push mode, external systems will asynchronously notify the RACS of changes to the static element and topology data.

Provisioning is a mandatory capability of RACS.

E.2.2 Discovery Elementary Function

The Discovery EF uses information received during Provisioning to learn additional data about the network environment. Network Discovery procedures may be initiated by a Provisioning event (e.g. new data provisioned to the RACS triggers a Network Discovery activity), a scheduled event (e.g. Network Discovery executes periodically according to operator defined configuration) or other internal events (e.g. a fault notification to the RACS causes it to initiate re-discovery activity).

Discovery is an optional, but highly desirable capability.

E.2.3 Partitioning Elementary Function

The Partitioning EF manages the distribution of provisioned and discovered data across RACS entities (e.g. x-RACFs). The Partitioning EF may be used during Provisioning, Discovery and Monitoring to determine the set of Functional Entities that should receive an update. For example, the operator may specify that "IP_Edge Device #1" is assigned to "x-RACF #1".

The Partitioning EF is only required if the RACS employs a single point of contact for receiving provisioning and/or discovery information. If a RACS deployment has multiple points of contact (e.g. each x-RACF has its own provisioning service), then the partitioning activity is assumed to be part of an external system (e.g. OSS) that determines which entity to send updates to.

E.2.4 Monitoring Elementary Function

The Monitoring EF tracks real-time changes to the state of provisioned and/or discovered information. The Monitoring EF receives notifications from external systems and updates the internal state of the resources affected by the event (e.g. mark a link or element as "up/down").

Monitoring is an optional, but highly desirable capability.

E.3 Topology and Resource Management Architectural Models

The deployment of the TRSF capability may be performed using Centralized or Distributed Models as architectural basis.
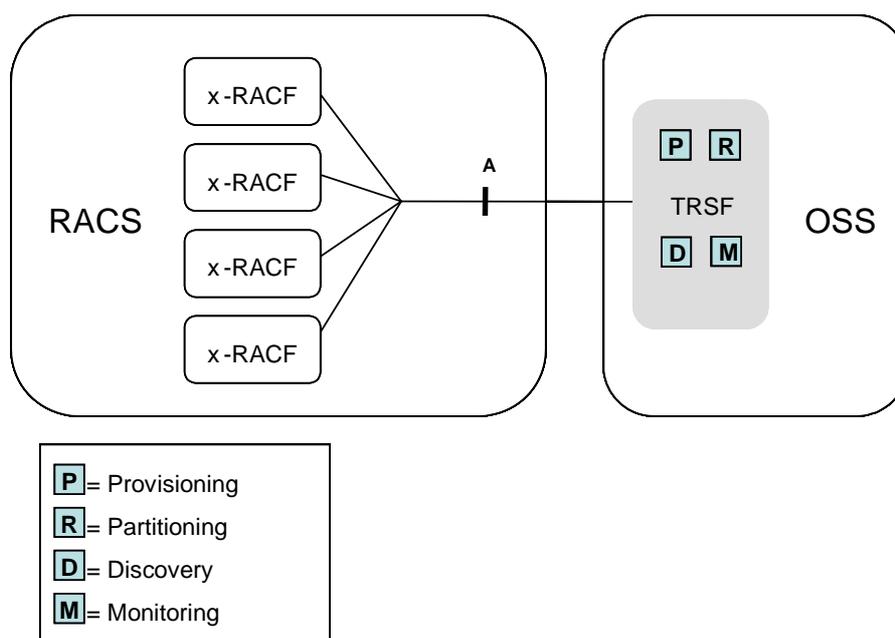
E.3.1   Centralized Model

In the centralized model, the TRSF is integrated in the RACS Sub-System. This single entity is responsible by the implementation of the Provisioning, Partitioning, Discovery and Monitoring Elementary Functions. The TRSF provides a single view of the network that is shared by the other RACS entities, and also provides a single point of contact for the OSS to communicate with RACS.
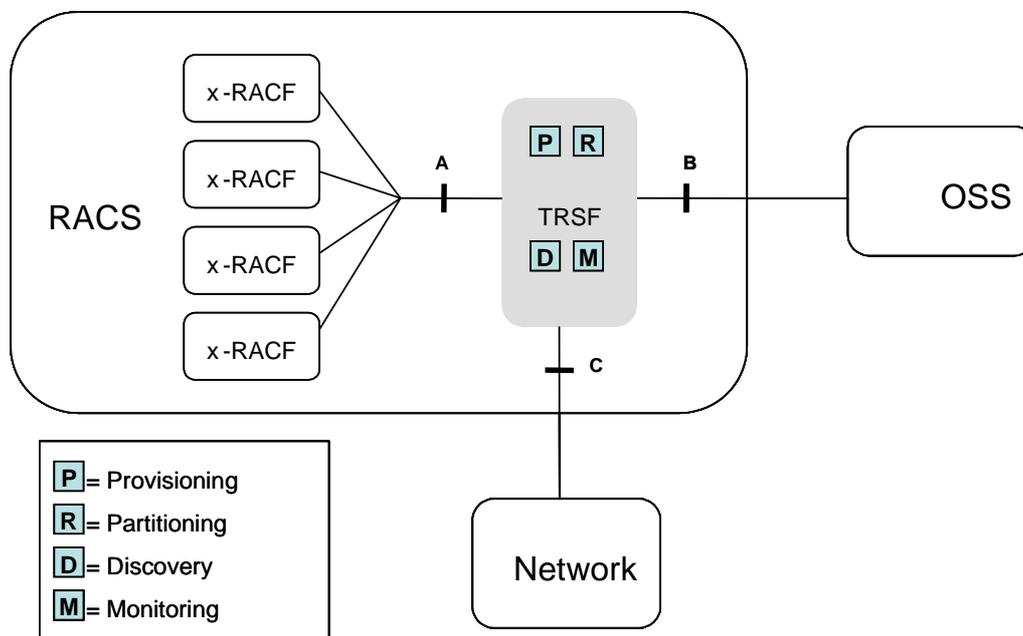
Figure E.9: TRSF deployment based in a centralized model with integration in RACS

In this model, the reference point "B" is the reference point between the OSS and the RACS. When the TRSF receives information over the "B" reference point it may optionally discover additional information from the network. The TRSF uses the history of information received over "B" as well as the discovered information from "C" to provide a complete and consistent view of the network over the reference point "A".

This centralized model may also be implemented by having as a basis an architecture where the functions of the TRSF are part of the OSS. This model is depicted below:


Figure E.10: TRSF deployment based in a centralized model with integration in OSS

In this model, the "A" reference point is the reference point between the OSS and the RACS. If this model is employed, the mechanisms by which the OSS maintains a current view of the network are outside the scope of RACS. However, RACS still requires the "A" reference point to provide each x-RACF Functional Entity with a complete and consistent view of the network.

E.3.2   Distributed Model

In the distributed model, each RACS Functional Entity handles its own Provisioning, Discovery and Monitoring elementary functions. The OSS in this model must provide the partitioning elementary function, as it must understand how requests should be routed to individual RACS entities. Each RACS Functional Entity has its own view of the network which is kept consistent independent of the operation of the other RACS components.
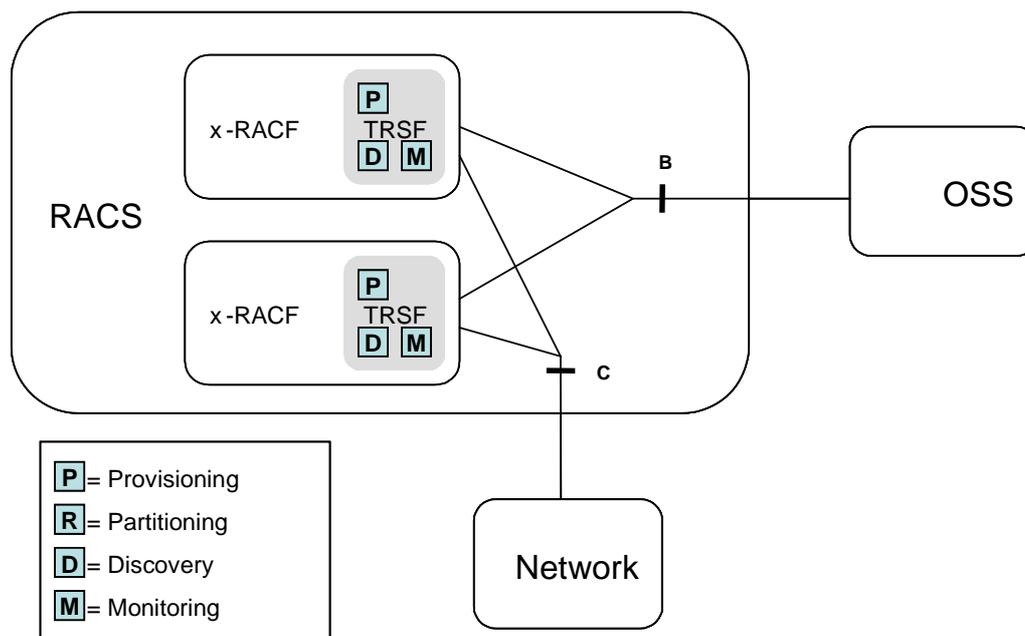
Figure E.11: TRSF architecture based in a distributed model

In this model, the "B" reference point is the reference point between the OSS and the RACS. However unlike the Centralized model, the OSS is presented with multiple "B" enabled endpoints. This means that the OSS must be aware of how topology information should be distributed amongst RACS Functional Entities. This also means that the TRSF function does not require a partitioning functional area.

Each x-RACF Functional Entity in this model will perform its own auto-discovery and monitoring over the "C" reference point.

Annex F (informative):
Architectural scenarios for supporting unicast and multicast

This annex outlines a number of possible Multicast architectural scenarios for RACS to support Multicast Resource Admission Control. It should be noted that these scenarios do not represent an exhaustive list. Information flows drawn from it are showed in annex G which are the candidates for inclusion in the formal RACS flows on multicast.

F.1   Example of an NGN Access Network Architecture for support of Multicast Resource Admission Control

The Transport Network Nodes require some functions in order for Resources Admission Control to support multicast and for these nodes to offer multicast based services such as IPTV. These Transport Network nodes may require interfacing with the RACS for Admission Control and Resource Reservation Requests and have support specific multicast transport functions for example IGMP Snooping.

Figure F.1 describes an example of an NGN Access Network Architecture, the Transport Network Nodes and their associated Multicast Functions and reference points required from Transport Network Nodes to the RACS NGN Sub-System.
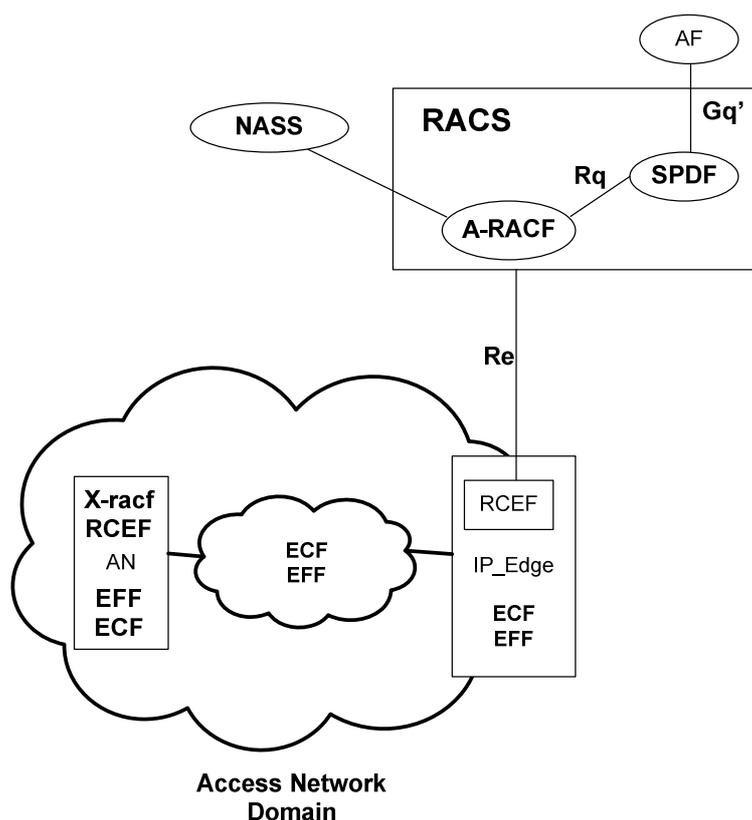

Figure F.1: Example of an NGN Access Network Domain Architecture with Transport Node Elements and supporting Functions required for Multicast Resource and Admission Control

All Transport Network Nodes in the Access Network Domain must be Multicast Aware, and therefore all Transport Network Nodes must support the Elementary Forwarding Function (EFF). The Access Node could also support the x-RACF Functional instance which enables the AN to query the RACS to verify if sufficient resources are available and make policy decisions on multicast traffic. The x-RACF functional instance may also be used to update the RACS of resources being consumed for Multicast based services. The Elementary Control Function (ECF) in the IP_Edge Node or Access Node is where IGMP and Multicast Listener Discovery (MLD) are terminated for Multicast Group Management in the Access Network Domain. The IP_Edge Node may also query the RACS to verify if sufficient resources are available for a requested Multicast Service and may update the RACS of resources being consumed in the Access Network domain.

F.2   Scenario for supporting multicast in push mode

This scenario supports the model where push mode is used.
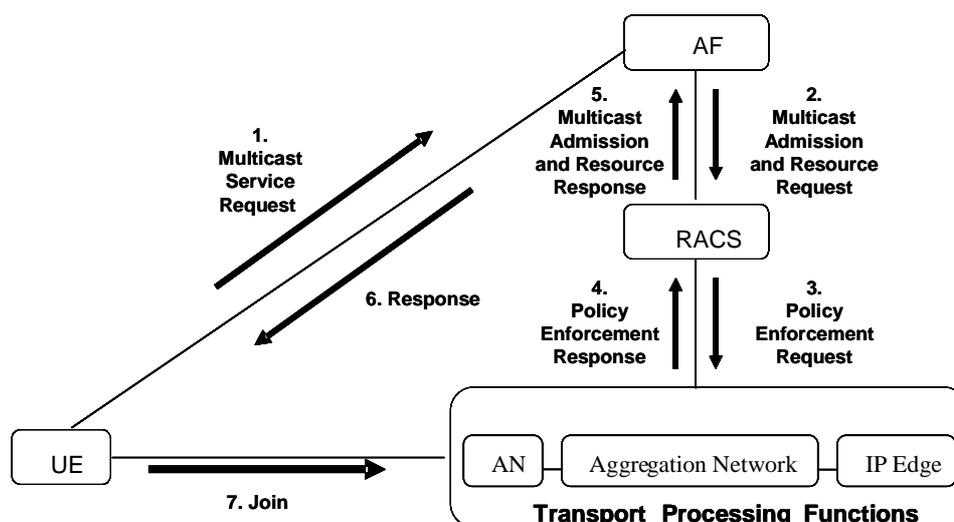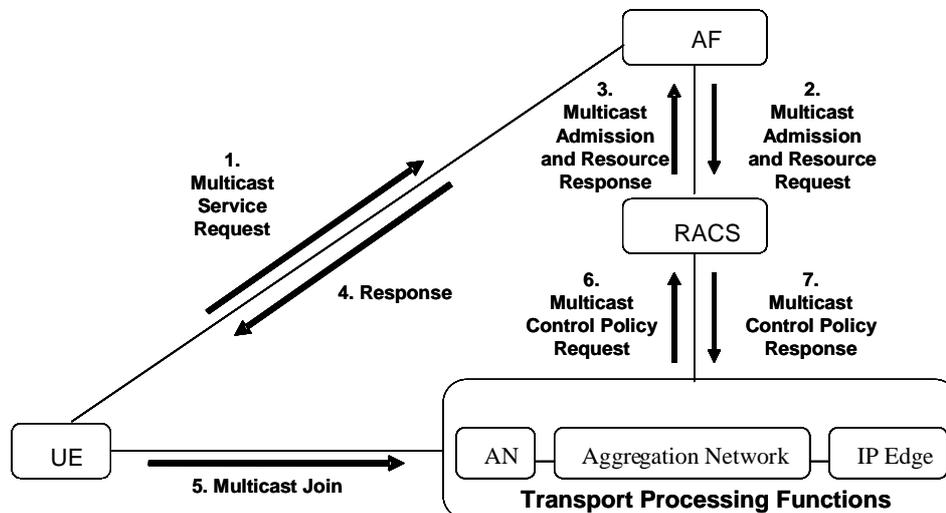

Figure F.2: Multicast in push mode

1) UE requests a multicast service from AF.

2) The AF issues a request to the RACS for multicast admission control and resource reservation.

3) The RACS performs multicast admission control, and resource reservation based on access network policies and resource status. RACS also decides if there are Multicast traffic policies to be installed, and pushes policy enforcement requests to the transport network element(s).

4) The transport network element(s) confirm the installation of the Multicast traffic policies and act according to the policies.

5) The RACS forwards the result of Multicast Admission Control and Resource reservation to the AF.

6) UE receives multicast service response from AF.

7) UE sends a multicast join message to request a multicast flow.

NOTE: RACS may perform admission control and reserve resources using either a centralized or distributed model:

- For a centralized model, RACS needs to maintain the multicast topology, identify and reserve resources and install multicast traffic policies to appropriate network elements.

- For the distributed model, RACS may provide messages to trigger transport network element in order to allow the transport network element to send path coupled signalling (e.g. IGMP) and to reserve resources link by link.

F.3   Scenario for supporting multicast with UE requested QoS policy-pull mode

This scenario supports the model where pull mode is used.

Figure F.3: Multicast with UE requested QoS policy-pull mode

1)   UE requests a multicast service from AF.

2)   The AF issues a request to the RACS for Multicast Admission control and Resource Reservation.

3)   The RACS performs Multicast Admission control and resource reservation based on access network policies and resource status.

4)   UE receives multicast service response from AF (see note).

5)   UE sends an multicast join message to join a multicast group.

6)   The ECF/RCEF in transport network element receives the join message and requests the Multicast traffic policies from RACS.

7)   The RACS confirms the Policy decision, and installs the Multicast traffic policies to the transport network elements.

NOTE: Step 4 may be followed by several sets of steps 5 to 7.

F.4   Scenario for supporting service authorization control when multicast uses the pull mode

This scenario supports the model where pull mode is used, and the RACS perform service authorization control. (including when RACS is implemented in the transport network element).
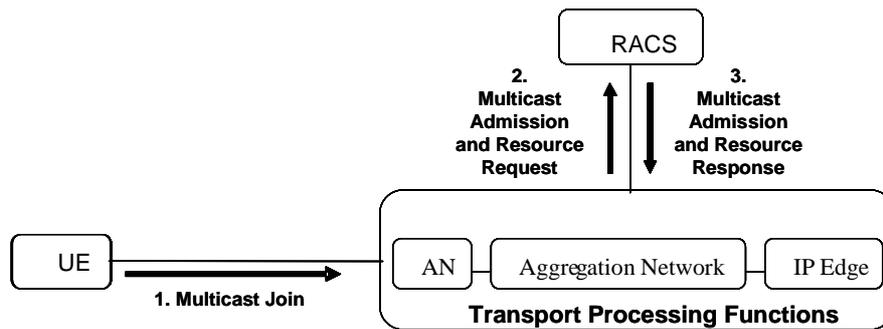
Figure F.4: Service authorization control when multicast uses the pull mode

1) UE sends a multicast join message to request a multicast flow.

2) The ECF/RCEF in transport network element acquires parameters (e.g. QoS and/or gate settings) according to the multicast group received from UE (see note 1), and issues a request to the RACS for multicast admission control and resource reservation (see note 2).

3) The RACS performs (see note 1) multicast admission control and resource reservation based on access network policies and resource status. Then confirms the policy decision, and enforces the Multicast traffic policies to the transport network elements.

NOTE 1: Multicast service authorization control may be performed by RACS either implemented in transport network element or in standalone server which locates outside transport layer.

NOTE 2: Service-based policies involving the SPDF are outside the scope of the present document.

Annex G (informative):
Information flows for supporting unicast and multicast

This annex outlines a number of flow diagrams that represent several unicast and multicast scenarios. The flows are intended to be regarded as informative as they only depict examples of possible solutions for those situations, but do not prevent other implementations.

Moreover, some flows assume functional and architectural capabilities not supported by the present document, which implies unresolved technical issues that are for further study and resolution in a future release. In those cases the flow depicts one of many possible evolution paths of the RACS architecture, and may or may not be supported in a future release once the technical issues are resolved.

G.1   Information flows for supporting unicast

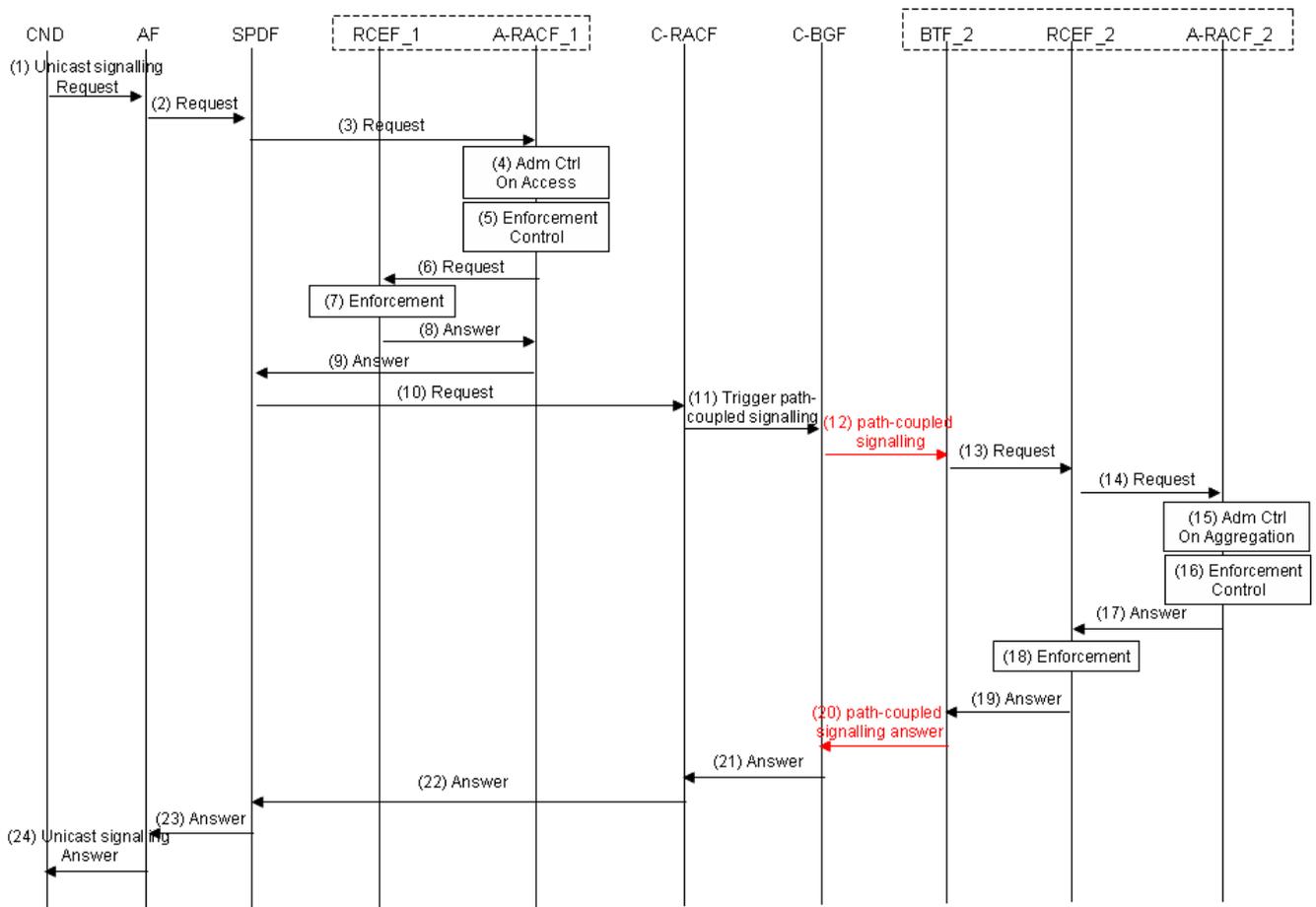## G.1.1   Unicast stream when a A-RACF is present in the AN

This scenario describes Admission Control for Unicast in case an A-RACF is present in AN ad IP_Edge.

In this scenario, it is assumed that:

- The CoD Server is not able to issue a path-coupled signalling.

- Path coupled signalling is triggered by the C-RACF in the C-BGF.

The following functional elements are involved:

- A-RACF_1 is an A-RACF deployed in the AN. A-RACF_1 performs admission control for unicast. Its scope is limited to the access segment.

- RCEF_1 is deployed in the AN.

- A-RACF_2 is an A-RACF deployed in the IP_Edge. A-RACF_2 performs admission control for unicast. Its scope is limited to the aggregation segment.

- RCEF_2 is deployed in the IP_Edge.

- BTF_2 is deployed in the IP_Edge.

Figure G.1: Unicast stream when a A-RACF is present in the AN

NOTE 1: In this scenario, the AF is assumed to be a trusted application.

NOTE 2: C-RACF is not intended to start path-coupled signalling.

1)   CND issues a COD request.

2)   AF triggers the SPDF.

3)   SPDF triggers A-RACF_1.

4)   A-RACF_1 performs admission control in the access.

5)   A-RACF_1 determines the policies to be installed in RCEF_1.

6)   A-RACF_1 communicates the policies to RCEF_1.

7)   RCEF_1 installs the policies.

8)   RCEF_1 answers to A-RACF_1.

9)   A-RACF_1 answers to the SPDF.

10)   SPDF triggers C-RACF.

11)   C-RACF triggers path-coupled signalling.

12)   C-BGF starts path-coupled signalling.

13)   BTF_2 triggers RCEF_2.

14)   RCEF_2 requests admission control and policy decision to A-RACF_2.

15)   A-RACF_2 performs admission control in the aggregation.

16)   A-RACF_2 determines the policies to be installed in RCEF_2.

17)   A-RACF_2 communicates the policies to RCEF_2.

18)   RCEF_2 installs the policies.

19)   RCEF_2 answers to BTF_2.

20)   BTF_2 issues path-coupled signalling to C-BGF.

21)   C-BGF answers to C-RACF.

22)   C-RACF answers to SPDF.

23)   SPDF answers to AF.

24)   AF answers to CND.

G.1.2   Unicast stream when a A-RACF is not present in the AN
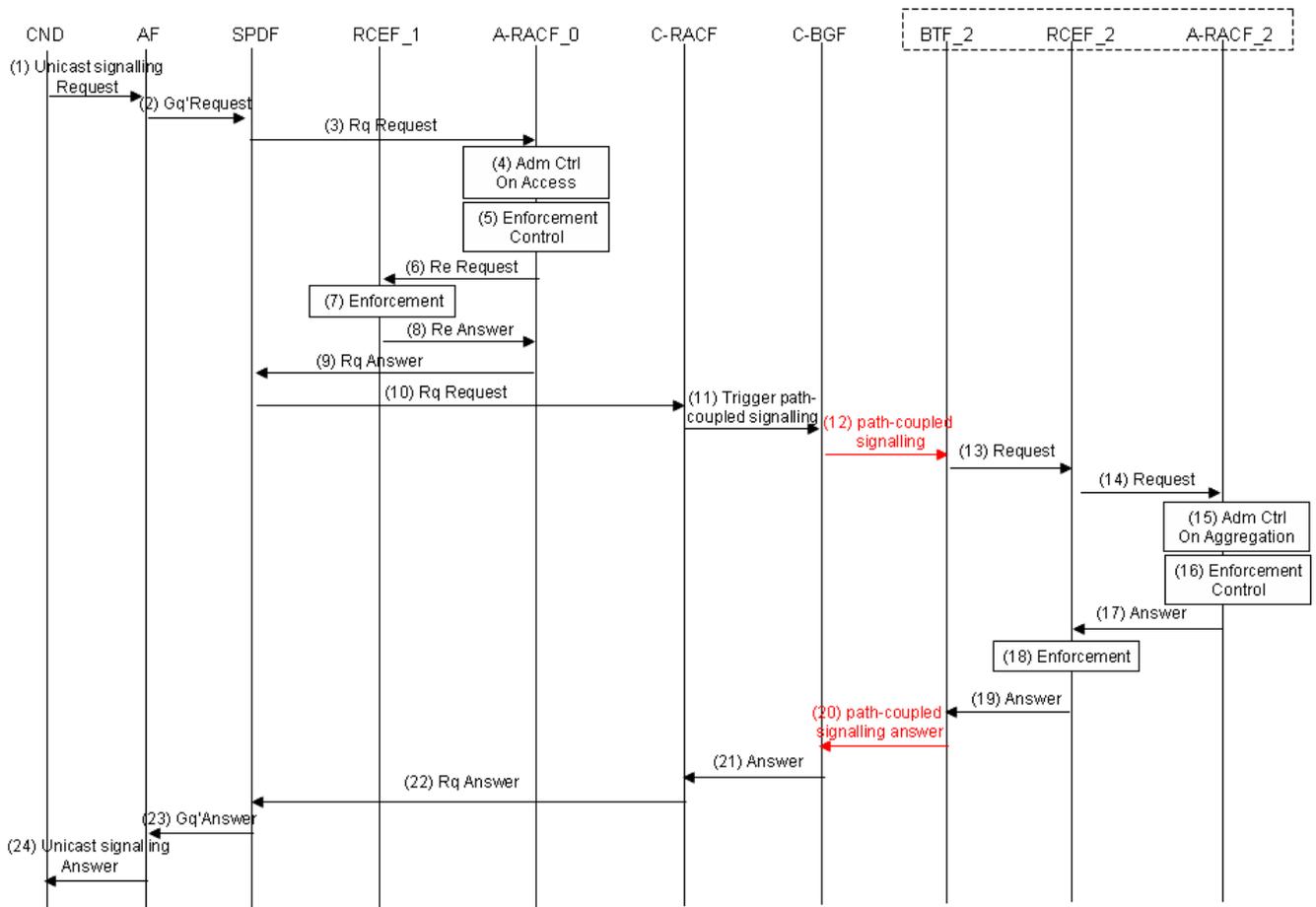
This scenario describes Admission Control for Unicast in case an A-RACF is not present in AN.

In this scenario, it is assumed that:

- The CoD Server is not able to issue a path-coupled signalling.

- Path coupled signalling is triggered by the C-RACF in the C-BGF.

The following functional elements are involved:

- A-RACF_0 is a centralized A-RACF; A-RACF_0 performs admission control for unicast. Its scope is limited to the access segment.

- RCEF_1 is deployed in the AN.

- A-RACF_2 is an A-RACF deployed in the Ip Edge; A-RACF_2 performs admission control for unicast. Its scope is limited to the aggregation segment.

- RCEF_2 is deployed in the IP_Edge.

- BTF_2 is deployed in the IP_Edge.

Figure G.2: Unicast stream when a A-RACF is not present in the AN

NOTE 1: In this scenario, the AF is assumed to be a trusted application.

NOTE 2: C-RACF is not intended to start path-coupled signalling.

1)   CND issues a COD request.

2)   AF triggers the SPDF.

3)   SPDF triggers A-RACF_0.

4)   A-RACF_0 performs admission control in the access.

5)   A-RACF_0 determines the policies to be installed in RCEF_1.

6)   A-RACF_0 communicates the policies to RCEF_1.

7)   RCEF_1 installs the policies.

8)   RCEF_1 answers to A-RACF_0.

9)   A-RACF_0 answers to the SPDF.

10)   SPDF triggers C-RACF.

11)   C-RACF triggers path-coupled signalling.

12)   C-BGF starts path-coupled signalling.

13)   BTF_2 triggers RCEF_2.

14)   RCEF_2 requests admission control and policy decision to A-RACF_2.

15)   A-RACF_2 performs admission control in the aggregation.

16)   A-RACF_2 determines the policies to be installed in RCEF_2.

17)   A-RACF_2 communicates the policies to RCEF_2.

18)   RCEF_2 installs the policies.

19)   RCEF_2 answers to BTF_2.

20)   BTF_2 issues path-coupled signalling to C-BGF.

21)   C-BGF answers to C-RACF.

22)   C-RACF answers to SPDF.

23)   23.SPDF answers to AF.

24)   AF answers to CND.

G.1.3   Unicast stream when multiple x-RACF instances are present

The Rr Reference Point allows x-RACF instances to synchronize with each others.

The following functional elements are involved:

- A-RACF_1 has a scope spanning the Access and Aggregation Segments.

- X-RACF_2 has a scope spanning the Metro Segment.

The corresponding signalling flow for a Unicast request is represented below:
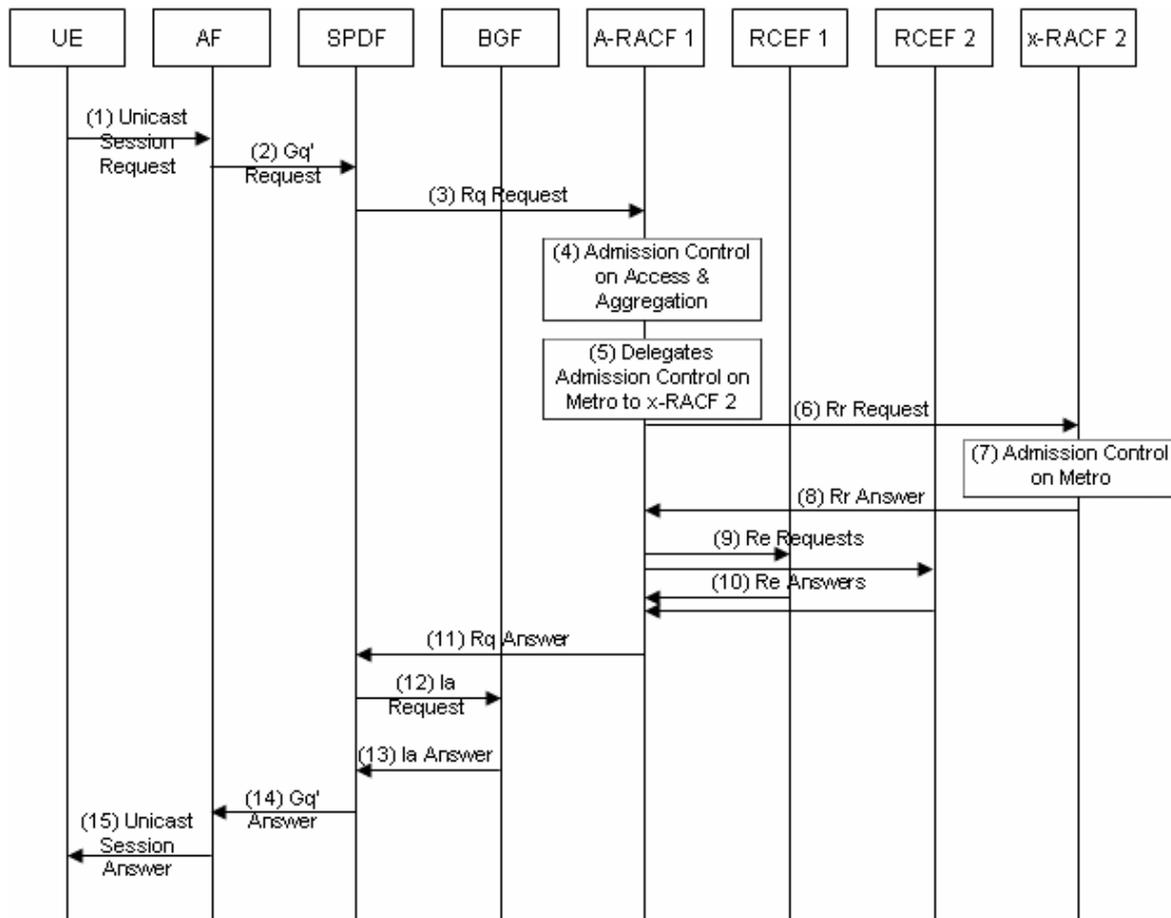
Figure G.3: Unicast stream when multiple x-RACF instances are present

NOTE: The above flow uses the single-stage reservation model.

1)   The AF receives a Unicast Signalling Request.

2)   The AF contacts the SPDF.

3)   From the point of view of the SPDF, a single x-RACF instance is visible: this is A-RACF_1. This simplifies
       the dispatching decision, since the SPDF only needs to be aware of A-RACF_1. For this reason, the SPDF
       contacts A-RACF_1.

4)   A-RACF_11 performs admission control for the Access and Aggregation segments.

5) and 6) A-RACF_1 then delegates admission control for the Metro Segment to x-RACF_2.

7)   x-RACF_2 verifies the resource availability in the Metro Segment.

8)   x-RACF_2 returns its decision to A-RACF_1. (Assumed to be granted in this example signalling flow).

9) and 10)   Policy Enforcement.

11)   A-RACF_1 returns a single answer to the SPDF Assumed to be granted in this example signalling flow).

12) and 13)   SPDF interacts with the BGF.

14)   SPDF returns the answer to the AF.

15)   The AF returns the answers to the UE.

# G.2   Information flows for enabling and disabling the multicast service

G.2.1   Control flow for enabling multicast service

A service package is a set of elementary services - an elementary service is for instance a multicast channel, interactive channel, mosaic - that a user may subscribe to. All service elements (e.g. channels) in one service package take the same service authorization and charging policy.

> NOTE 1: Service package has been described in TS 182 027 [15], clause 7.1. Here the service package takes the same definition but applies to not only IMS-based IPTV but also non IMS-based IPTV multicast service.

The following flow shows the procedure for enabling multicast service in RACS. The AF activates the service package via RACS, and then the UE initiates multicast request messages for joining/leaving channels within the service package.

> NOTE 2: This information flow only applies to access and aggregation network.
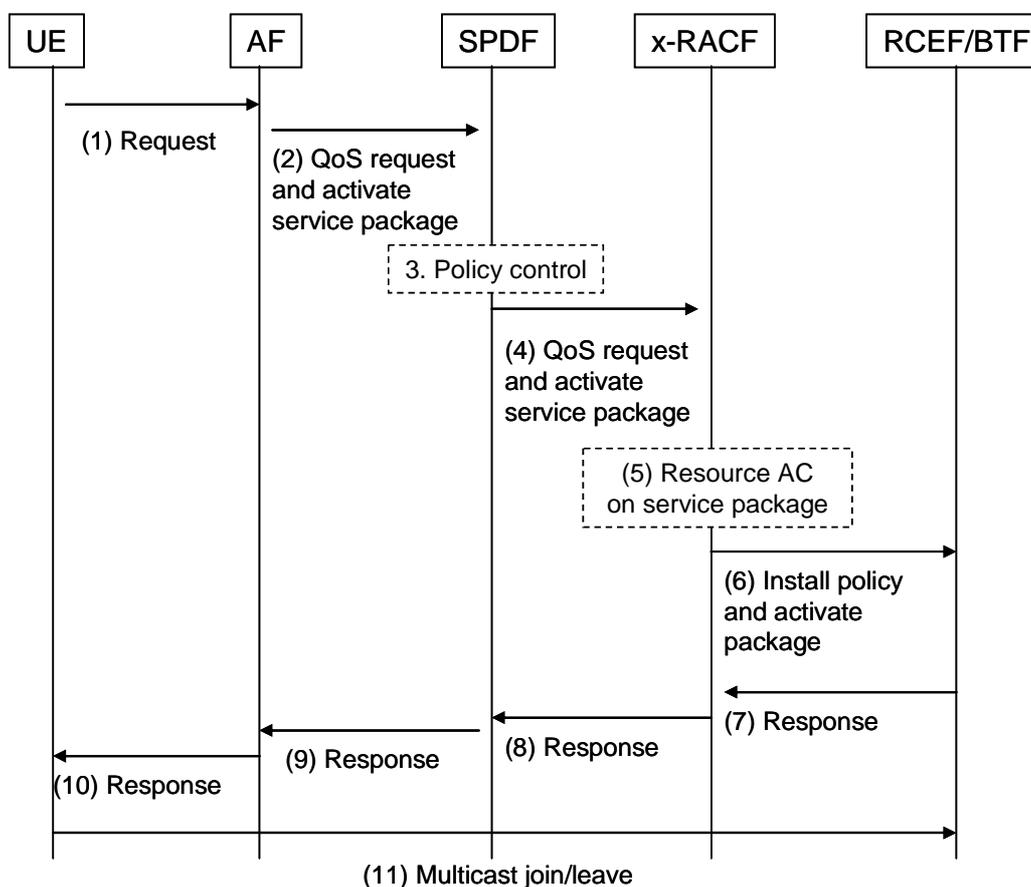
Figure G.4: Enable of the multicast service

1)   The UE initiates a session request to one service package which contains one or more multicast flows.

2)   AF authorizes and accepts the request, and sends request to SPDF to request network resource and meantime indicate SPDF to activate the service package for the UE.

3)   SPDF performs service-based policy control on the service package.

4)   SPDF sends request to x-RACF to reserve resource and activate the service package.

5)   x-RACF may performs resource admission control on both access and aggregation segment for the service package. (e.g. x-RACF may reserve the summed bandwidth of all channels contained in the service package in aggregation segment and the maximum bandwidth among the channels in access segment).

6) x-RACF contacts RCEF/BTF in transport node to install policies and activate the service package.

7) RCEF/BTF sends response to x-RACF.

8) x-RACF sends response to SPDF.

9) SPDF sends response to AF.

10) AF sends response to UE to inform it that the requested service package can be consumed.

11) UE initiates multicast join/leave request messages to consume the channels within the service package.

NOTE 1: Step 5 is optional because admission control may also be performed using Pull mode.

NOTE 2: Step 6 is optional because operator may also select x-RACF in a stand alone server to perform multicast service authorization control.

NOTE 3: This flow does not regulate how to do channel changing.

G.2.2 Control flow for disabling multicast service

The following flow shows the procedure for disabling multicast service in RACS. The AF deactivates the service package via RACS.
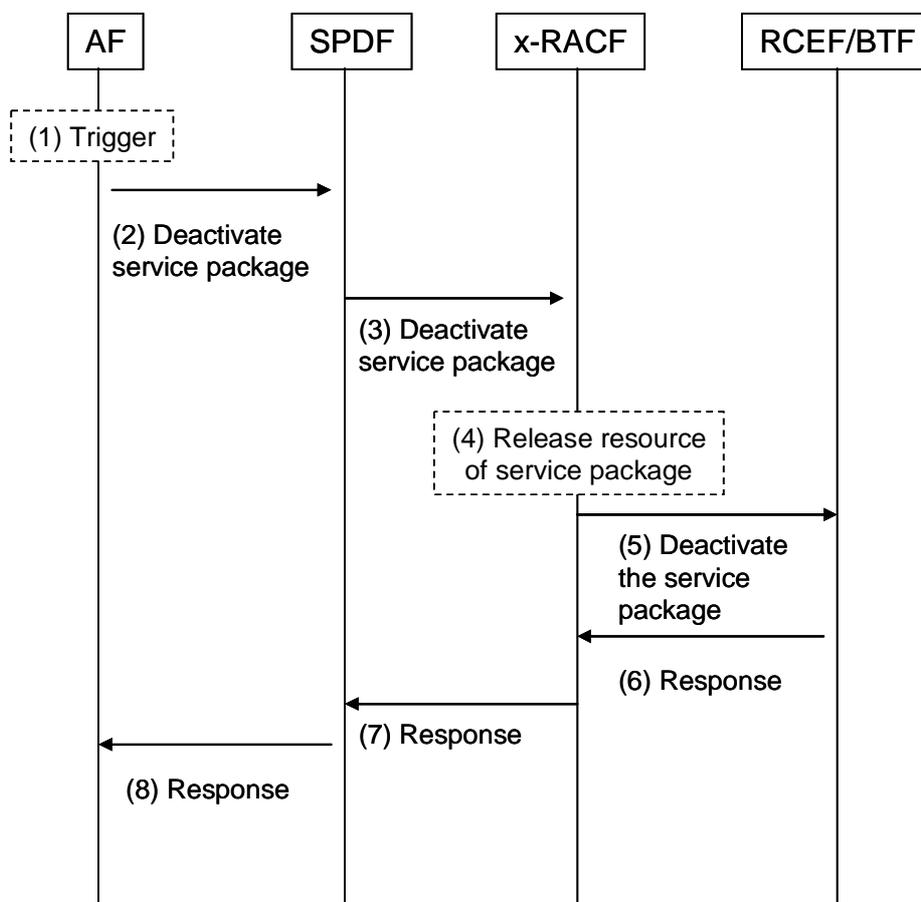
Figure G.5: Disable of the multicast service

1) AF gets a trigger to disable one service package of one user (e.g. user request or session keep-alive test failed).

2) AF sends request to SPDF to deactivate the service package of the user.

3) SPDF sends request to x-RACF to deactivate the service package.

4) x-RACF authorizes the request and release related resource of access/aggregation segment.

NOTE: For aggregation segment, x-RACF does not release the resource when there are other user consuming the same service package.

5)   x-RACF contacts RCEF/BTF in transport element to deactivate the service package of the user.

6)   RCEF/BTF deactivates the service package for the user and responses to x-RACF.

7)   x-RACF sends response to SPDF.

8)   SPDF send response to AF.

G.3   Information flows for supporting multicast in pull mode

The information flows in this clause of this annex have been recognized as technically correct. For the next releases, the issue to be resolved for allowing the contents of this clause to be inserted in the normative text is the clarification of the relationships between the elementary functions and the functional entities involved and the physical nodes (AN and IP_Edge).

G.3.1   Request Resource in the pull mode

This clause provides an example of how a request for resources can be performed by using the pull mode mechanism.
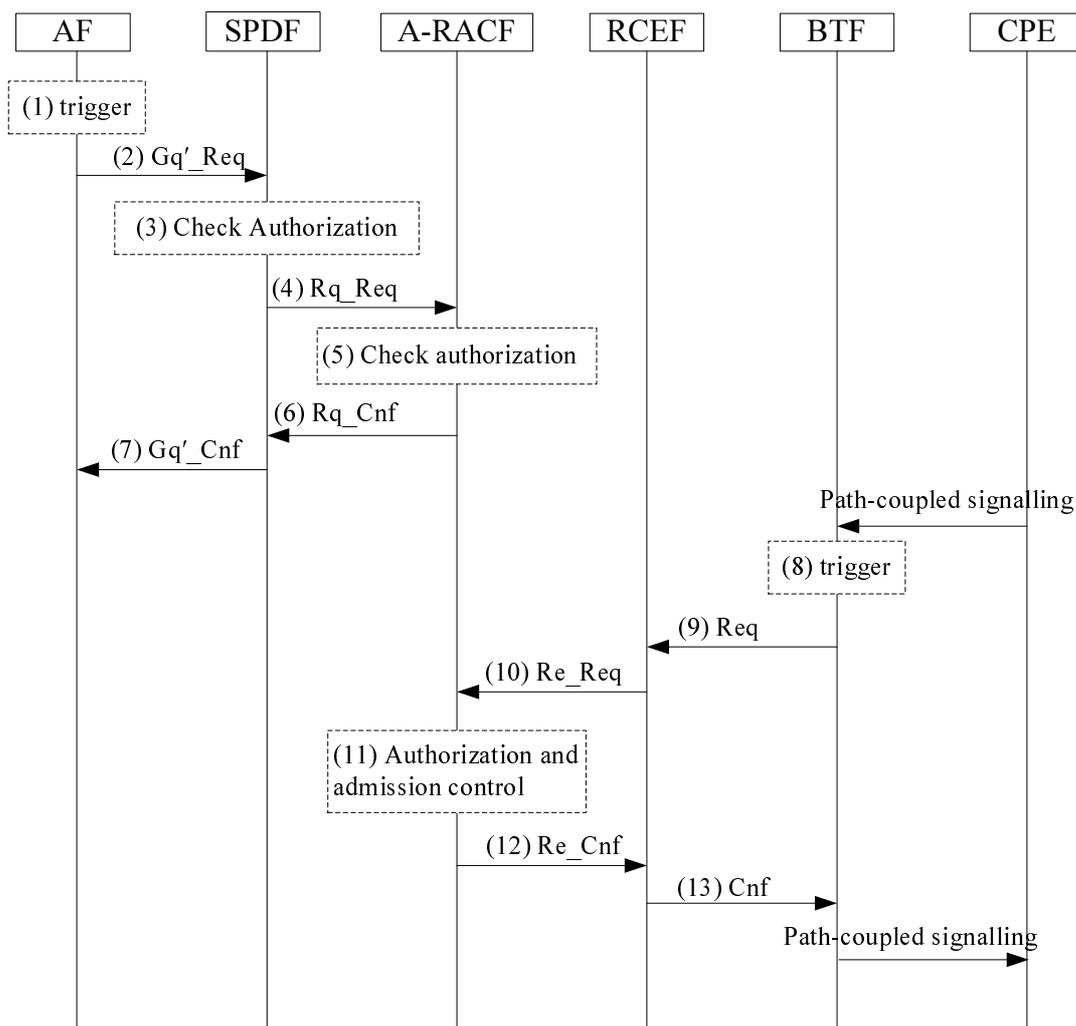

Figure G.6: Request resource (Pull Mode)

1) The resource initiation request is usually triggered by a service establishment signalling message.

2) The AF sends a service request to the SPDF.

3) The SPDF authorizes the request. This process consists of verifying if the required resources, present in the service request, are consistent with operator policy rules defined in the SPDF for that particular AF.

4) In case the service is authorized, the SPDF determines how to serve the request. It may be required to send the request to allocated resources of the A-RACF. The SPDF uses the local policies and the parameters in the request in order to take the decision.

5) The A-RACF maps the request from the SPDF into the internal network topology. The A-RACF performs authorization based on access network policies.

6) If the resources are authorized, the A-RACF confirms the operation to the SPDF.

7) The SPDF forwards the result to the AF.

8) The CPN initiates an explicit request for resource reservation directly to the transport functions through a dedicated path-coupled transport signalling. A resource decision request is usually triggered by a request indicated through the signalling from the CPN to reserve the required QoS resource for a given flow.

9) The BTF forwards the request to the RCEF. The BTF shall be able to filter duplicate or malicious request messages, especially if the transport signalling is refreshed periodically.

10) Based on the request from the BTF, the RCEF sends a request to the A-RACF to pull the admission control decisions from it.

11) The A-RACF checks the authorization, and evaluates the availability, if successful, reserves resources.

12) The A-RACF shall confirm the operation to the RCEF.

13) The RCEF sends the response to the BTF.

G.3.2 Multicast stream in pull mode when a A-RACF is present in the AN

This scenario describes Admission Control for Multicast in case an A-RACF is present in AN.

In this scenario, it is assumed that the content is present in the IP_Edge. If the content is in the AN steps 9 to 18 are not required.

The following functional elements are involved:

- A-RACF_1 is an A-RACF deployed in the AN. A-RACF_1 performs admission control for multicast. Its scope is limited to the access segment.

- RCEF_1 is deployed in the AN.

- BTF_1 is deployed in the AN.

- A-RACF_2 is an A-RACF deployed in the IP_Edge. A-RACF_2 performs admission control for multicast. Its scope is limited to the aggregation segment.

- RCEF_2 is deployed in the IP_Edge.

- BTF_2 is deployed in the IP_Edge.
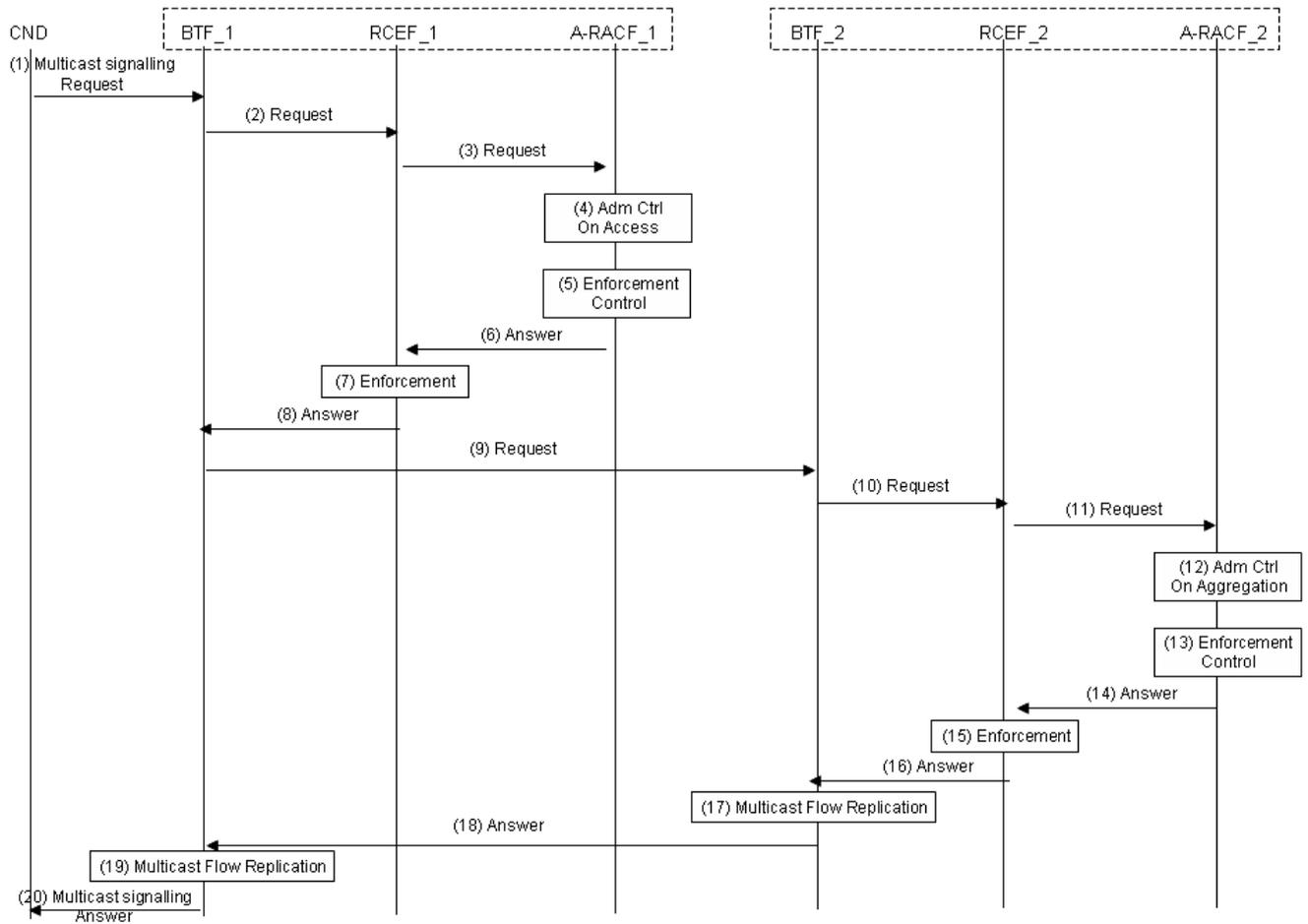
Figure G.7: Multicast stream in pull mode when a A-RACF is present in the AN

1)   CND issues a BC request.

2)   BTF_1 triggers RCEF_1.

3)   RCEF_1 requests admission control and policy decision to A-RACF_1.

4)   A-RACF_1 performs admission control in the access.

5)   A-RACF_1 determines the policies to be installed in RCEF_1.

6)   A-RACF_1 communicates the policies to RCEF_1.

7)   RCEF_1 installs the policies.

8)   RCEF_1 answers to BTF_1.

9)   BTF_1 triggers BTF_2.

10)   BTF_2 triggers RCEF_2.

11)   RCEF_2 requests admission control and policy decision to A-RACF_2.

12)   A-RACF_2 performs admission control in the aggregation.

13)   A-RACF_2 determines the policies to be installed in RCEF_2.

14)   A-RACF_2 communicates the policies to RCEF_2.

15)   RCEF_2 installs the policies.

16)   RCEF_2 answers to BTF_2.

17) BTF_2 replicates the flow.

18) BTF_2 answers to BTF_1.

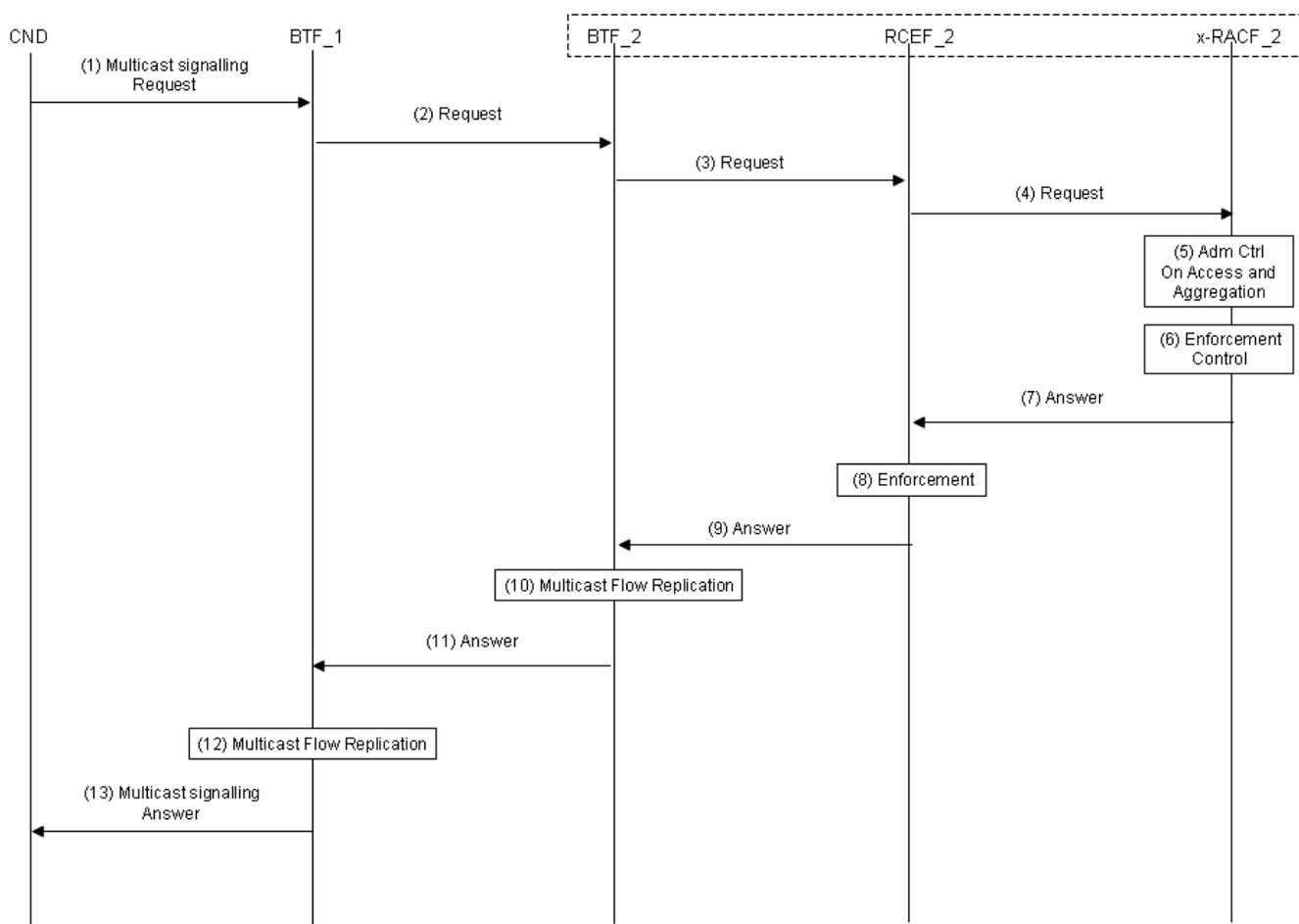19) BTF_1 replicates the flow.

20) BTF_1 answers to CND.

G.3.3   Multicast stream in pull mode when a A-RACF is not present in the AN and the content is in the IP_Edge

This scenario describes Admission Control for Multicast in case an A-RACF is not present in AN and the content is in the IP_Edge.

In this scenario, it is assumed that the content is present in the IP_Edge.

The following functional elements are involved:

- BTF_1 is deployed in the AN.

- A-RACF_2 is an A-RACF deployed in the IP_Edge. A-RACF_2 performs admission control for multicast. Its scope spans both access and aggregation segment.

- RCEF_2 is deployed in the IP_Edge.

- BTF_2 is deployed in the IP_Edge.

Figure G.8: Multicast stream in pull mode when a A-RACF is not present in the AN and the content is in the IP_Edge

1)   CND issues a BC request.

2)   BTF_1 triggers BTF_2.

3)   BTF_2 triggers RCEF_2.

4)   RCEF_2 requests admission control and policy decision to A-RACF_2.

5)   A-RACF_2 performs admission control in the access and in the aggregation.

6)   A-RACF_2 determines the policies to be installed in RCEF_2.

7)   A-RACF_2 communicates the policies to RCEF_2.

8)   RCEF_2 installs the policies.

9)   RCEF_2 answers to BTF_2.

10)   BTF_2 replicates the flow.

11)   BTF_2 answers to BTF_1.

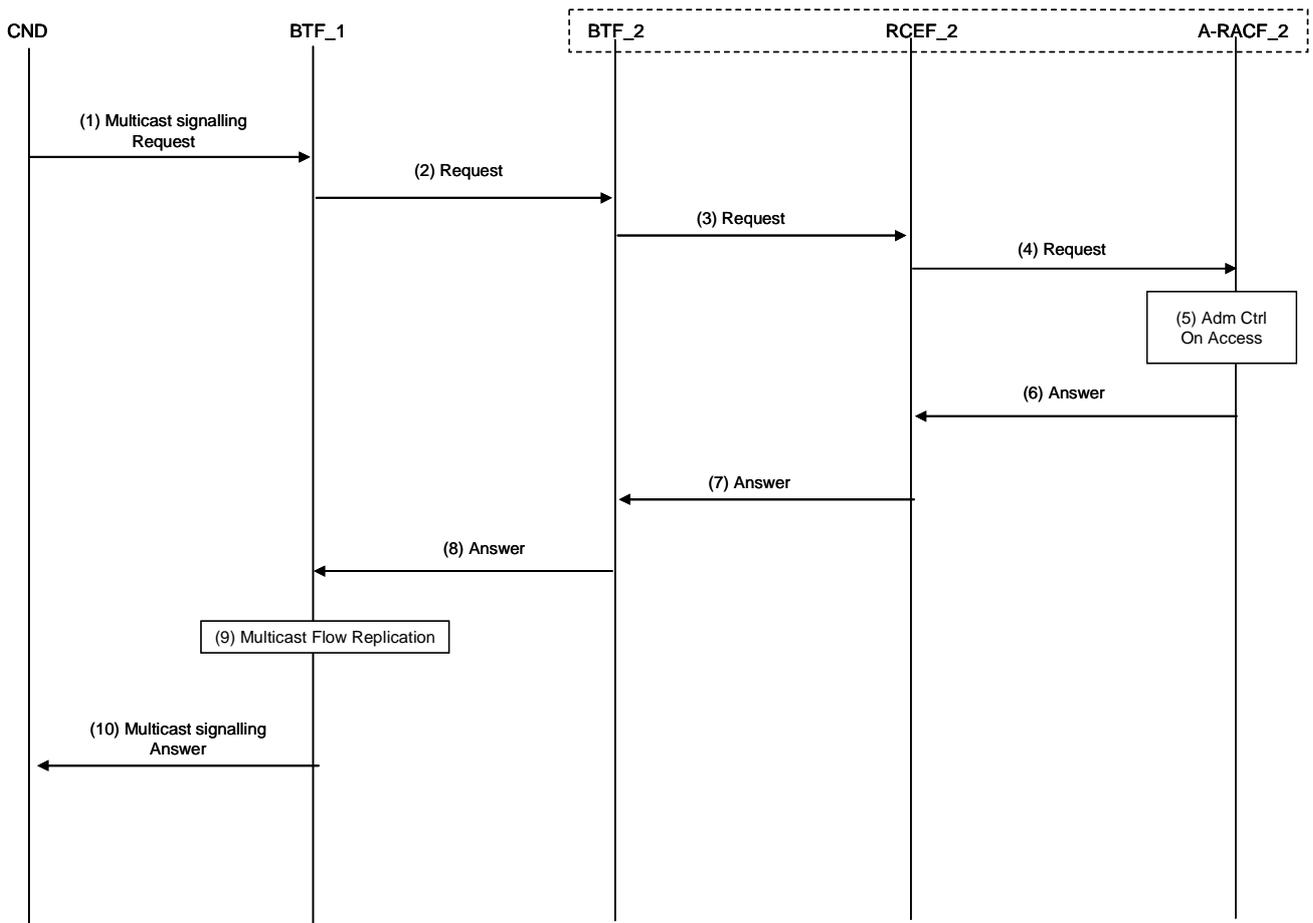12)   BTF_1 replicates the flow.

13)   BTF_1 answers to CND.

G.3.4   Multicast stream in pull mode when a A-RACF is not present in the AN and the content is in the AN

This scenario describes Admission Control for Multicast in case an A-RACF is not present in AN and the content is in the AN.

In this scenario, it is assumed that the content is present in the AN.

The following functional elements are involved:

- BTF_1 is deployed in the AN.

- A-RACF_2 is an A-RACF deployed in the IP_Edge. A-RACF_2 performs admission control for multicast. Its scope spans both access and aggregation segment.

- RCEF_2 is deployed in the IP_Edge.

- BTF_2 is deployed in the IP_Edge.

**Figure G.9: Multicast stream in pull mode when a A-RACF is not present
in the AN and the content is in the AN**

1)   CND issues a COD request.

2)   BTF_1 triggers BTF_2.

3)   BTF_2 triggers RCEF_2.

4)   RCEF_2 requests admission control to A-RACF_2.

5)   A-RACF_2 performs admission control in the access.

6)   A-RACF_2 answers to RCEF_2.

7)   RCEF_2 answers to BTF_2.

8)   BTF_2 answers to BTF_1.

9)   BTF_1 replicates the flow.

10)   BTF_1 answers to CND.

G.3.5   Multicast Admission Control for the Access Segment only

In this scenario, Multicast content is pre-distributed up to the Access Node.

The following functional entities are involved:

- A-RACF_1 is an A-RACF deployed in the AN. A-RACF_1 performs Admission Control for Multicast only. Its scope spans the Multicast resources in Access Segment.

- RCEF_1 is deployed in the AN.

- BTF_1 is deployed in the AN.

NOTE: The interactions between BTF_1, RCEF_1 and A-RACF_1 are internal and may be different from illustrated.

The signalling flow for a Multicast Request is illustrated in the figure below (internal interactions are illustrated as dashed lines):
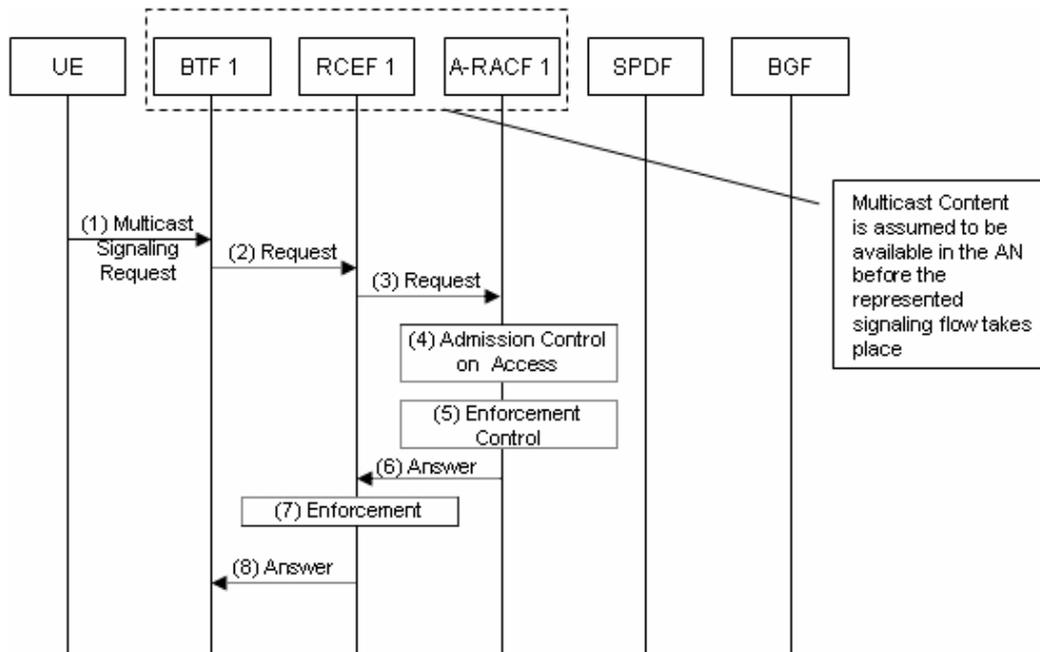
Figure G.10: Multicast Admission Control for the Access Segment only

1)   BTF_1 receives a multicast signalling request.

2)   BTF_1 triggers RCEF_1.

3)   RCEF_1 requests a Policy Decision from A-RACF_1.

4)   A-RACF_1 performs Admission Control on the Access Segment.

5)   A-RACF_1 determines the Policy to be installed on RCEF_1.

6)   A-RACF_1 answers to RCEF_1.

7)   RCEF_1 installs the policy.

8)   RCEF_1 answers to BTF_1.

G.3.6   Multicast Admission Control when the maximum bandwidth associated with Multicast service is over-provisioned in the aggregation segment and beyond

In this scenario, it is assumed that:

- Multicast content is not pre-distributed up to the Access Node.

- Admission Control for Resources for the Multicast service does not need to be performed in the Aggregation segment or beyond. This may be the case, for example, if the maximum bandwidth associated with Multicast service is over-provisioned in the aggregation segment and beyond.

The following functional entities are involved:

- A-RACF_1 is an A-RACF deployed on the AN. A-RACF_1 performs Admission Control for Multicast only. Its scope spans the Multicast resources in Access Segment.

- RCEF_1 is deployed in the AN.

- BTF_1 is deployed in the AN.

- RCEF_2 is deployed in the IP_Edge.

- BTF_2 is deployed in the IP_Edge.

NOTE 1: The interactions between BTF_1, RCEF_1 and A-RACF_1 are internal, and may be different from the illustrated.

NOTE 2: The interactions between BTF_2 and RCEF_2 are internal, and may be different from the illustrated.

The signalling flow for a Multicast Request is illustrated in the figure below (internal interactions are illustrated as dashed lines):
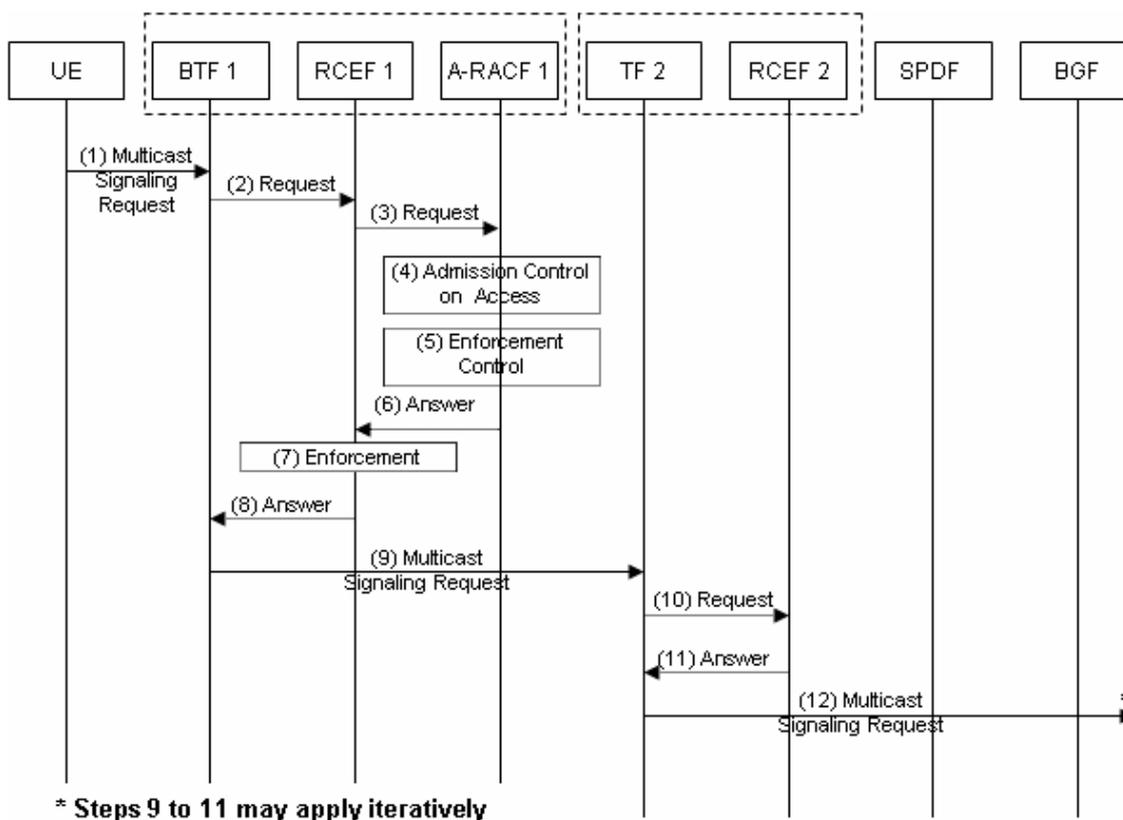
Figure G.11: Multicast Admission Control when the maximum bandwidth associated with Multicast service is over-provisioned in the aggregation segment and beyond

1) BTF_1 receives a multicast signalling request.

2) BTF_1 triggers RCEF_1.

3) RCEF_1 requests a Policy Decision from A-RACF_1.

4) A-RACF_1 performs Admission Control on the Access Segment.

5) A-RACF_1 determines the Policy to be installed on RCEF_1.

6) A-RACF_1 answers to RCEF_1.

7) RCEF_1 installs the policy.

8)   RCEF_1 answers to BTF_1.

9)   BTF_1 forwards the multicast signalling request to BTF_2.

10) BTF_2 triggers RCEF_2. The corresponding policy is assumed to be present in RCEF_2.

11) RCEF_2 answers to BTF_2.

12) If needed, BTF_2 forwards the multicast signalling request to the next BTF. Steps 9, 10 and 11 may be applied iteratively.

G.4   Information flows for supporting multicast in mixed push and pull mode

The information flows in this clause have been recognized as technically correct. For the next releases the issue to be resolved for allowing the contents of this clause to be inserted in the normative text is the clarification of the relationships between the elementary functions and the functional entities involved and the physical nodes (AN and IP_Edge).
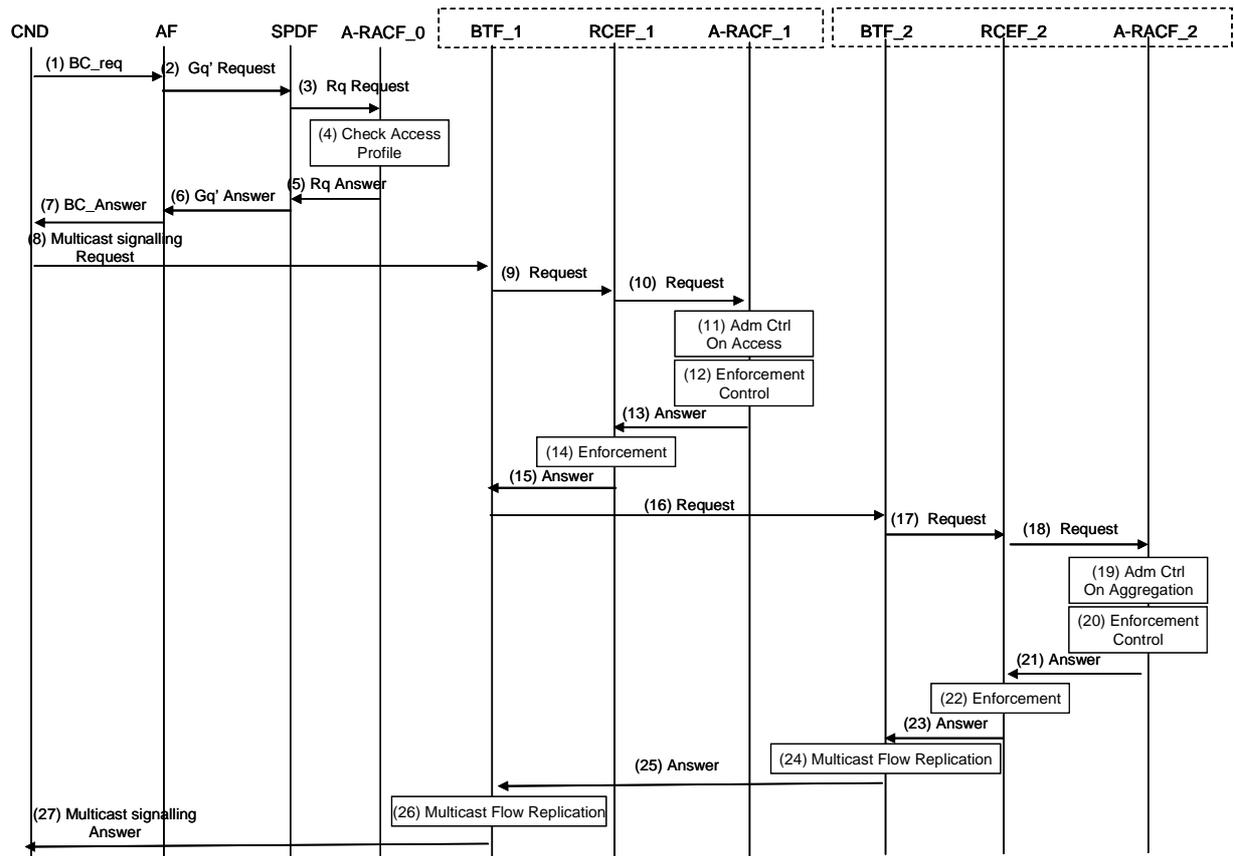
G.4.1   Multicast stream in mixed push and pull mode when a A-RACF is present in the AN

This scenario describes Admission Control for Multicast in mixed push and pull mode in case an A-RACF is present in AN and the content is in the IP_Edge

In this scenario, it is assumed that the content is present in the IP_Edge. If the content is in the AN steps from 16 to 25 are not required.

The following functional elements are involved:

- A-RACF_0 is a centralized A-RACF; A-RACF_0 performs the authorization of the request by checking the access profile.

- A-RACF_1 is an A-RACF deployed in the AN. A-RACF_1 performs admission control for multicast. Its scope is limited to the access segment.

- RCEF_1 is deployed in the AN.

- BTF_1 is deployed in the AN.

- A-RACF_2 is an A-RACF deployed in the Ip_Edge; A-RACF_2 performs admission control for multicast. Its scope is limited to the aggregation segment.

- RCEF_2 is deployed in the IP_Edge.

- BTF_2 is deployed in the IP_Edge.

Figure G.12: Multicast stream in mixed push and pull mode when a A-RACF is present in the AN

NOTE: In this scenario, the AF is assumed to be a trusted application.

1)   CND issues a BC request.

2)   AF triggers the SPDF.

3)   SPDF triggers A-RACF_0.

4)   A-RACF_0 authorizes the request by checking the access profile.

5)   A-RACF_0 answers to the SPDF.

6)   SPDF answers to the AF.

7)   AF answers to the CND.

8)   CDN issues a Multicast signalling Request.

9)   BTF_1 triggers RCEF_1.

10)   RCEF_1 requests admission control and policy decision to A-RACF_1.

11)   A-RACF_1 performs admission control in the access.

12)   A-RACF_1 determines the policies to be installed in RCEF_1.

13)   A-RACF_1 communicates the policies to RCEF_1.

14)   RCEF_1 installs the policies.
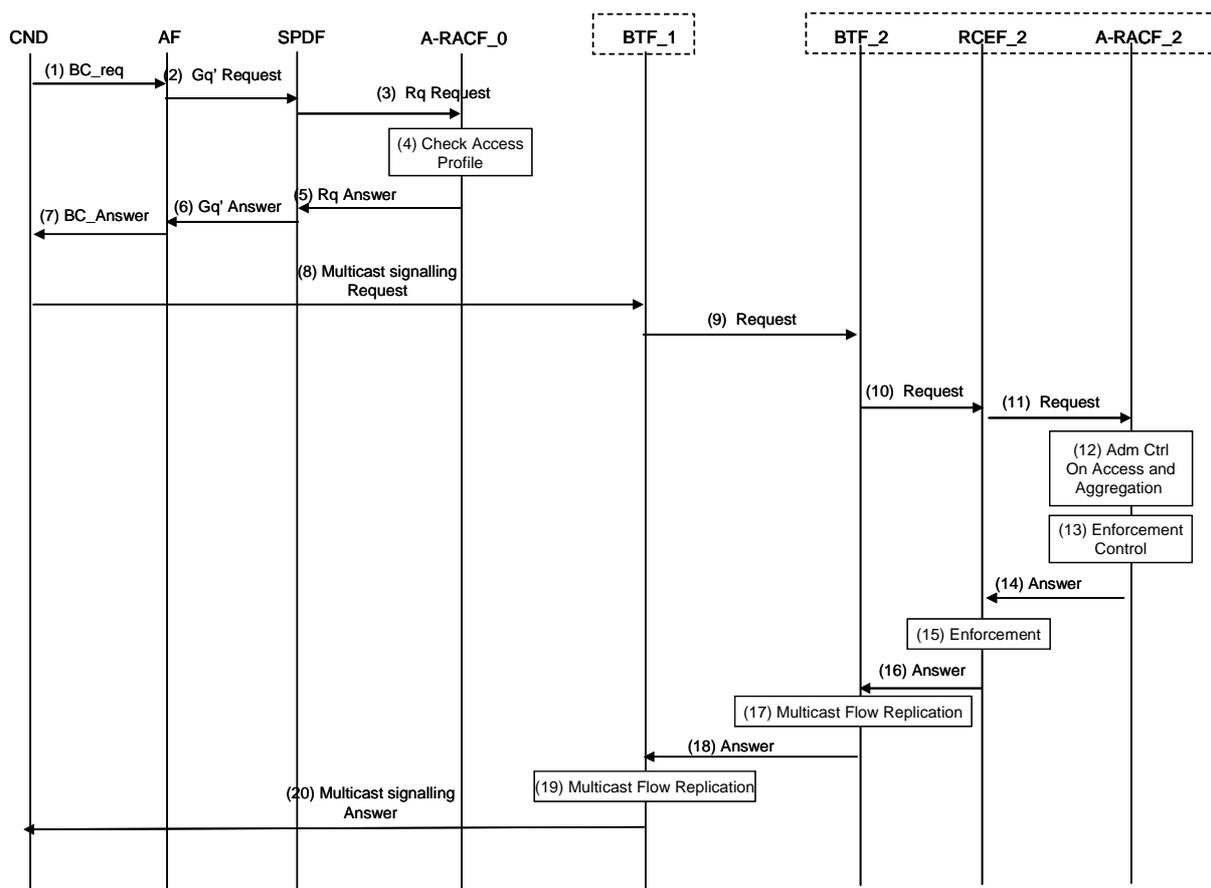
15)   RCEF_1 answers to BTF_1.

16)   BTF_1 triggers BTF_2.

17) BTF_2 triggers RCEF_2.

18) RCEF_2 requests admission control and policy decision to A-RACF_2.

19) A-RACF_2 performs admission control in the aggregation.

20) A-RACF_2 determines the policies to be installed in RCEF_2.

21) A-RACF_2 communicates the policies to RCEF_2.

22) RCEF_2 installs the policies.

23) RCEF_2 answers to BTF_2.

24) BTF_2 replicates the flow.

25) BTF_2 answers to BTF_1.

26) BTF_1 replicates the flow.

27) BTF_1 answers to CND.

G.4.2   Multicast stream in mixed push and pull mode when a A-RACF is not present in the AN and the content is in the IP_Edge

This scenario describes Admission Control for Multicast in mixed push and pull mode in case an A-RACF is not present in AN and the content is in the IP_Edge. In this scenario, it is assumed that the content is present in the IP_Edge.

The following functional elements are involved:

- A-RACF_0 is a centralized A-RACF; A-RACF_0 performs the check of the access profile.

- BTF_1 is deployed in the AN.

- A-RACF_2 is an A-RACF deployed in the Ip Edge; A-RACF_2 performs admission control for multicast. Its scope spans both access and aggregation segment.

- RCEF_2 is deployed in the IP_Edge.

- BTF_2 is deployed in the IP_Edge.

**Figure G.13: Multicast stream in mixed push and pull mode
when a A-RACF is not present in the AN**

NOTE: In this scenario, the AF is assumed to be a trusted application.

1)   CND issues a BC request.

2)   AF triggers the SPDF.

3)   SPDF triggers A-RACF_0.

4)   A-RACF_0 performs the check of the access profile.

5)   A-RACF_0 answers to the SPDF.

6)   SPDF answers to the AF.

7)   AF answers to the CND.

8)   CDN issues a Multicast signalling Request.

9)   BTF_1 triggers BTF_2.

10)   BTF_2 triggers RCEF_2.

11)   RCEF_2 requests admission control and policy decision to A-RACF_2.

12)   A-RACF_2 performs admission control in the access and in the aggregation.

13)   A-RACF_2 determines the policies to be installed in RCEF_2.

14)   A-RACF_2 communicates the policies to RCEF_2.

15)   RCEF_2 installs the policies.

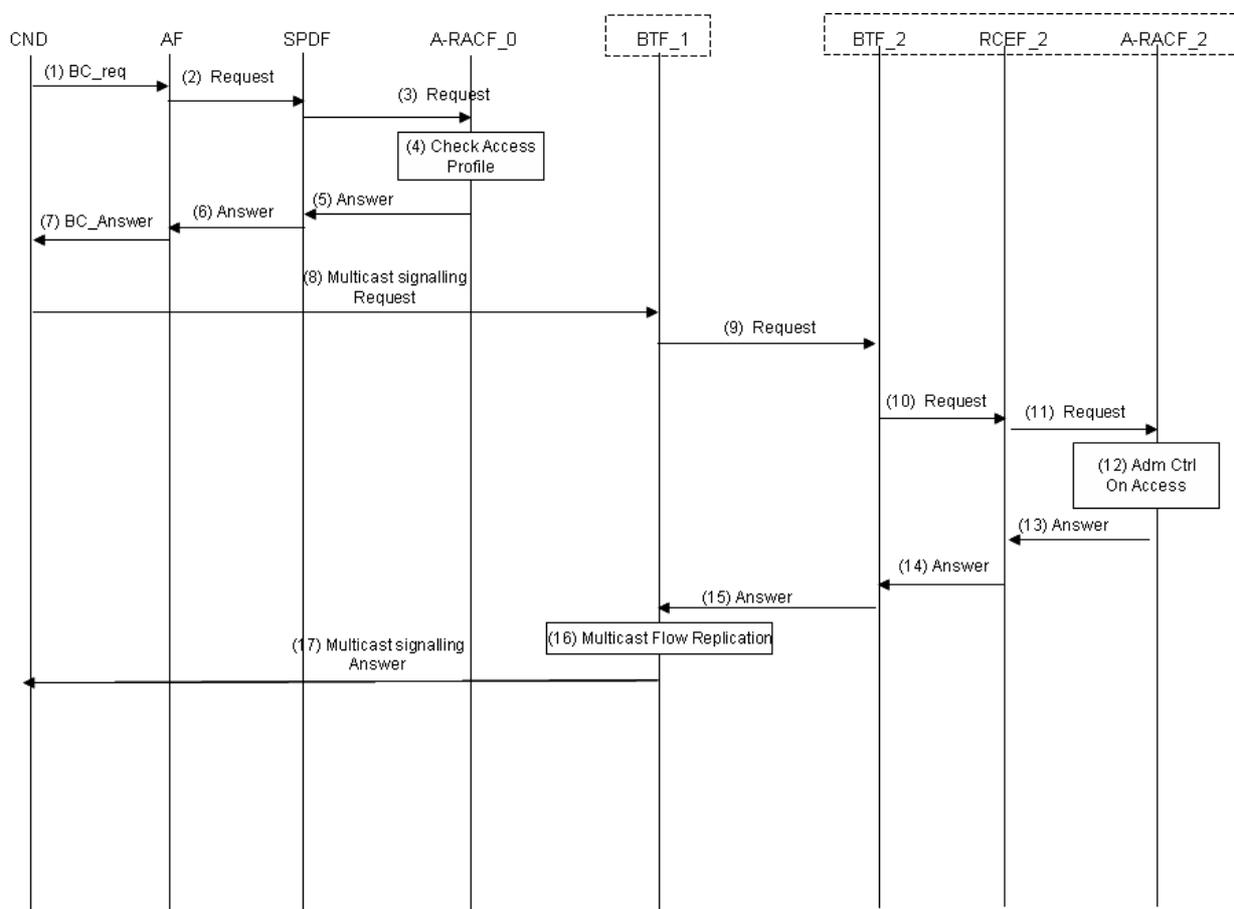16) RCEF_2 answers to BTF_2.

17) BTF_2 replicates the flow.

18) BTF_2 answers to BTF_1.

19) BTF_1 replicates the flow.

20) BTF_1 answers to CND.

G.4.3 Multicast stream in mixed push and pull mode when a A-RACF is not present in the AN and the content is in the AN

This scenario describes Admission Control for Multicast in mixed push and pull mode in case an A-RACF is not present in AN and the content is in the AN. In this scenario, it is assumed that the content is present in the AN.

The following functional elements are involved:

- A-RACF_0 is a centralized A-RACF; A-RACF_0 performs the check of the access profile.BTF_1 is deployed in the AN.

- A-RACF_2 is an A-RACF deployed in the Ip Edge; A-RACF_2 performs admission control for multicast. Its scope is limited to the access segment.

- RCEF_2 is deployed in the IP_Edge.

- BTF_2 is deployed in the IP_Edge.

**Figure G.14: Multicast stream in mixed push and pull mode
when a A-RACF is not present in the AN and the content is in the AN**

NOTE: In this scenario, the AF is assumed to be a trusted application.

1) CND issues a BC request.

2) AF triggers the SPDF.

3) SPDF triggers A-RACF_0.

4) A-RACF_0 performs the check of the access profile.

5) A-RACF_0 answers to the SPDF.

6) SPDF answers to the AF.

7) AF answers to the CND.

8) CDN issues a Multicast signalling Request.

9) BTF_1 triggers BTF_2.

10) BTF_2 triggers RCEF_2.

11) RCEF_2 requests admission control to A-RACF_2.

12) A-RACF_2 performs admission control in the access.

13) A-RACF_2 answers to the RCEF_2.

14) RCEF_2 answers to BTF_2.

15) BTF_2 answers to BTF_1.

16) BTF_1 replicates the flow.

17) BTF_1 answers to CND.

G.5   Information flows for supporting combined unicast and multicast together with resource handling

G.5.1   Unicast and multicast services do NOT share resources on the Access Segment

This scenario describes Admission Control for Unicast and Multicast, in case Multicast and Unicast do not share the same resources in the Access Segment.

In this scenario, it is assumed that:

- Unicast and Multicast service are associated with dedicated transport resources in the Access segment.

- Unicast and Multicast service are associated with dedicated transport resources in the Access segment.

The following functional elements are involved:

- A-RACF_1 is an A-RACF deployed in the AN. A-RACF_1 performs Admission Control for Multicast only. Its scope is limited to the Multicast resources in Access Segment.

- RCEF_1 is deployed in the AN.

- BTF_1 is deployed in the AN.

- RCEF_2 is deployed in the IP_Edge.

- BTF_2 is deployed in the IP_Edge.

- A-RACF_0 is an A-RACF performing Admission Control for Unicast only. Its scope spans the Unicast resources in Access Segment and in the Aggregation Segment.

NOTE: The interactions between BTF_1, RCEF_1 and the A-RACF_1 are internal and may be different from illustrated. The interactions between BTF_2 and RCEF_2 are internal and may be different from illustrated.

The signalling flows for a Unicast Request and a Multicast Request are illustrated in figure G.15, where internal interactions are illustrated as dashed lines:
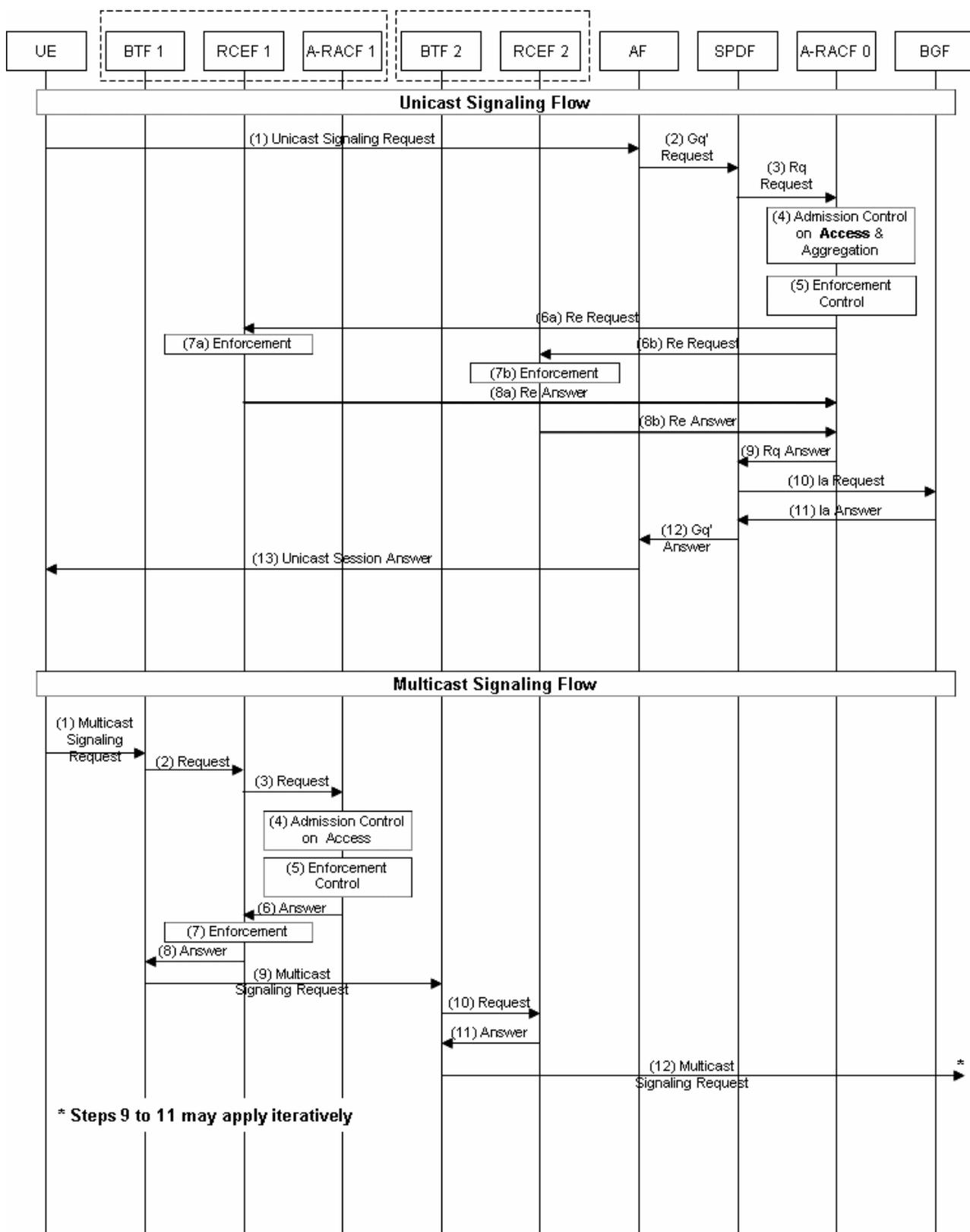
Figure G.15: Unicast and multicast services do NOT share resources on the Access Segment

Unicast Signalling Flow:

1) The AF receives a Unicast Signalling Request.

2) The AF contacts the SPDF.

3) From the point of view of the SPDF, a single x-RACF instance is visible: this is A-RACF_0.

4)   A-RACF_0 performs admission control for the Access and Aggregation segments.

5)   A-RACF_0 performs enforcement control.

6a) and 6b)   A-RACF_0 instructs RCEF_1 and RCEF_2 for enforcement operations.

7a) and 7b)   Policy Enforcement.

8a) and 8b)   Answers from RCEF_1 & RCEF_2 to A-RACF_0.

9)   Answer from A-RACF_0 to SPDF.

10) and 11)   SPDF interacts with the BGF.

12)   Answer from SPDF to the AF.

13)   Answer from the AF to the UE.

Multicast Signalling Flow:

1)   The AF receives a Unicast Signalling Request.

2)   BTF1 triggers RCEF1.

3)   RCEF1 requests admission control and policy decision from A-RACF_1.

4)   A-RACF_1 performs admission control in the access segment.

5)   A-RACF_1 determines the policies to be installed in RCEF_1.

6)   A-RACF_1 communicates the policies to RCEF_1.

7)   RCEF_1 enforces the policies.

8)   RCEF_1 answers to BTF_1.

9)   BTF_1 triggers BTF_2.

10)   BTF_2 triggers RCEF_2.

11)   RCEF_2 answers to BTF_2.

12)   Steps 9 to 11 may apply recursively.

G.5.2   Unicast and multicast applications share resources on the Access Segment

This scenario describes Admission Control for Unicast and Multicast, in case Multicast and Unicast share the same resources in the Access Segment.

In this scenario, it is assumed that:

- Unicast and Multicast service share the same transport resource in the Access segment.

- Unicast and Multicast service have different transport resources in the Aggregation segment.

- Admission Control for Resources for the Multicast service does not need to be performed in the Aggregation segment or beyond.

The following functional elements are involved:

- A-RACF_1 is an A-RACF deployed in the AN. A-RACF_1 performs Admission Control for the Access Segment for both Multicast and Unicast.

- RCEF_1 is deployed in the AN.

- BTF_1 is deployed in the AN.

- RCEF_2 is deployed in the IP_Edge.

- BTF_2 is deployed in the IP_Edge.

- A-RACF_0 is an A-RACF performing Admission Control for Unicast in the Aggregation Segment only. It relies on A-RACF1 for Admission Control of the Unicast service over the Access Segment.

In the presented scenario, A-RACF_1 performs admission control for multicast on the Access Segment without consulting A-RACF_0. Unicast and Multicast services share the same transport resource on the Access Segment: as such, the actual available bandwidth in the Access Segment is not known by A-RACF_0.

For this reason, whenever Admission Control for Unicast is required for the Access Segment, A-RACF_0 must delegate this Admission Control step to A-RACF_1. A-RACF_0 cannot grant a Unicast request before A-RACF_1 has indicated whether sufficient resources are available in the Access Segment.

The signalling flows for a Unicast Request and a Multicast Request are illustrated in figure G.16, where internal interactions are illustrated as dashed lines:
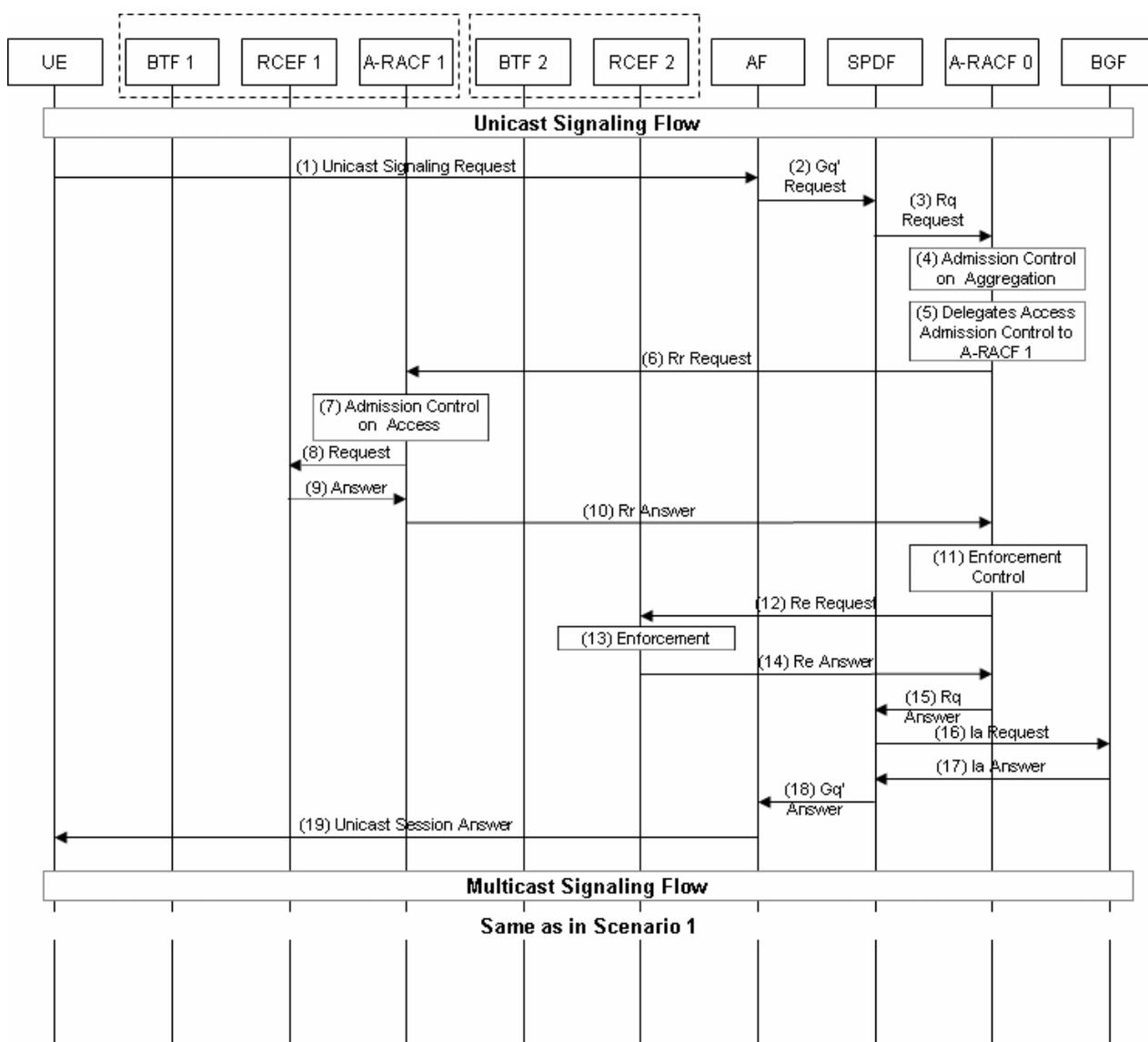

Figure G.16: Unicast and multicast applications share resources on the Access Segment

Unicast Signalling Flow:

1) The AF receives a Unicast Signalling Request.

2) The AF contacts the SPDF.

3) From the point of view of the SPDF, a single x-RACF instance is visible: this is A-RACF_0. This simplifies the dispatching decision, since the SPDF only needs to be aware of A-RACF_0. For this reason, the SPDF contacts A-RACF_0.

4) A-RACF_0 performs admission control for Aggregation segment.

5) and 6) A-RACF_0 delegates admission control for the access Segment to A-RACF_1.

7) A-RACF_1 verifies the resource availability in the Access Segment.

8) and 9) A-RACF_1 interacts with RCEF_1.

10) A-RACF_1 returns its decision to A-RACF_0 (Assumed to be granted in this example signalling flow).

11) A-RACF_0 performs enforcement control.

12), 13) and 14) A-RACF_0 interacts with RCEF_2 for enforcement.

15) A-RACF_0 returns a single answer to the SPDF (Assumed to be granted in this example signalling flow).

16) and 17) SPDF interacts with the BGF.

18) SPDF returns the answer to the AF.

19) The AF returns the answers to the UE.

Multicast Signalling Flow:

The same as the steps of multicast applications in clause G.5.1.

G.5.3   Unicast and multicast applications share resources on the Access Segment

This scenario describes Admission Control for Unicast and Multicast, in case Multicast and Unicast share the same resources in the Access Segment.

In this scenario, it is assumed that:

- Unicast and Multicast service share the same transport resource in the Access segment.

- Unicast and Multicast service have different transport resources in the Aggregation segment.

- Admission Control for Resources for the Multicast service does not need to be performed in the Aggregation segment or beyond.

The following functional elements are involved:

- A-RACF_1 is an A-RACF deployed in the AN. A-RACF_1 performs Admission Control for the Access Segment for Multicast only.

- RCEF_1 is deployed in the AN.

- BTF_1 is deployed in the AN.

- RCEF_2 is deployed in the IP_Edge.

- BTF_2 is deployed in the IP_Edge.

- • A-RACF_0 is an A-RACF performing Admission Control for Unicast in the Aggregation Segment and in the Access Segment. It is further handling Admission Control for Multicast in the Access Segment through delegating an Admission Control budget to A-RACF_1. A-RACF_0 is hence aware of resource reservations in both the Aggregation and Access segment.

It should be noted that it is assumed that all desired multicast streams are already present at the AN. Hence, BTF_2 and RCEF_2 need not to be involved in processing each multicast service request originating from the UE.

In the presented scenario, A-RACF_1 performs admission control for multicast on the Access Segment without consulting A-RACF_0. Unicast and Multicast services share the same total budged, i.e. transport resource, on the Access Segment. At each point in time, this total budget is strictly divided between the A-RACF_1 and the A-RACF_0 by that the A-RACF_1 is given a share of the total budget to be used for Multicast Admission Control from A-RACF_0. This share of the total budget is dynamically adapted using the Rr reference point.

An optional initialization signalling flow for installing a resource budget into A-RACF_1 is illustrated in the figure below. Alternatives to this initialization signalling flow is to provisioning the initial resource budget to A-RACF or to entirely rely on the negotiations of steps 3.1 and 3.2 in the unicast and multicast signalling flows respectively (i.e. when A-RACF_1 and A-RACF_0 adapts the total budget in them between). Figure G.17 shows signalling flows for a Unicast Request and a Multicast Request. It should be noted that steps 3.1 and 3.2 in both the Unicast Signalling Flow and the Multicast Signalling Flow are invoked only when he shared resource budget for the Access segment needs to be adapted (i.e. when part of this budget should be moved from A-RACF_0 to A-RACF_1 or vice versa).
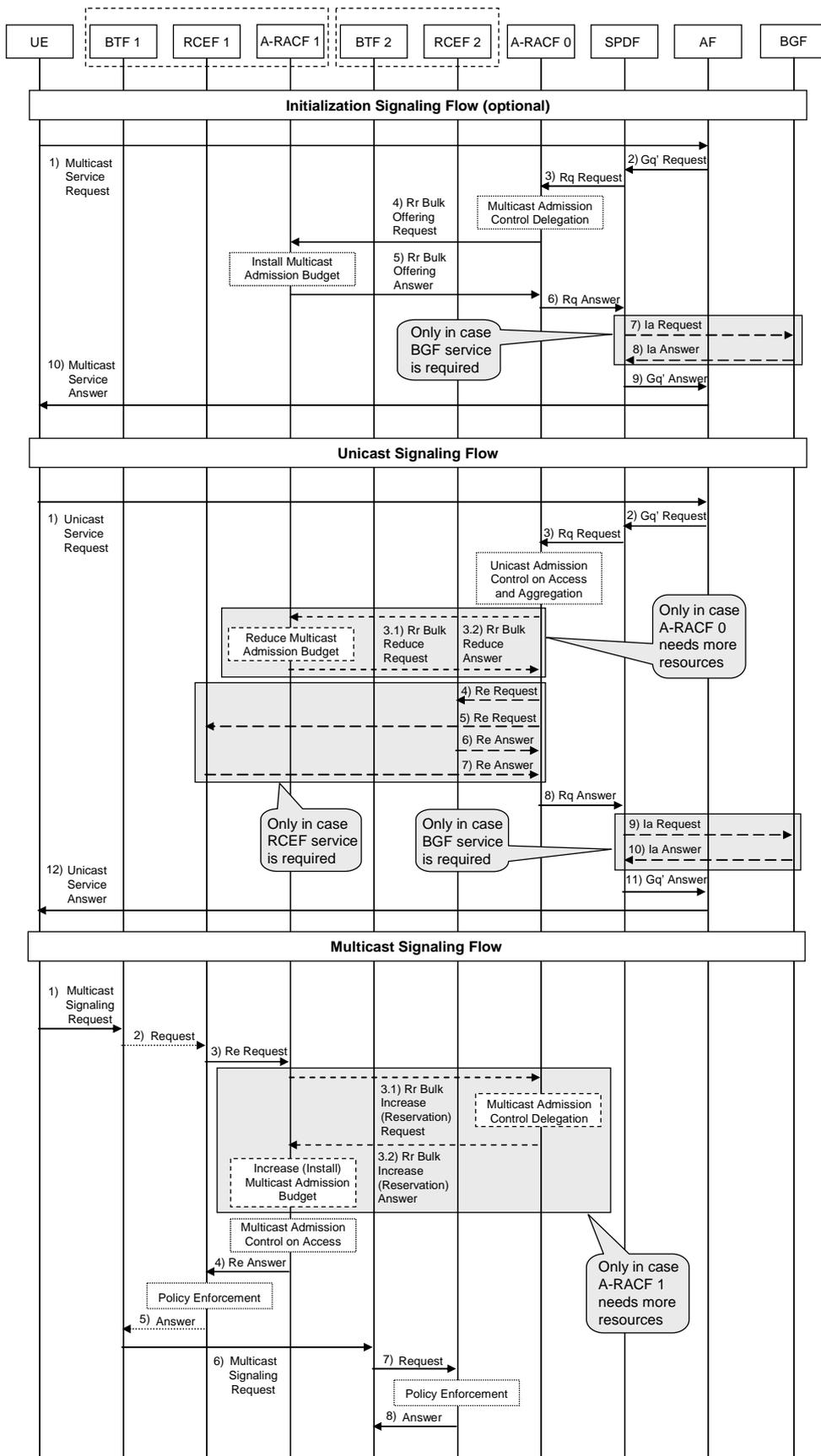
**Figure G.17: Signalling Flows for Unicast and multicast applications
sharing resources on the Access Segment**

Steps in Initialization Signalling Flow

This signalling flow is optional. As an alternative the multicast admission control budget can be installed using local configuration (i.e. provisioned into A-RACF_1) and thereafter adapted as part for the Multicast Signalling Flow and/or the Unicast Signalling Flow. As an additional alternative the multicast admission control budget can be both initialized and adapted as part of the Multicast Signalling Flow and/or the Unicast Signalling Flow:

1) The UE requests initialization of a multicast service from the AF. This step may involve application layer authorization. The AF may further complement the request with application layer profile information for the user requesting the service before issuing a request to RACS (e.g. determining the amount of bulk bandwidth needed).

2) The AF request the multicast service to be initialized. In this request the Service Class information element is used to indicate that the request is to initialization a multicast service. The requested bulk bandwidth corresponds to the expected demand for the most common usage. This bandwidth may be adapted as part of the Multicast Signalling Flow and/or the Unicast Signalling Flow.

3) SPDF derives the Rq request from the message in step 2.

4) The bulk bandwidth originally requested by the AF is offered to A-RACF_1 by A-RACF_0.

5) A-RACF_1 acknowledges that it has received the offered bulk bandwidth and is ready to use it for multicast admission requests arriving from RCEF_1.

6) A-RACF_0 replies to the SPDF that the bulk bandwidth is ready to be used in service multicast admission control requests.

7) In case BGF service is required, the SPDF requests those services from the BGF. It should be noted that this requests could also occur before the interaction with A-RACF_0 and A-RACF_1, or in parallel.

8) Reply from the BGF that the requested services are now available.

9) The SPDF replies to the AF to inform of that all requested initialization is performed in RACS.

10) AF informs the UE of the requested multicast service is now ready to be used.

Steps in Unicast Signalling Flow

It should be noted that this signalling flow is exactly the same as for release 1 from the perspective of the AF and the SPDF. The additional operations are limited to the A-RACF.

1) The UE requests a unicast service from the AF. This could be a request for an IMS session where the AF is instantiated by a P-CSCF, or a non-IMS service with another type of AF.

2) The AF requests the unicast service from RACS.

3) The SPDF derives the Rq request from the message in step 2.

   3.1) In case A-RACF_0 cannot admit the requested bandwidth immediately based on the resources it is currently in charge over, it issues a request to A-RACF_1 asking if it is willing to reduce its multicast resource budget.

   3.2) Based on local policies and/or current usage of multicast resources A-RACF_1 determines whether or not it can reduce its multicast resource budget. In this example, A-RACF_1 answer back to A-RACF_0 returning the desired resources for them to be used for the requested unicast service.

4) In case RCEF_1 service is needed for the requested service, A-RACF_0 issues a request to that entity.

5) RCEF_1 replies back to A-RACF_0.

6) In case RCEF_2 service is needed for the requested service, A-RACF_0 issues a request to that entity.

7) RCEF_2 replies back to A-RACF_0.

8) A-RACF_0 replies to the SPDF.

9) In case BGF service is required, the SPDF requests those services from the BGF. It should be noted that this requests could occur before the interaction with A-RACF_0 and A-RACF_1, or in parallel.

10) Reply from the BGF that the requested services are now available.

11) The SPDF replies to the AF.

12) The AF replies to the UE.

Steps in Multicast Signalling Flow

It should be noted that this signalling flow does not involve any interaction with any AF, the SPDF or the BGF.

1) The UE requests a multicast service from BTF_1. This request can be an IGMP join or a request made using a different mechanism.

2) BTF_1 derives the request to RCEF_1 from step 1.

3) RCEF_1 derives the request to A-RACF_1 from step 2.

   3.1) In case A-RACF_1 cannot admit the requested bandwidth immediately based on the resources it is currently in charge over, it issues a request to A-RACF_0 asking if it is willing to provided more bandwidth to the multicast resource budget over which A-RACF_1 is in charge.

   3.2) Based on local policies and/or current usage of unicast resources A-RACF_1 determines whether or not it can provide more bandwidth to the multicast resource budget owned by A-RACF_1. In this example, A-RACF_1 answer back to A-RACF_0 providing the desired resources for them to be used for the requested multicast service.

4) A-RACF_1 replies to RCEF_1 whereby it can activate the needed policy enforcement.

5) RCEF_1 replies to BTF_1.

6) BTF_1 forward the multicast service request to BTF_2.

7) BTF_2 requests policy enforcement from RCEF_2.

8) RCEF_2 activate the requested policy enforcement and replies back to BTF_2.

History

Document history		
V1.1.1	June 2006	Publication
V2.0.0	March 2008	Membership Approval Procedure MV 20080509: 2008-03-11 to 2008-05-09