

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2111

(11/2011)

SERIES Y: GLOBAL INFORMATION
INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS
AND NEXT-GENERATION NETWORKS

Next Generation Networks – Quality of Service and
performance

Resource and admission control functions in next generation networks

Recommendation ITU-T Y.2111



International
Telecommunication
Union
Documents

Document Sharing Hub

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

GLOBAL INFORMATION INFRASTRUCTURE

General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899

INTERNET PROTOCOL ASPECTS

General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999

NEXT GENERATION NETWORKS

Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Numbering, naming and addressing	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Smart ubiquitous networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
Future networks	Y.3000–Y.3099

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Y.2111

Resource and admission control functions in next generation networks

Summary

Recommendation ITU-T Y.2111 specifies the functional architecture and requirements for the resource and admission control functions (RACF) in next generation networks (NGN), which may involve a variety of access and core transport technologies and multiple domains. The RACF provides real-time application-driven and policy-based transport resource management in support of end-to-end quality of service (QoS), gate control, network address translation, and traversal of remote network address translators. The RACF is not service-specific. Services can make use of RACF whether the IP multimedia subsystem is involved or not.

In particular, this edition of Recommendation ITU-T Y.2111 includes extensions to the 2008 edition to address issues related to the interaction with 3GPP policy control functionalities, resource and admission control between NGNs and RACF-unaware IP networks, wholesale, time-shifted TV services, QoS downgrading, mobility, resource and admission control based on user subscription profile, support of deep packet inspection (DPI), communication between RACF and management of performance measurement (MPM), policy-based charging control, and IPTV service by invitation.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T Y.2111	2006-09-13	13
2.0	ITU-T Y.2111	2008-11-13	13
3.0	ITU-T Y.2111	2011-11-29	13

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2012

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

		Page
1	Scope	1
2	References.....	1
3	Definitions	2
	3.1 Terms defined elsewhere	2
	3.2 Terms defined in this Recommendation.....	3
4	Abbreviations and acronyms	5
5	Conventions	8
6	Overview and requirements	8
	6.1 Overview	8
	6.2 High-level requirements	9
7	RACF mechanisms and scenarios	11
	7.1 QoS resource control mechanisms and scenarios.....	11
	7.2 NAPT control and NAT traversal mechanisms and scenarios	16
	7.3 Resource control for unicast and multicast processes	17
	7.4 Resource control for QoS downgrading	20
	7.5 Inter-operator communications	21
	7.6 Resource control mechanisms and scenarios for RACF and MPM interactions	26
	7.7 Resource control cooperation between the RACF and RACF-like resource control functions	26
8	Functional architecture	27
	8.1 Overview	28
	8.2 Functional entity descriptions.....	30
	8.3 Mechanisms.....	37
9	Reference points	38
	9.1 Reference point Rs	38
	9.2 Reference point Rw	50
	9.3 Reference point Rc	64
	9.4 Reference point Ru	66
	9.5 Reference point Rt.....	71
	9.6 Reference point Rp	84
	9.7 Reference point Ri	95
	9.8 Reference point Rd	107
	9.9 Reference point Rn	119
	9.10 Reference point Rh	119
	9.11 Reference point Rm	129
	9.12 Reference point Ro	131
	9.13 Reference point Rh'	134



	Page
9.14 Domain scope of the reference points	134
10 Procedures	134
10.1 Procedures for QoS control	135
10.2 Procedures for NAPT control and NAT traversal	152
11 Security considerations and requirements	155
11.1 Overview of threats and potential attacks	155
11.2 Security requirements	156
Annex A – Resource control mechanisms and scenarios for RACF and MPM communication	158
Annex B – RACF enhancement for supporting policy-based charging control	161
B.1 Overview of enhancements	161
B.2 Functional architecture	162
B.3 Functional architecture	163
Appendix I – Examples of the implementation of the RACF architecture	164
Appendix II – TRC-FE over different transport technologies	166
II.1 The TRC-FE over an IP network.....	166
II.2 The TRC-FE over an MPLS network.....	166
II.3 The TRC-FE over an Ethernet network.....	166
II.4 The TRC-FE over a broadband wireless network	167
Appendix III – Example of methods for detecting and determining resource availability in the TRC-FE.....	168
Appendix IV – Examples of admission control procedures for unicast and multicast	169
IV.1 Examples of admission control procedures for unicast and multicast	169
IV.2 Example of multicast resource control scenario.....	175
Appendix V – The consideration of the CPN gateway control mode.....	177
V.1 The architecture for CPN gateway control.....	177
V.2 The procedure of the CPN gateway control mode	178
V.3 Example of the implementation of the RACF for CPN gateways.....	179
V.4 CPN gateway control in wholesale mode.....	180
Appendix VI – Resource control deployment scenarios for multicast	182
Appendix VII – Inter-operator RACF communication scenarios for end-to-end QoS control involving nomadicity.....	184
Appendix VIII – Comparison between reference point Rw and Rh	186
Appendix IX – An example of an approach supporting time-shifted TV	187
Appendix X – Performance notification between the RACF and the MPM	189
X.1 Communication of multiple MPM functions	189
X.2 The comparison of the specifications of the reference points between the Rc and the Rm in the RACF	191
X.3 Use cases based on RACF-MPM communication	191

	Page
Appendix XI – Interaction examples between the RACF and the PCC	194
Appendix XII – Example admission control for IPTV service by invitation	200
Bibliography.....	202

Document Sharing Hub

Copyright International Telecommunication Union/ITU Telecommunication Sector
Provided by IHS Markit under license with ITU-T
No reproduction or networking permitted without license from IHS

Recommendation ITU-T Y.2111

Resource and admission control functions in next generation networks

1 Scope

This Recommendation specifies the resource and admission control functions (RACF) in support of end-to-end quality of service (QoS) and network border control (at access-core and inter-domain boundaries) in next generation networks (NGNs). The RACF is aimed at providing real-time application-driven and policy-based transport resource management for a wide range of services and for a variety of transport technologies (e.g., fixed or mobile). Services can make use of RACF whether the IP multimedia subsystem (IMS) is involved or not. This Recommendation defines the related requirements and functional architecture covering aspects such as resource reservation, admission control and gate control, network address port translation (NAPT) and firewall control, and network address translator (NAT) traversal. This Recommendation defines the related requirements and functional architecture covering aspects such as interactions with 3GPP policy control functionalities, resource and admission control between NGNs and RACF-unaware IP networks, wholesale, time-shifted TV services, QoS downgrading, mobility, resource and admission control based on user subscription profile, support of deep packet inspection (DPI), communication between RACF and management of performance measurement (MPM), policy-based charging control, and IPTV service by invitation.

It also defines the reference points between different functional entities and the pertinent stage 2 requirements and describes the procedures for QoS-related transport resource control, NAPT control, NAT traversal, inter-operator communication including other NGN and non-NGN providers, mobility support, performance measurement support, and policy-based charging control support.

The pertinent protocol specifications are described in separate Recommendations. End-to-end information flows for representative applications, such as VoIP, bulk data transfer and video on demand, are for further study.

Note that network management functionality is outside the scope of this Recommendation.

Administrations may require operators and service providers to take into account national regulatory and national policy requirements in implementing this Recommendation.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

- [ITU-T Y.1291] Recommendation ITU-T Y.1291 (2004), *An architectural framework for support of Quality of Service in packet networks*.
- [ITU-T Y.2001] Recommendation ITU-T Y.2001 (2004), *General overview of NGN*.
- [ITU-T Y.2011] Recommendation ITU-T Y.2011 (2004), *General principles and general reference model for Next Generation Networks*.
- [ITU-T Y.2012] Recommendation ITU-T Y.2012 (2010), *Functional requirements and architecture of next generation networks*.

- [ITU-T Y.2014] Recommendation ITU-T Y.2014 (2010), *Network attachment control functions in next generation networks*.
- [ITU-T Y.2018] Recommendation ITU-T Y.2018 (2009), *Mobility management and control framework and architecture within the NGN transport stratum*.
- [ITU-T Y.2173] Recommendation ITU-T Y.2173 (2008), *Management of performance measurement for NGN*.
- [ITU-T Y.2233] Recommendation ITU-T Y.2233 (2010), *Requirements and framework allowing accounting and charging capabilities in NGN*.
- [ETSI TS 123 203] ETSI TS 123 203 Ver. 10.4.0 (2011), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Policy and charging control architecture*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 accounting [ITU-T Y.2233]: The process of collecting and analysing NGN service and NGN resource usage metrics for the purposes of capacity and trend analysis, cost allocation, auditing, and billing, etc. Accounting management requires that resource consumption be measured, rated, assigned, and communicated between appropriate business entities.

3.1.2 billing [ITU-T Y.2233]: The process after rating in which the NGN transactions of NGN event usage are compiled and bills are produced.

3.1.3 chargeable event [ITU-T Y.2233]: Activity utilizing NGN network resources and related services for:

- user-to-user communication (e.g., a single call, a data communication session or a short message); or
- user-to-network communication (e.g., service profile administration); or
- inter-network communication (e.g., transferring calls, signalling, or short messages); or
- mobility (e.g., roaming or inter-system handover); and
- any other types of service activities the network operator may want to charge for.

As a minimum, a chargeable event characterizes the resource/service usage and indicates the identity of the involved end user(s).

3.1.4 charging [ITU-T Y.2233]: Function within the NGN network and the associated offline charging, online charging, and billing domain components whereby information related to a chargeable event is collected, formatted, transferred and evaluated in order to make it possible to determine usage for which the charged party may be billed (offline charging) or the subscriber's account balance may be debited (online charging).

3.1.5 charging event [ITU-T Y.2233]: Set of charging information forwarded by the charging trigger function (CTF) towards the charging collection function (CCF) (offline charging) or towards the online charging function (OCF) (online charging). Each charging event matches exactly one chargeable event.

3.1.6 flow [ITU-T Y.2233]: A flow is defined as a set of IP packets passing an observation point in the network during a certain time interval. All packets belonging to a particular flow have a set of common properties. Each property is defined as the result of applying a function to the values of:

- 1) One or more packet header fields (e.g., destination IP address), transport header fields (e.g., destination port number), or application header field (e.g., RTP header fields);
- 2) One or more characteristics of the packet itself (e.g., number of MPLS labels);
- 3) One or more fields derived from packet treatment (e.g., next hop IP address, output interface).

3.1.7 metering [ITU-T Y.2233]: See usage metering.

3.1.8 multicast [b-ITU-T H.323]: A process of transmitting packet data units or a media stream from one source to many destinations. The actual mechanism (i.e., IP multicast, multi-unicast, etc.) for this process may be different for different network technologies.

3.1.9 nomadicity [b-ITU-T Y.101]: Continuity of access between two information infrastructure components as they move in space.

NOTE – Especially in this Recommendation, nomadicity is extended to mean the ability of the user to change the network access point after moving; when changing the network access point, the user's service session is completely stopped and then started again, i.e., no handover is involved. It is assumed that the normal usage pattern is that users shut down their service session before moving to another access point or changing terminal.

3.1.10 offline charging [ITU-T Y.2233]: Charging mechanism where charging information does not affect, in real-time, the service rendered.

3.1.11 online charging [ITU-T Y.2233]: Charging mechanism where charging information can affect, in real-time, the service rendered and therefore a direct interaction of the charging mechanism with resource/session/service control is required.

3.1.12 policy based charging and accounting [ITU-T Y.2233]: Charging and accounting capability based on different factors or factor group (e.g., access specific characteristics, QoS provided by the transport for the service, specific service types, time, user subscription information, etc.).

3.1.13 rating [ITU-T Y.2233]: The process of calculating the charges for an NGN transaction.

3.1.14 real-time [ITU-T Y.2233]: Real-time charging and billing information is to be generated, processed, and transported to a desired conclusion in less than 1 second.

3.1.15 session [ITU-T Y.2233]: Logical connection between parties involved in a packet-switched based communication.

NOTE – This term is used for IP connections rather than the term "call" that is normally used for a connection over conventional (circuit switched) systems. A session can be composed of one or more unidirectional and/or bidirectional flows.

3.1.16 unicast [b-ITU-T H.323]: A process of transmitting messages from one source to one destination.

3.1.17 usage metering [b-ITU-T Q.825]: The abstraction of activities that monitor the utilization of resources, for the purpose of accounting and controlling the recording of usage data.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 absolute QoS: The mode of QoS description which is expressed using numerical bounds on some or all parameters. These bounds may be physical limits, or enforced 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.

3.2.2 application session: An end-to-end user process that is established through the service control function (SCF) (using SIP or other protocol) and may trigger a resource control session.

3.2.3 firewall working mode selection: The operation of selecting the packet inspection mode (e.g., IP, TCP/UDP header, or higher layer) of a packet-filtering-based firewall for accepting or rejecting the packets of a media flow based on related service and security requirements.

3.2.4 gate: A construct used to enable or disable the forwarding of IP packets based on the policy decision. A gate is identified by the classifier (e.g., IPv4 5-tuple) and direction of a media flow or a group of media flows that are in conformity with the same set of policy decisions.

3.2.5 gate control: The operation of opening or closing a gate. When a gate is open, the packets in the media flows are allowed to pass through; when a gate is closed, the packets in the media flows are not allowed to pass through.

3.2.6 hard state: A state that is persistent until explicitly removed.

3.2.7 media flow: A unidirectional media stream, which is specified by two endpoint identifiers and bandwidth, as well as a class of service if needed.

3.2.8 NAPT control: The operation of providing network address mapping information and NAPT policy rules to a near-end NAT in the media flow.

3.2.9 NAT traversal: The operation of adapting the IP addresses so that the packets in the media flow can pass through a far-end (remote) NAT.

3.2.10 network address port translation (NAPT): The operation by which IP addresses and transport or port identifiers such as TCP and UDP port numbers are translated (i.e., mapped) from one address domain to another address domain.

3.2.11 network address translation: The operation by which IP addresses are translated (mapped) from one address domain to another address domain.

3.2.12 network address translator (NAT): An entity that implements network address translation or NAPT functions. It consists of two types of NATs: near-end NAT that can be controlled by the operators directly, and far-end (remote) NAT that cannot be controlled by the operators directly.

3.2.13 path-coupled QoS signalling: A mode of signalling where the signalling messages follow a path that is tied to the data packets. Signalling messages are routed only through nodes that are in the data path.

3.2.14 RACF-like control function: Policy-based resource admission and control function which is defined by other standardization organizations such as policy and charging control (PCC) from 3GPP.

NOTE – PCC is specified in 3GPP technical specification [ETSI TS 123 203] as the architecture which provides flow-based charging and policy control.

3.2.15 RACF-unaware IP networks: The IP-based networks which are not capable of supporting RACF based QoS control, but do have the capability to support DiffServ or other transport QoS mechanisms such as congestion avoidance, queue management, scheduling, packet marking, traffic policing and traffic shaping.

3.2.16 relative QoS: The mode of QoS description where bounds on QoS parameters such as delay are not expressed in absolute terms. It describes the circumstances where certain classes of traffic are handled differently from other classes of traffic, and the classes achieve different levels of QoS.

3.2.17 resource control session: A process for a set of media flows associated with an application session for a period of time in order to control resources required for the application session.

3.2.18 soft state: A state that has a limited lifetime and requires renewal to be kept alive.

3.2.19 technology dependent resource control functions: The functions that require specific knowledge of the link-layer technology in use in order to perform resource control.

3.2.20 technology independent resource control functions: The functions that do not require specific knowledge of the link-layer technology in use in order to perform resource control.

3.2.21 wholesale: The leasing of physical network infrastructures or selling of their services or capabilities by one provider to another provider enabling the other provider to deliver its own products or services to its own customers.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AAA	Authentication, Authorization, and Accounting
ACS	Auto Configuration Server
AF	Application Function
AS	Application Server
AS-FE	Application Support Functional Entity
ATM	Asynchronous Transfer Mode
CAF	Charging and Accounting Function
CBR	Constant Bit Rate
CCF	Charging Collection Function
CDMA	Code Division Multiple Access
CGPD-FE	CPN Gateway Policy Decision Functional Entity
CGPE-FE	CPN Gateway Policy Enforcement Functional Entity
CMTS	Cable Modem Termination System
CNPS	Core Network Path Selection
CPE	Customer Premises Equipment
CPN	Customer Premises Network
CR-LDP	Constraint Routed Label Distribution Protocol
CSCF	Call Session Control Function
CTF	Charging Triggering Function
DHCP	Dynamic Host Configuration Protocol
DiffServ	Differentiated Services
DoS	Denial of Service
DPI	Deep Packet Inspection
DSCP	Differentiated Services Code Point
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
ERC	Element Resource Control
ETS	Emergency Telecommunications Service
FDP	Final Decision Point
FQDN	Fully Qualified Domain Name



FWMS	Firewall Working Mode Selection
GC	Gate Control
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GTP	GPRS Tunnelling Protocol
H	Home
HTTP	Hypertext Transfer Protocol
ID	Identifier
IGMP	Internet Group Management Protocol
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IP-CAN	IP-Connectivity Access Network
IPMC	IP Packet Marking Control
IPsec	security architecture for Internet Protocol
LAN	Local Area Network
LSP	Label-Switched Path
MAC	Media Access Control
MLD	Multicast Listener Discovery
MMCF	Mobility Management and Control Function
MP	Measurement Point
MPLS	Multi-Protocol Label Switching
MPM	Management of Performance Measurement
MRF	Multicast Replication Function
MSCF	Multicast Service Control Function
MTCF	Multicast Transport Control Function
NACF	Network Attachment Control Function
NAPT	Network Address Port Translation
NAPTC	NAPT Control
NAT	Network Address Translator
NGN	Next Generation Network
NMS	Network Management System
NRM	Network Resource Maintenance
NS	Network Selection
NTM	Network Topology Maintenance
NTRD	Network Topology and Resource Database
OCF	Online Charging Function
PCC	Policy and Charging Control

PCEF	Policy and Charging Enforcement Function
PCRF	Policy and Charging Rule Function
P-CSCF	Proxy-Call Session Control Function
PD-FE	Policy Decision Functional Entity
PE-FE	Policy Enforcement Functional Entity
PME-FE	Performance Measurement Execution Functional Entity
PMP-FE	Performance Measurement Processing Functional Entity
PMR-FE	Performance Measurement Reporting Functional Entity
PNNI	Private Network-to-Network Interface
PPP	Point-to-Point Protocol
QMTD	QoS Mapping – Technology Dependent
QMTI	QoS and Priority Mapping – Technology Independent
QoE	Quality of Experience
QoS	Quality of Service
RACF	Resource and Admission Control Functions
RAR	Resource Action Request
RDP	Resource Decision response
RDR	Resource Decision Request
RIP	Resource Initiation response
RIR	Resource Initiation Request
RLC	Rate Limiting Control
RMR	Resource Modification Request
RRR	Resource Release Request
RSP	Retail Service Provider
RSVP	Resource reservation Protocol
RTCP	RTP Control Protocol
RTP	Real-Time Transport Protocol
SCF	Service Control Function
SCPF	Service Control Proxy Function
SDP	Session Description Protocol
SGSN	Serving GPRS Support Node
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SLS	Service Level Specification
SNMP	Simple Network Management Protocol
SUP-FE	Service User Profile Functional Entity
TCP	Transmission Control Protocol

TDDP	Technology Dependent Decision Point
TDR	Telecommunications for Disaster Relief
TLS	Transport Layer Security
TRC-FE	Transport Resource Control Functional Entity
TRE-FE	Transport Resource Enforcement Functional Entity
UDP	User Datagram Protocol
UE	User Equipment
UGS	Unsolicited Grant Service
UMTS	Universal Mobile Telecommunications System
V	Visited
VBR	Variable Bit Rate
VC	Virtual Channel
VCI	Virtual Channel Identifier
VLAN	Virtual Local Area Network
VMTN	Virtual MPLS Transport Network
VoIP	Voice over Internet Protocol
VP	Virtual Path
VPC	Virtual Path Connection
VPI	Virtual Path Identifier
VPN	Virtual Private Network
WLAN	Wireless Local Area Network
WSP	Wholesale Service Provider

5 Conventions

None.

6 Overview and requirements

6.1 Overview

Within the NGN architecture [ITU-T Y.2001] and [ITU-T Y.2011], the resource and admission control functions (RACF) act as the arbitrator between service control functions (SCF) and transport functions for QoS [ITU-T Y.1291] related transport resource control within access and core networks. The policy decisions made by the RACF are based on transport subscription information, service level agreements (SLAs), network policy rules, service priority (e.g., defined by [b-ITU-T Y.2171]), and transport resource status and utilization information. Figure 1 depicts a schematic view of the RACF in the overall NGN architecture.

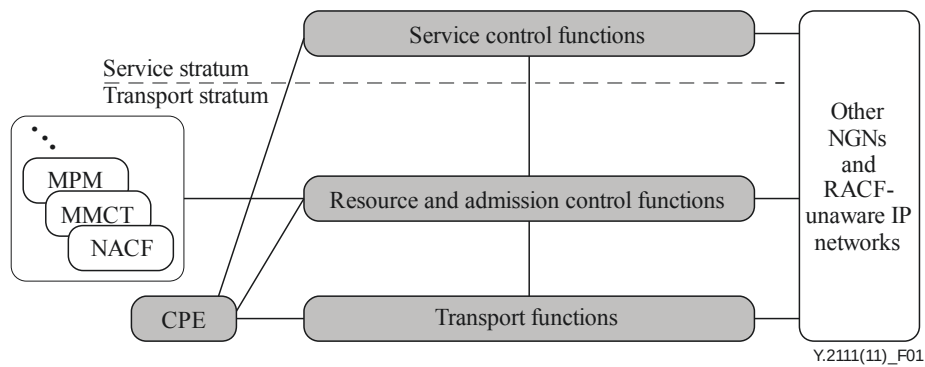


Figure 1 – RACF within the NGN architecture

The RACF provides an abstract view of transport network infrastructure to the SCF and decouples the provision of services from the details of transport facilities such as network topology, connectivity, resource utilization and QoS mechanisms/technology. The RACF interacts with the SCF, other transport control functions (e.g., mobility management and control function (MMCF) [ITU-T Y.2018], MPM [ITU-T Y.2173]), and transport functions for a variety of applications (e.g., SIP-based call [b-IETF RFC 3261] or video streaming) that require the control of NGN transport resources, including QoS control, NAPT/firewall control and NAT traversal.

The RACF executes policy-based transport resource control upon the request of the SCF or other transport control functions; it determines transport resource availability, makes admission decisions, and applies controls to transport functions for enforcing the policy decisions. The RACF interacts with transport functions for the purpose of controlling one or more of the following functions in the transport stratum: bandwidth reservation and allocation, packet filtering; traffic classification, marking, policing, and priority handling; network address and port translation; firewall.

The RACF takes into account the capabilities of transport networks and associated transport subscription information for subscribers in support of the transport resource control. The RACF interacts with network attachment control functions (NACF), [ITU-T Y.2014], including network access registration, authentication and authorization, parameter configuration, etc., for checking transport subscription information.

For delivery of those services across multiple providers or operators, SCF, RACF and transport functions may interact with the corresponding functions in other NGNs or RACF-unaware IP networks.

6.2 High-level requirements

6.2.1 Requirements specified in Recommendation ITU-T Y.2111 (2006)

The resource and admission control functional architecture meets the following mandatory requirements:

- 1) Control the QoS-related transport resources within packet networks and at the network boundaries in accordance with their capabilities.
- 2) Support different access and core transport technologies (e.g., xDSL, UMTS, CDMA2000, cable, LAN, WLAN, Ethernet, MPLS, IP, ATM), while hiding network technological and administrative details (e.g., network topology, connectivity, control mechanisms) from the SCF.
- 3) Support customer premises equipment (CPE)'s differing intelligence and capability. For example, some CPEs may support transport QoS signalling (e.g., GPRS session management signalling [b-ETSI TS 123 207], RSVP [b-IETF RFC 2205]), while others may not.

- 4) Support resource and admission control within a single administrative domain and between administrative domains.
- 5) Act as the arbitrator for QoS-related transport resource negotiation between SCF and transport functions in the access and core networks.
- 6) Support both relative QoS control and absolute QoS control.
- 7) Verify transport resource availability on an end-to-end basis. The verification may be loose or strict, depending on whether the request is for relative or absolute QoS. The RACF may act to reserve the resource.
- 8) Support QoS differentiation over various categories of packet traffic including packet-type flows (i.e., different packet-type flows may receive different QoS treatments) and user designations (i.e., different user traffic may receive different QoS treatments depending on the user's classifications).
- 9) Support QoS signalling [b-ITU-T Q.Sup.51]. This may include the ability to perform admission control based on estimated performance achieved along the path, compliant with QoS objectives.
- 10) Authorize requests for QoS and operate only on the authorized requests for QoS, for example, using information derived from transport subscription information, service priority, and network policy rules.
- 11) Support dynamic near-end NAPT control and firewall working mode selection.
- 12) Support far-end (remote) NAT traversal.
- 13) Support distributed and centralized transport resource control architectures.

The resource and admission control functional architecture meets the following optional requirements:

- 1) Export information to support charging based on resource usage and/or QoS treatments.
- 2) Support methods for resource-based admission control.
- 3) Have access to and make use of information provided by network management on performance monitoring to assist in making resource-based admission decisions.
- 4) Have access to and make use of the network status information provided by the underlying network infrastructure in support of end-to-end QoS when transport functions detect and report a failure.
- 5) Make use of the service priority information for priority handling (e.g., admission control based on service priority information). This includes passing of service priority information between entities where applicable.
- 6) Support path selection between ingress and egress points within a single domain to satisfy QoS resource requirements.

6.2.2 Additional requirements specified in Recommendation ITU-T Y.2111 (2008)

The resource and admission control functional architecture meets the following mandatory requirements in Recommendation ITU-T Y.2111 (2008):

- 1) Resource and admission control for multicast in support of, e.g., IPTV.
- 2) Resource and admission control in support of nomadicity.

The resource and admission control functional architecture meets the following optional requirement in Recommendation ITU-T Y.2111 (2008):

- 1) Support the interaction between the CPE/customer premises network (CPN) and RACF.

6.2.3 Additional requirements specified in this edition

The resource and admission control functional architecture meets the following mandatory requirements in this edition:

- 1) Support the interaction with 3GPP PCC [ETSI TS 123 203].
- 2) Resource and admission control based on inter-provider SLA for the service delivery over interconnection between NGNs and RACF-unaware IP networks.
In order to provide guaranteed QoS level support, RACF-unaware IP networks may also have specific transport mechanisms for admission control and overload protection based on policies configured by operators.
- 3) Resource and admission control in support of wholesale activities.

The resource and admission control functional architecture meets the following optional requirements in this edition:

- 1) Resource and admission control in support of time-shifted TV services.
- 2) Resource and admission control in support of QoS downgrading.
- 3) Resource and admission control in support of mobility.
- 4) Resource and admission control based on a user subscription profile upon network attachment.
- 5) Resource and admission control in support of deep packet inspection (DPI).
- 6) Resource and admission control in support of an IPTV service by invitation.

7 RACF mechanisms and scenarios

7.1 QoS resource control mechanisms and scenarios

7.1.1 QoS resource control mechanisms

QoS capability of CPE

According to the capability of QoS negotiation, the CPE can be categorized as follows:

- Type 1 – CPE without QoS negotiation capability (e.g., vanilla soft phone, gaming consoles):
The CPE does not have any QoS negotiation capability at either the transport or the service stratum. It can communicate with the SCF for service initiation and negotiation, but cannot request QoS resources directly.
- Type 2 – CPE with QoS negotiation capability at the service stratum (e.g., SIP phone with SDP [b-IETF RFC 4566]/SIP QoS extensions [b-IETF RFC 3312]):
The CPE can perform service QoS negotiation (such as bandwidth) through service signalling, but is unaware of QoS attributes specific to the transport. The service QoS concerns characteristics pertinent to the application.
- Type 3 – CPE with QoS negotiation capability at the transport stratum (e.g., UMTS user equipment (UE)):
The CPE supports RSVP-like or other transport signalling (e.g., GPRS session management signalling, ATM PNNI/Q.931). It is able to directly perform transport QoS negotiation throughout the transport facilities (e.g., DSLAM, CMTS, SGSN/GGSN).

Note that the SCF is required to be able to invoke the resource control process for all types of CPE.

Resource control modes

In order to handle different types of CPE and transport QoS capabilities, the RACF is required to support the following QoS resource control modes as part of its handling of a resource request from the SCF:

- **Push mode:** The RACF makes the authorization and resource control decision based on policy rules and autonomously instructs the transport functions to enforce the policy decision.
- **Pull mode:** The RACF makes the authorization decision based on policy rules and, upon the request of the transport functions, re-authorizes the resource request and responds with the final policy decision for enforcement.

The push mode is suitable for the first two types of CPE. For type 1 CPE, the SCF determines the QoS requirements of the requested service on behalf of the CPE; for type 2 CPE, the SCF extracts the QoS requirements from service signalling. The pull mode is suitable for type 3 CPE, which can explicitly request QoS resource reservation through transport QoS signalling.

Resource control states

Regardless of the QoS negotiation capability of a particular CPE and the use of a particular resource control mode, the QoS resource control process consists of three logical states:

- **Authorization (Authorized):** The QoS resource is authorized based on policy rules. The authorized QoS bounds the maximum amount of resource for the resource reservation.
- **Reservation (Reserved):** The QoS resource is reserved based on the authorized resource and resource availability. The reserved resource can be used by best effort media flows when the resource has not been committed in the transport functions.
- **Commitment (Committed):** The QoS resource is committed for the requested media flows when the gate is opened and other admission decisions (e.g., bandwidth allocation) are enforced in the transport functions.

The general resource control criteria are required to be:

- The amount of committed resources is not greater than the amount of reserved resources.
- The amount of reserved resources is not greater than the amount of authorized resources.

Note that the amount of committed resources typically equals the amount of reserved resources.

Resource control schemes

Given the variety of application characteristics and performance requirements, the RACF supports three resource control schemes:

- **Single-phase scheme:** Authorization, reservation and commitment are performed in a single step. The requested resource is immediately committed upon successful authorization and reservation. The single-phase scheme is suitable for client-server-like applications to minimize the delay between the service request and the ensuing reception of content.
- **Two-phase scheme:** Authorization and reservation are performed in one step, followed by commitment in another step. Alternatively authorization is performed in one step, followed by reservation and commitment in another step. The two-phase scheme is suitable for interactive applications, which have stringent performance requirements and need to have sufficient transport resources available.
- **Three-phase scheme:** Authorization, reservation and commitment are performed in three steps sequentially. The three-phase scheme is suitable for network-hosted services in an environment where transport resources are scarce.

These resource control schemes involve the PD-FE, TRC-FE, PE-FE and certain reference points. The specific reference points involved depend on the implementation scenarios. Distributed transaction processing, which requires interactions among the involved functional entities, is supported in these three schemes.

Information for resource control

The RACF is required to perform resource control based on the following information:

- Service information: A set of data provided by the SCF for a resource control request, derived from service subscription information, service QoS requirement and service policy rules.
- Transport network information: A set of data collected from the transport networks, which may consist of transport resource admission decisions and network policy rules.
- Transport subscription information: A set of data for the transport subscription profile such as the maximum transport capacity per subscriber.

Policy rules for the enforcement of resource control results

The RACF may assist the installation of two types of policy rules related to the enforcement of resource control results:

- Policy decision: A set of policy conditions and actions for the enforcement of resource control results on a per flow basis, which is produced dynamically upon the individual resource request from the SCF. The RACF is required to make policy decisions based on the information for resource control described in the above paragraph and install the policy decisions to the transport functions autonomously or upon the request of the transport functions. The policy decision can be modified and updated within the lifetime of a resource control session.
- Policy configuration: A set of static policy rules for default network resource configuration. The policy configuration is predefined by network operators and the policy rules will not be influenced by individual service requests. The policy configuration can be pre-provisioned statically in transport functions, e.g., mapping rules of the IP layer QoS to link layer QoS. In some cases, the RACF may help install the initial policy configuration for resource control, such as default resource control configuration (e.g., default gate setting). The related details are for further study.

Note that the RACF may use the soft-state (state that has a lifetime and requires renewal to keep alive) or hard-state (state that is persistent until explicitly removed) approach in support of transport resource control.

Levels of resources

The RACF may control the resource at different levels. At least, two levels have been identified:

- Aggregate level: The resources controlled at this level correspond to bulk of traffic independent of the start and stop of an application session and may carry more than one application session at the same time.
- Media flow level: The resources controlled in this level correspond to individual user traffic flow.

For example, the aggregate level may concern:

- A bulk of traffic belonging to the same class of service, disregarding the kind of data and application session; a bulk of bandwidth between two nodes or a label-switched path (LSP), a VPN or a VLAN, disregarding the type of applications or data belonging to this application session.

7.1.2 QoS resource control scenarios

On account of different QoS capabilities of CPE and transport networks, two QoS resource control scenarios are described as examples.

Note that the intent of these examples is to illustrate the relationship between RACF and relevant entities. For the following example scenarios only the originating CPE is shown for simplicity.

Scenario 1: Push mode QoS resource control scenario

The QoS resource control scenario using the push mode is required to be applied to all types of CPE.

The CPE type 1 does not have any QoS negotiation capability. It cannot initiate an explicit QoS request. The SCF (including the IP multimedia subsystem (IMS) [b-ETSI TS 123 228] and non-IMS) is responsible for deriving the QoS needs of the requested service and sending a request to the RACF for QoS resource authorization and reservation.

The CPE type 2 supports QoS negotiation at the service stratum. It can initiate an explicit service QoS request through the service signalling with QoS extensions (e.g., SDP/SIP extensions for application QoS requirements) or through dedicated application layer QoS signalling used for application signalling protocols that lack QoS extensions or are difficult to extend. The SCF (e.g., P-CSCF in IMS) is responsible for extracting the service QoS requirements and sending a request to the RACF for QoS resource authorization and reservation.

The CPE type 3 supports path-coupled QoS signalling in the transport stratum and can operate in push mode. In this case, the QoS resource authorization and reservation is conducted in the same way as the common push mode, where authorized and/or reserved QoS resource information is required to be pushed to the transport functions in advance. Path-coupled QoS signalling can be used to invoke resource commitment at the transport functions that, in turn, interact with the RACF or can indicate the result of resource commitment to the CPE.

In this scenario, the single-phase or two-phase resource control scheme can be used.

Figure 2 depicts the high-level QoS resource control procedure for scenario 1. The detailed information flows can be found in clause 10.1.1.

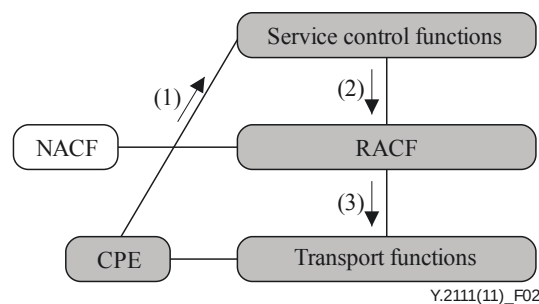


Figure 2 – Flow diagram for scenario 1

- 1) The CPE requests an application-specific service by sending a service request (e.g., SIP Invite, HTTP Get) to the SCF and may also send a dedicated application layer QoS signalling request. The service request may or may not contain any explicit service QoS requirement parameters.
- 2) The SCF extracts or derive the service QoS requirement parameters (e.g., bandwidth) of the requested service, and then requests QoS resource authorization and reservation from the RACF by sending a request for resource reservation which contains the explicit QoS requirement parameters.

- 3) The RACF performs authorization and admission control based on policy rules, resource admission decision and transport subscription profile stored in the NACF. If the request is granted, the RACF pushes the gate control, packet marking and bandwidth allocation decisions to the transport functions.

Scenario 2: Pull mode QoS resource control scenario

The QoS resource control scenario using the pull mode is applied to CPE and transport networks that support path-coupled transport signalling, which includes QoS signalling (e.g., RSVP) and other transport signalling.

The CPE type 3 supports dedicated path-coupled transport QoS signalling (e.g., GPRS session management signalling, RSVP) that passes only through the nodes on the data path. It can initiate an explicit QoS request (actually a resource reservation request) directly to the transport functions or just initiate a resource request without QoS information.

Figure 3 depicts the high-level QoS resource control steps for the scenario. The detailed information flows can be found in clause 10.1.2. The QoS resource reservation may or may not need the involvement of the SCF.

In the scenario with the involvement of the SCF, the two-phase or three-phase resource control scheme can be used for coordination between the service signalling and the dedicated path-coupled transport signalling. In this scenario, all steps are required to perform the resource reservation.

In the scenario without the involvement of the SCF, the CPE initiates a QoS request using the transport signalling to the transport function. After receiving the request, the transport function sends a request to RACF for admission control and resource reservation. The RACF will send back the decision to the transport function. In this scenario, only steps (4), (5) and (6) are required.

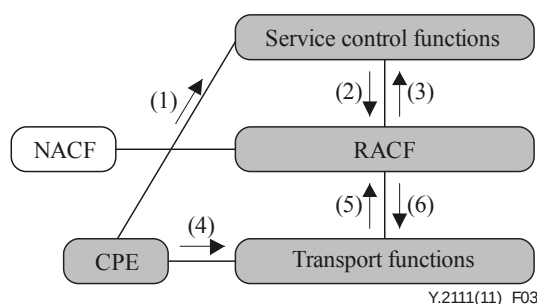


Figure 3 – Flow diagram for scenario 2

- 1) The CPE requests an application-specific service by sending a service request (e.g., SIP Invite, HTTP Get) to the SCF. The service request may or may not contain any explicit (application) service QoS requirements.
- 2) The SCF extracts or derives service QoS requirements (e.g., bandwidth) for the requested service, and sends an authorization request to the RACF that contains explicit QoS requirements.
- 3) The RACF checks authorization based on network policy rules. If the resources are authorized, an authorization token [b-IETF RFC 3520] is assigned to this service and informed to the CPE. The use of authorization token is optional. It is possible to perform authorization without the use of a token.
- 4) The CPE may initiate a request with QoS information for resource reservation directly to the transport functions through a dedicated path-coupled transport QoS signalling. This QoS request contains the explicit transport QoS requirement parameters for an application-specific service. It may also contain an authorization token assigned at the first phase. Alternatively, the CPE may initiate a request without explicit QoS information.

- 5) On receipt of the QoS request, the transport functions at the network edge send a request to the RACF for resource reservation and admission control that may contain the authorization token as an option. When the CPE sends a request without explicit QoS information, the transport functions send the QoS request to RACF on behalf of the CPE.
- 6) The RACF makes a reservation and admission control decision based on transport subscription profile held in the NACF, service information, network policy rules and resource availability. If the request is granted, the RACF provides the gate control, packet marking and bandwidth allocation decisions to the transport functions.

7.2 NAPT control and NAT traversal mechanisms and scenarios

7.2.1 NAPT control and NAT traversal scenarios

The RACF is required to provide the control function in support of the following NAPT scenarios.

Near-end NAPT control

In order to hide transport network addresses between different sub-networks and/or domains as a security measure, or to use private addresses due to the shortage of public addresses, near-end NAT devices controlled by operators are required to perform the NAPT at the border of access-to-core and/or the border of core-to-core. All NAPT techniques in support of network address hiding ultimately involve the installation of address bindings in NAPT devices, and the modification of the application signalling messages to reflect the bindings created by the NAPT.

Far-end (remote) NAT traversal

Far-end (remote) NAT devices are widely deployed in enterprise and residential networks to protect the customer premises networks. Both signalling and media of the application have to go through such NAT devices, if they exist. By default the applications assume the CPE's local network address is unique and reachable globally; the application signalling uses this local address to set up the end-to-end connection. However, the far-end NAT has broken those properties because the network address of media packets will be changed by the far-end NAT. The application cannot work through the far-end NAT, and NAT traversal mechanisms are required. All NAT traversal techniques ultimately involve the modification of the application protocol messages to reflect the address mapping necessitated by the far-end NAT.

7.2.2 NAPT control and NAT traversal mechanisms

The RACF is required to interact with the SCF and transport functions to perform the NAPT control and NAT traversal functions. Both NAPT control and NAT traversal can be supported by the same set of functional entities. The pertinent functions are distributed in the SCF, RACF and transport functions as shown in Figure 4:

- NAPT proxy function: is a service stratum function, which modifies the address and/or port in the message body of application signalling to reflect the address binding information created by NAPT enforcement function defined below.
- NAPT control function: obtains the address binding information, performs the NAPT policy control along with gate control (i.e., instruct the opening/closing of a gate).
- NAPT enforcement function: is a transport stratum function, which enforces the NAPT and media relay (address latching) to change the address and port number of the media packets.

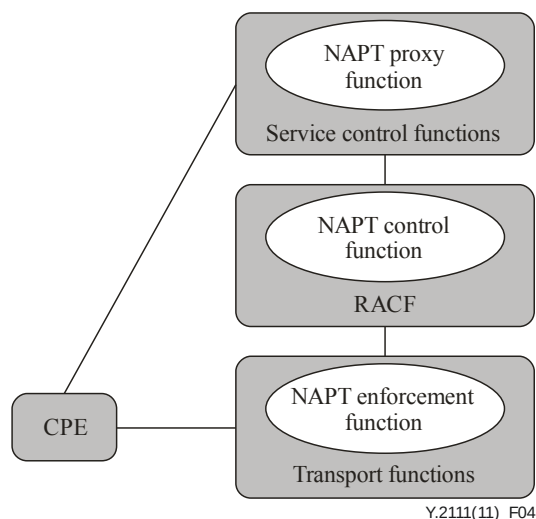


Figure 4 – NAPT and NAT traversal control mechanisms

The NAPT control function in RACF is required to provide the NAPT and NAT traversal control functions for address/port binding and NAPT policy control along with gate control; interact with NAPT proxy function in the SCF for modifying the message body of application signalling; and interact with NAPT enforcement function in the transport functions for requesting NAPT information.

7.3 Resource control for unicast and multicast processes

7.3.1 Introduction

In order to deliver content efficiently to many receivers simultaneously, multicast can be used. One of the expected applications of multicast is IPTV service.

For example, in order to provide an attractive IPTV service, many providers offer bundles of TV channels to customers with a very large number of channels, even if some of the TV channels remain frequently unwatched. IPTV traffic is carried over the network along with VoD traffic and Internet traffic. Often, the number of TV channels offered to customers is greater than the number of channels that can be simultaneously carried over the access and aggregation network, and at least some channels will be watched by more than one user on a given access node. Therefore, multicast is likely to be used for an IPTV service.

In this configuration, the risk of congestion is high and will result in the degradation of the QoS being provided, as well as the impossibility to attend to new service requests. It is therefore of the utmost importance to monitor, prevent, if possible, and control this situation. The RACF aims to address related issues.

7.3.2 Multicast resource control descriptions

7.3.2.1 Elementary functions for multicast processing

Two new elementary functions are defined to process multicast services:

Multicast replication function (MRF): The operation of replicating packets of a multicast group based on the membership tracked by the multicast transport control function (MTCF). A multicast group is identified by the combination of a unicast source address and a multicast destination address, or only by a multicast destination address.

Multicast transport control function (MTCF): The operation of processing the requests (e.g., IGMP, MLD) for joining or leaving a multicast group and tracking the group membership. It may interact with the RACF for admission control of the requests based on subscriber information (i.e., multicast access control list and subscribed multicast bandwidth) as well as the QoS-related transport resource information.

7.3.3 Resource control schemes for multicast services

The MTCF may interact with the RACF for the following purposes:

- Request the RACF to perform resource and admission control based on the initial processing of multicast requests (e.g., when the transport node is not already part of requested multicast group).
- Request the RACF to release related-resources when all end users leave an existing multicast group.
- Notify the RACF of abnormal events (e.g., link failure).

Two implementation scenarios are possible in the context of RACF to perform resource control for multicast services:

Standalone RACF: Multicast resource and admission control is performed in a separate node from MTCF.

Co-located RACF: Multicast resource and admission control is performed in the same node as MTCF.

The use of these two schemes is dependent on the multicast service control mechanism. For instance, when transport-layer signalling (e.g., IGMP, MLD) is used for multicast request, a co-located scheme is commonly employed to accommodate the performance requirement of channel zapping.

7.3.4 Resource control scenarios for multicast

The resource control scenarios for multicast are illustrated as follows. However, they are dependent on the multicast capability and mechanisms supported by the CPE and networks.

Scenario 1: MTCF requested QoS resource authorization and reservation

In this scenario, the multicast resource authorization and reservation are triggered by the MTCF when the MTCF receives a multicast group joining message (e.g., IGMP, MLD) from the CPE.

- 1) The CPE requests a multicast service (i.e., the request for an individual TV channel) by sending a transport signalling (e.g., IGMP, MLD) to the transport functions.
- 2) Upon receiving the service request from the CPE, the MTCF performs the multicast control, and if needed, requests the QoS resource authorization and reservation by sending a resource reservation request to the RACF.
- 3) The RACF performs authorization and admission control based on relevant information, e.g., policy rules, resource admission decision and transport subscription profile. If the request is granted, the RACF will send the policy decisions to the transport functions (i.e., MTCF) for enforcing the policy decisions.

Scenario 2: SCF requested QoS resource authorization and reservation

In this scenario, the resource authorization and reservation are triggered by the SCF. Joining the multicast group is requested by the CPE through sending transport signalling (e.g., IGMP, MLD) or by RACF without sending transport signalling.

- 1) The CPE requests a multicast service (e.g., the request for an individual TV channel or for a set of channels) by sending a service request to the SCF.

- 2) Upon receiving the service request, the SCF performs the service control and requests the QoS resource authorization and reservation by sending a request for resource reservation to the RACF.
- 3) The RACF performs authorization and admission control based on the relevant information, e.g., policy rules, resource admission decision and transport subscription profile. If the request is granted, the RACF will push the policy decisions to the transport functions.

Scenario 3: MTCF requested QoS resource release

In this scenario, the multicast resource release is triggered by the MTCF, when the MTCF receives a multicast group leave message (e.g., IGMP, MLD) from the CPE, or when the MTCF detects multicast group membership timeout for the CPE.

- 1) The CPE requests that it leaves the multicast service by sending transport signalling (e.g., IGMP, MLD) to the transport functions.
- 2) Upon receiving the leave request from the CPE, the MTCF performs the multicast control, and if needed, requests the QoS resource release by sending a resource release request to the RACF.
- 3) The RACF updates its resource status based on relevant information, e.g., session information which includes the available resources from recalculation based on the current participating users.

Scenario 4: SCF requested QoS resource release

In this scenario, the resource release is triggered by the SCF. The request to leave the multicast by the CPE occurs through sending transport signalling (e.g., IGMP, MLD) or by the RACF without transport signalling.

- 1) The CPE requests that it leaves a multicast service by sending a release request to the SCF.
- 2) Upon receiving the release request, the SCF performs the service control and requests the QoS resource release by sending a resource release request to the RACF.
- 3) The RACF checks if all the participating users left the session. If so, the RACF will send the resource release policy decision to the corresponding transport functions.

7.3.5 Resource control approaches for multicast and unicast

When the RACF is used to provide resource control for both multicast and unicast services, three approaches are supported:

- 1) Exclusive resource allocation approach: dedicated resources are allocated to multicast services and unicast services respectively through other manners (e.g., network management system). The unicast and multicast services do not share any network resources. In this case, two RACF instances operate independently to support the resource admission control for multicast and unicast services respectively without any interaction.
- 2) Adjustable resource allocation approach: Similar to the above approach, dedicated resources are allocated to multicast services and unicast services respectively through other manners (e.g., network management system). However, the RACF may adjust the ratio of the dedicated resources (i.e., maximum number of channels or bandwidth) between multicast and unicast services.

The RACF instances may interact with each other to negotiate the resource adjustment at the aggregate level. The relationship between the RACF instances may be either master-slave or client-server.

- 3) Dynamic resource allocation approach: multicast and unicast services share common resources. Each instance of the RACF is responsible for the resource and admission control for both multicast and unicast services in a particular network segment, e.g., access,

aggregation and/or core networks. Different RACF instances may interact with each other to make the final resource and admission control decision. The interactions may be either at the aggregate level or at the per media flow level.

7.3.6 Resource control for unicast and multicast resource reuse

Unicast and multicast resource reuse occurs when switching between a unicast service and a multicast service such as broadcast TV and its trick mode. In order to support the unicast and multicast resource reuse, RACF (including the co-located TRC-FE and the top-tier TRC-FE) needs to receive a message where a mechanism is provided to reuse the resource on the access network. Based on the message received, RACF can reuse the resources previously allocated to the active mode for the other mode.

NOTE – In this edition of this Recommendation, resource reuse mechanisms are not defined. They are for further study.

7.4 Resource control for QoS downgrading

NOTE – In this edition, QoS downgrading for a particular session/media flow does not consider any resulting side-effects. QoS downgrading is for further study.

QoS downgrading is the act of adjusting the QoS provided to an existing session (e.g., bandwidth and the time duration for using this bandwidth). A requester (e.g., SCF) can request that the QoS be downgraded for a service, without forcing it to terminate.

QoS downgrading may occur when a new incoming session needs to be admitted, and there is insufficient network resources available for the new session. The requester may decide to allow QoS downgrading for one or more existing sessions according to the SLA, between the user and the provider. The QoS of the existing session(s) may be degraded in order to provide resources for the new incoming session. Alternatively, the RACF may degrade the QoS of the new incoming session according to the indication from the requester. The downgraded QoS must be less than the maximum downgradable QoS subscribed in the NACF.

The RACF is required to provide mechanisms to:

- allow the requester to express the desire to be informed in case the amount of resources controlled by the RACF are insufficient to complete a request, but it might be able to complete the request by downgrading the QoS for a set of existing sessions allocated to this particular requester;
- inform the requester that a situation occurred where the amount of resources controlled by the RACF are insufficient to complete a request, but it might be able to complete the request by downgrading the QoS for a set of existing sessions allocated to this particular requester;
- allow the requester to indicate whether the QoS of a new request can be downgraded or not. When the RACF cannot allocate enough resources to a new request, the RACF can decide whether to degrade the requested QoS or not, based on the indication from the requester. If the requested QoS can be degraded, the RACF degrades it, and re-allocates the resources to the requested session. If the requested QoS cannot be degraded, the RACF may reject the request;
- allow the requester to indicate whether the QoS of a request can be restored or not. If the QoS of the existing session has been downgraded, the requester can indicate to the RACF to check whether the QoS of this session can be restored or not. If the QoS of the request can be restored, the RACF checks the resources availability. If there are sufficient resources, the QoS of this session will be restored;

- allow the requester to indicate whether the QoS of a request has been downgraded or not for a roaming scenario. In the roaming scenario, the requester (the home RACF) informs the visited RACF whether the QoS of the current session has been downgraded or not. If the visited network has sufficient resources, it should retrieve the original QoS of the session, rather than the current downgraded QoS.

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

It is also required that the RACF has a capability to downgrade existing sessions belonging to the other subscribers. In the current RACF architecture, the new session request will be rejected once the network resource (e.g., bandwidth) is fully occupied by the existing sessions. However, there can be many different levels of service priority. For example, an emergency call request to the fire service or to the police should be treated in a higher priority than the regular services. In the regular call services, the service can be further refined as the premium service that requires absolute bandwidth and the low cost service that allows the QoS downgrading when the network is congested. The network bandwidth can be managed more efficiently by downgrading the bandwidth of lower priority services. In order to support this, the RACF is required to provide mechanisms to:

- receive the additional information in the resource request for the processing of the QoS downgrading. The additional information includes the indication of the downgradable session and the minimum bandwidth for the session;
- maintain the list of admitted downgradable sessions for future downgrading;
- perform the reduction of the bandwidth of the existing downgradable session. By reducing the bandwidth of the existing downgradable session, the RACF secures the additional bandwidth to admit new sessions.

7.5 Inter-operator communications

7.5.1 Resource control scenarios for nomadicity

This clause describes the nomadicity scenario involving two operators playing the roles of the NGN home provider and the NGN visited provider. The NGN home provider owns the subscriber and the transport resources of the subscriber's home network, and the NGN visited provider owns the transport resources of the access network visited by the subscriber. The resource initiation can be triggered by the SCF deployed in either an NGN home provider or an NGN visited provider.

The NGN home provider performs initial policy decisions based on the user transport subscription profile, its own network policy rules, and service information. The NGN visited provider performs final policy decisions based on available resources, its own network policy rules, and the SLA with the NGN home provider. The NGN home provider maintains the user profile information, and it can be requested by the NGN visited provider as needed. In the case that the user profile information updated by the NGN visited provider is to be conveyed to the NGN home provider, it can be done in the reverse direction as well.

Figure 5 depicts a general network configuration involving inter-operator communications in support of nomadicity when resource initiation is triggered by the SCF deployed in the NGN home provider.

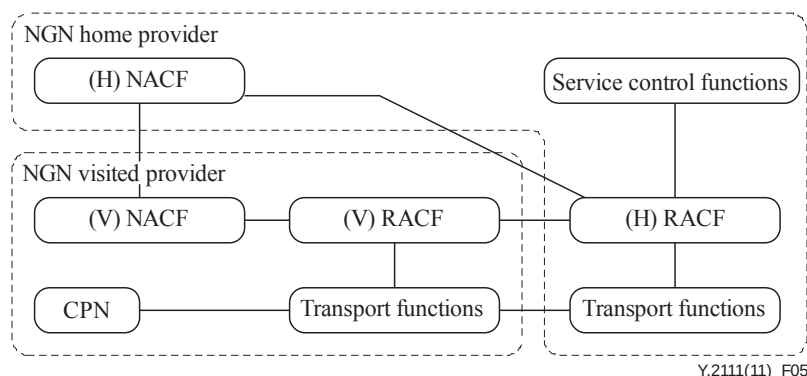


Figure 5 – Inter-operator communications for a nomadicity scenario

NOTE – Inter-NACF communication across domains is outside the scope of this Recommendation.

NOTE – The SCF connects with the RACF of the NGN home provider for resource control. The SCF may belong to the NGN home provider or third party providers which have a business relationship with the NGN home provider.

There are two resource control scenarios for nomadicity.

Scenario 1: The SCF-requested QoS resource reservation procedure (push mode)

- 1) The home SCF sends a resource initiation request to the home RACF ((H)RACF).
- 2) The (H)RACF authorizes the request including checking if the required QoS resources are consistent with the transport subscription information held in the home NACF ((H)NACF), and finds that the required resources belong to the visited network. Then the (H)RACF sends the request to the visited RACF ((V)RACF).
- 3) The (V)RACF checks if the required QoS resources are consistent with its own network policy rules, and also checks the resource availability.
- 4) The (V)RACF makes the final admission decisions, and then responds to the (H)RACF.

Scenario 2: The CPE-requested QoS control procedure (pull mode)

This scenario usually contains two phases: the SCF-requested QoS initial authorization phase and the CPE-requested QoS resource reservation phase.

- 1) The home SCF sends an initial resource authorization request to the (H)RACF as triggered by a service establishment signalling message from the CPE.
- 2) The (H)RACF makes a QoS resource authorization decision based on the subscription profile from the (H)NACF and the operator policies. If the required resources belong to the visited network, the (H)RACF asks the (V)RACF for authorization.
- 3) The CPE requests a QoS resource reservation in the visited network through path-coupled transport signalling.
- 4) (Optional) If the (H)RACF previously requested the initial authorization, the (V)RACF sends a message to the (H)RACF for retrieving the related service information.
- 5) Based on the 'QoS request' from the CPE, the (V)RACF checks if the required QoS resources and the service information are consistent with network policy rules and the initial authorization information, and also checks the resource availability. Then the (V)RACF makes the final admission decisions.

The (H)NACF provides user profile information for authorizing and authenticating the requests for user access to the visited network and network resource.

7.5.2 Resource control scenarios for wholesale

This clause describes the wholesale scenario involving two providers playing the roles of the retail service provider (RSP) and the wholesale service provider (WSP). RSP has overall responsibility for the provision of a service or set of services to users associated with a subscription as a result of commercial agreements established with the users (i.e., subscription relationships). WSP combines a retailing service provider's service capabilities with its own network service capabilities to enable users to obtain services. The user profile is maintained by the RSP and the WSP can interact with the RSP to request the user profile information if needed. Service provision is the result of combining wholesale network services and service provider service capabilities.

The RSP performs admission control, based on service information from the SCF, the access user profile from the NACF and its own network policy rules. WSP performs admission control based on resource availability, the SLA with the RSP and its own network policy rules.

Figure 6 depicts a general network configuration of wholesale scenario.

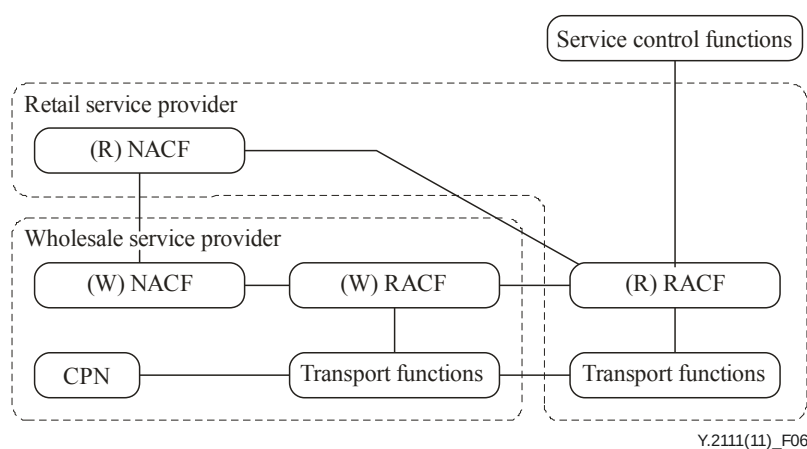


Figure 6 – Inter-operator communications for a wholesale scenario

NOTE – Inter-NACF communication across domains is outside the scope of this Recommendation.

There are two resource control scenarios for wholesale.

Scenario 1: The SCF-requested QoS resource reservation procedure (push mode)

- 1) The SCF sends a resource initiation request to the RSP.
- 2) The RSP authorizes the request including checking if the required QoS resources are consistent with the transport subscription information stored in the RSP's NACF. If successful, the resource initiation request is further sent to the WSP.
- 3) The WSP checks if the required QoS resources are consistent with its own network policy rules, and also checks the resource availability.
- 4) The WSP makes the final admission decisions, and then responds to the RSP.

Scenario 2: The CPE-requested QoS control procedure (pull mode)

This scenario usually contains two phases: the SCF-requested QoS initial authorization phase and the CPE-requested QoS resource reservation phase.

- 1) The SCF sends an initial resource authorization request to the RSP as triggered by a service establishment signalling message from the CPE.
- 2) The RSP makes a QoS resource authorization decision based on the subscription profile from the RSP's NACF and the operator policies. If successful, the RSP asks the WSP for authorization.

- 3) The CPE requests a QoS resource reservation in the wholesale network through path-coupled transport signalling.
- 4) (Optional) If the RSP previously requested the initial authorization, the WSP sends a message to the RSP for retrieving the related service information.
- 5) Based on the 'QoS request' from the CPE, the WSP checks if the required QoS resources and the service information are consistent with network policy rules and the initial authorization information, and also checks the resource availability. Then the WSP makes the final admission decisions.

The RSP's NACF provides user profile information for authorizing and authenticating the requests for user access to the wholesale network and network resources.

7.5.3 QoS control scenarios for interactions between NGNs and RACF-unaware IP networks

This clause describes the QoS control scenarios when NGNs interact with RACF-unaware IP networks, and the services supported which need to meet the QoS requirements as defined in the SLA.

The inter-provider SLA is a bilateral agreement which may include specific QoS requirements in terms of service types, bandwidth, service level specification (SLS) parameters or other attributes for each service that the NGN provides to the RACF-unaware IP networks provider, as well as, those which the RACF-unaware IP networks provide to the NGN provider. Furthermore, it may include an upper bound on the total amount of bandwidth used for traffic delivery over an interconnection point. As a basic assumption, QoS-related parameters handled at the RACF's reference point (see clause 9.7 for detail) may be consulted as the actual SLA parameters. Besides inter-provider SLAs, the two operators may still have an end-to-end SLA directly with end users. In this scenario, a new reference point for exchanging inter-provider SLAs (including manual exchanges, such as paper or e-mail) is required. However, the new reference point is not within the scope of this Recommendation.

The general network configuration of this scenario is depicted in Figure 7.

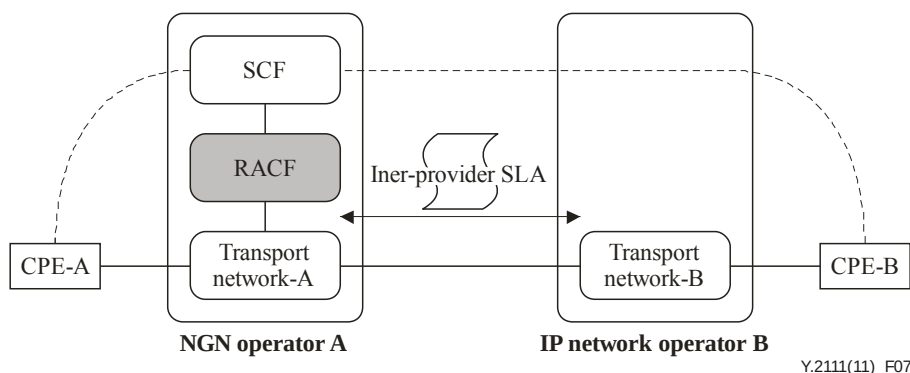


Figure 7 – Inter-operator communication between NGNs and RACF-unaware IP networks

The QoS control scenario for interaction between NGNs and RACF-unaware IP networks can be described as two cases:

- 1) The CPE in the NGN (CPE_A) sends the service request to the SCF, then, the SCF requests QoS control from the RACF.
- 2) The CPE in the RACF-unaware IP networks network (CPE_B) sends the service request to the SCF, then, the SCF requests QoS control from the RACF.

In case (1), the RACF performs the admission control and resource reservation based on a transport user profile from the NACF and information defined in the inter-provider SLA by using either push mode or pull mode. In case (2), the transport user profile is not stored in the NACF in the NGN and the path-coupled signalling (e.g., RSVP) may not be supported by RACF-unaware IP networks. This is so that the RACF performs the admission control and resource reservation based only on the inter-provider SLA by using push mode. SLA information may be manually configured to the RACF. In this case, the inter-operator SLA interface does not require an additional reference point and does not affect existing reference points.

In both cases, RACF-unaware IP networks are responsible for the delivery of service traffic with a required QoS level based on an inter-provider SLA without transport QoS signalling communication with the RACF.

When utilizing parameters that are supported by the RACF's reference point, and if the session information is also handled by the inter-provider SLA interface, SCF signalling (i.e., case (1) and (2)) is not required.

7.5.4 Resource control scenarios for handover

This clause describes the handover scenario involving two operators playing the roles of the NGN home provider and the NGN visited provider. The NGN home provider owns the subscriber and the transport resources of the subscriber's home network, and the NGN visited provider owns the transport resources of the access network visited by the subscriber. The resource initiation can be triggered by the MMCF in the NGN visited provider.

The MMCF may interact with the RACF for the following purposes:

- The MMCF queries the RACF to verify that resources are available to serve the user prior to handover.
- The MMCF requests that the RACF reserves session QoS resources by providing address binding information, and to release QoS resources on the old path once handover is complete.

The resource control scenario for handover includes two primary procedures: verification of resource availability and resource re-provisioning.

Verification of resource availability:

- 1) The candidate visited MMCF ((V)MMCF) checks with the candidate visited RACF ((V)RACF) to verify available resources on the candidate access links.
- 2) The candidate (V)RACF interacts with the home RACF ((H)RACF) to retrieve the original session information, such as QoS resource information.
- 3) The candidate (V)RACF responds to the candidate (V)MMCF to confirm the status of the checked user.

Resource re-provisioning:

- 1) The (V)MMCF sends a request to the (V)RACF to reserve the resources of the moved UE by providing address binding information.
- 2) The (V)RACF reserves session QoS resources, and the (V)RACF responds to the (V)MMCF to confirm the status of reservation operation.
- 3) The (V)MMCF sends a request to the (H)RACF through the (V)RACF or the (H)MMCF to release the resources for the original session.

Figure 8 depicts a general network configuration involving inter-operator communication in support of handover when resource initiation is triggered by the MMCF.

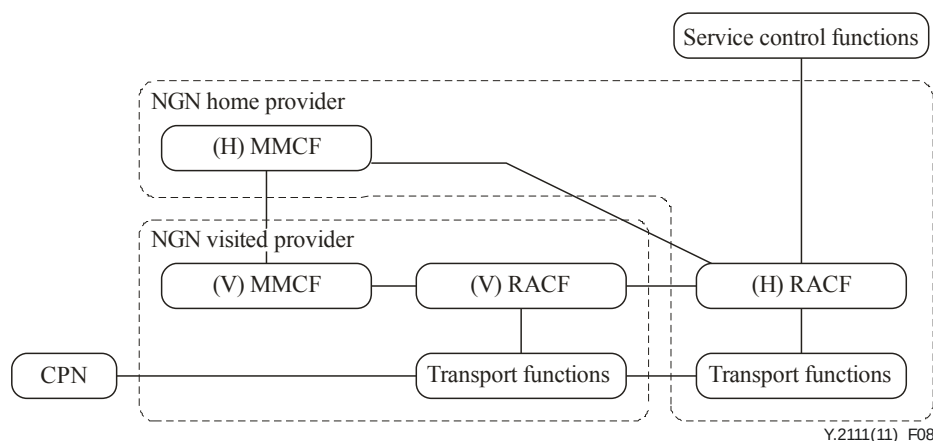


Figure 8 – Inter-operator communication for a handover scenario

NOTE – Inter-MMCF communication across domains is outside the scope of this Recommendation.

7.6 Resource control mechanisms and scenarios for RACF and MPM interactions

It is recommended to support interactions between RACF and MPM under the following situations:

- In the NGN, abnormal situations (e.g., congestion, packet loss, and delay) can occur regardless of bandwidth resource availability for various reasons. The causes can be physical (e.g., link failure and system down) or logical (e.g., routing loop). The physical failure can be reported to the RACF without involving the MPM. Nevertheless, the MPM can provide additional performance information besides bandwidth such as delay, delay variation, and packet loss which will help to make more accurate admission decisions in case of a logical failure situation.
- In a normal situation, in addition to bandwidth, network policy rules, and subscription information, performance information such as delay, delay variation, and packet loss may still be needed when RACF makes admission decisions.
- Upon receipt of an explicit request from the SCF including an indication of specific performance monitoring, the RACF can communicate with the MPM to perform the request and receive status reports of the requested performance monitoring.
- Upon receipt of the network performance information from the MPM, the RACF or the SCF decides to adjust the allocated resource, if necessary.

The descriptions about the communication between the RACF and the MPM are listed in Annex A.

The details about the scenario, mechanism, and interfaces of the MPM are described in Appendix X.

7.7 Resource control cooperation between the RACF and RACF-like resource control functions

It is recommended to support cooperation between the RACF and RACF-like resource control functions under the following two situations:

- 1) The CPE connected to an RACF-controlled network requests an application-specific service with another CPE connecting a network controlled by RACF-like functions. The SCF in the RACF-controlled network has the capability of negotiating with application functions (AF, an SCF equivalent) in the network controlled by RACF-like functions (which could be fixed or mobile) according to the service QoS profile. In this situation:
 - a) The SCF negotiates with the AF to achieve the corresponding QoS profile based on their own policy database.

- b) The SCF in the RACF-controlled network requests QoS resource authorization and reservation from the RACF according to the corresponding QoS profile.
 - c) An AF in a network controlled by RACF-like functions requests QoS resource authorization and reservation from the RACF-like functions.
 - d) RACF makes the final policy decisions and performs the policy-based transport resource control upon the request of the SCF without negotiation with RACF-like functions.
- 2) The CPE connecting a network controlled by RACF-like functions requests an application-specific service from the SCF in an RACF-controlled network. In this situation:
- a) The SCF in an RACF-controlled network requests QoS resource authorization and reservation from the RACF according to the service QoS profile.
 - b) The RACF negotiates directly or indirectly with RACF-like functions to achieve the corresponding QoS profile based on transport resource availability and its policy rules.
 - c) The RACF performs the policy-based transport resource control of an RACF-controlled network according to the corresponding QoS profile.
 - d) RACF-like functions perform the policy-based transport resource control of a network controlled by RACF-like functions according to the corresponding QoS profile.

8 Functional architecture

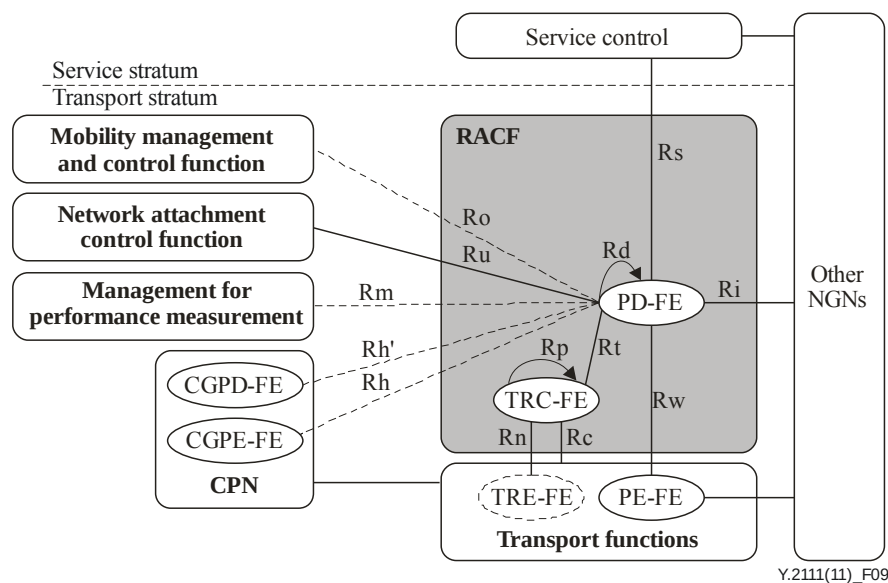


Figure 9 – Generic resource and admission control functional architecture in NGN

Figure 9 describes the functional architecture with functional entities and the relevant reference points. This architecture includes:

- SCF (service control functions);
- PD-FE (policy decision functional entity);
- TRC-FE (transport resource control functional entity);
- TRE-FE (transport resource enforcement functional entity);
- PE-FE (policy enforcement functional entity);
- CGPD-FE (CPN gateway policy decision functional entity);

- CGPE-FE (CPN gateway policy enforcement functional entity);
- NACF (network attachment control functions);
- MMCF (mobility management and control function);
- MPM (management of performance measurement).

The CPE/CPN may be connected to the PE-FE in access network domains and the PE-FE can reside at the network boundary to interconnect with other NGNs.

NOTE – It is foreseen that for efficient support of IPTV services the CPN would include the CPN gateway policy decision functional entity (CGPD-FE) and require direct interactions and a new reference point between the CGPD-FE and the PD-FE. Such interactions and reference point are for further study.

Other NGNs may include access networks only or core networks only or both them. The transport functions could also apply to access networks and core networks. NGN is recommended to allow both IPv4 and IPv6, so the impacts of NATs on the architecture and reference points (e.g., Rs and Rw) are required to be considered as a whole. The NACF is required to be connected to the PD-FE in access network domains. The MMCF is required to have a reference point with the PD-FE to support QoS updates for mobile nodes. The dashed line for TRE-FE and reference point Rn is for further study. Note that the Rc reference point may be connected to any instances of the transport functions as needed, including the PE-FE, TRE-FE and other transport processing functional entities in the transport stratum defined in [ITU-T Y.2012], to obtain the pertinent information.

Administrative domains are not represented in Figure 9. At least one PD-FE is required to be deployed in each network administrative domain (e.g., access network domain and/or core network domain) with associated PE-FEs and TRC-FEs. Depending on the business model and implementation choices, the RACF may be present in an access network domain or core network domain, or may be present in both access and core network domains. The implementation and physical configuration of the PD-FE and TRC-FE are flexible; they can be distributed or centralized, and may be a stand-alone device or part of an integrated device. Appendix I depicts some implementation examples.

8.1 Overview

The RACF consists of two types of resource and admission control functional entities: the PD-FE (policy decision functional entity) and the TRC-FE (transport resource control functional entity). This decomposition of the PD-FE and the TRC-FE enables the RACF to support a variety of access and core networks (e.g., fixed and mobile access networks) within a general resource control framework.

- The PD-FE provides a single contact point to the SCF and hides the details of transport network from the SCF. The PD-FE makes the final decision regarding network resource and admission control based on network policy rules, SLAs, service information provided by the SCF, transport subscription information provided by the NACF in access networks, and resource-based admission decision results provided by TRC-FE. The PD-FE controls the gates in the PE-FEs at a per flow level. The PD-FE consists of transport technology-independent resource control functions and is independent of the SCF as well. The policy rules used by the PD-FE are service-based and are assumed to be provided by the network operators.
 - One PD-FE instance may serve multiple service providers.
 - One PD-FE instance may control all or a sub-set of PE-FE instances belonging to the same domain.
 - Multiple PD-FE instances within the same network operator's domain can be interconnected through the Rd reference point.

- The TRC-FE deals with the diversity of underlying transport technologies and provides the resource-based admission control decision results to the PD-FE. The TRC-FE is service-independent and consists of transport technology-dependent resource control functions. The PD-FE requests the TRC-FE instances in the involved transport networks through the Rt reference point to detect and determine the requested QoS resource along the media flow path. The TRC-FE may collect and maintain the transport network topology and the transport resource status information and authorize resource admission control of a transport network based on network information such as topology and/or connectivity, network and element resource availability, as well as the transport subscription information in access networks.
 - Multiple TRC-FE instances may coexist in a transport network, for the control of different sub-domains or areas without overlapping.
 - Multiple TRC-FE instances in the same core transport network can be interconnected through the Rp reference point.
 - TRC-FE instances in different operators' domains interact indirectly through PD-FE instances.
 - The PD-FE may contact only one designated TRC-FE instance, and then TRC-FE instances communicate with each other through the Rp reference point to detect and determine the requested QoS resource from edge to edge in the involved network; or
 - the PD-FE may contact multiple TRC-FE instances and determine the requested QoS resource from edge to edge in the involved network.
 - Within a single domain, a given TRC-FE instance may interact with multiple PD-FE instances; a given PD-FE instance may interact with multiple TRC-FE instances.

The SCF represents an abstract notion of the functional entities in the service stratum of NGN [ITU-T Y.2012] that request the QoS resource and admission control for media flows of a given service via the Rs reference point.

The NACF includes a collection of functional entities that provide a variety of functions for user access network management and configuration based on the user profiles.

The MMCF includes a collection of functional entities to support mobility in transport stratum.

The MPM includes a collection of functional entities to support the management of performance measurement.

A transport infrastructure is shared among multiple SCF instances and even possibly shared among multiple service providers. Transport resource separation mechanisms (i.e., L1/L2/L3 VPN) may be used among SCF instances for security and network performance.

The PE-FE (policy enforcement functional entity) in the transport stratum is a packet-to-packet gateway at the boundary of different packet networks and/or between the CPN and access network. It is the key injection node to enforce dynamic QoS and resource control, NAPT control and NAT traversal.

The CGPD-FE (CPN gateway policy decision functional entity) in the CPN makes a decision of admission control inside the CPN. It interacts with the PD-FE via the Rh' reference point to exchange CPN admission control policy decision information.

The CGPE-FE (CPN gateway policy enforcement functional entity) in the CPN enforces the transport policy rules for upstream traffic instructed by the PD-FE.

The TRE-FE (transport resource enforcement functional entity) in the transport stratum enforces the transport resource policy rules instructed by the TRC-FE at the technology-dependent aggregate level. Note that the detailed requirements for TRE-FE are different for different transport technologies. These requirements are specified in other related Recommendations (e.g., the MPLS-related specifics are specified in [b-ITU-T Y.2174]).

8.2 Functional entity descriptions

8.2.1 Service control functions (SCF)

The SCF in different domains can interact with the PD-FE via the Rs reference point. The SCF makes requests for transport resources and may receive notifications when resources are reserved and released.

- The SCF is required to provide information to the PD-FE to identify media flows and their required QoS characteristics (e.g., service class, bandwidth).
- The SCF may provide service priority information to the PD-FE to facilitate appropriate priority handling (e.g., priority processing of the resource request, resource pre-emption if needed).
- The SCF may request resource usage information through the PD-FE for charging or other usage metering.
- The SCF may provide service information to the PD-FE to facilitate appropriate dynamic firewall working mode selection.
- The SCF is required to indicate when the resource is to be committed (i.e., opening gate and allocating bandwidth). A resource may either be committed immediately or just reserved for a later commitment.
- When a NAPT function is required, the SCF is required to request address binding (mapping) information and perform required modifications in signalling messages. This includes any address information modifications that may be required for binding.
- When the pull mode along with a path-coupled resource reservation mechanism is used, the SCF is required to indicate to the PD-FE whether it is notified when resources are reserved, modified and released.
- When an authorization token mechanism is used, the PD-FE may provide the SCF one or multiple authorization tokens, which are required to be included in a signalling message to CPE.

8.2.2 Network attachment control functions (NACF)

The NACF provides the following:

- Dynamic provision of IP address and other user equipment configuration parameters.
- Authentication of user access network, prior or during the IP address allocation procedure.
- Authorization of user access network, based on user profiles (e.g., access transport subscription).
- Access network configuration, based on user profiles.
- Location management.

The PD-FE in the access network interacts with the NACF via the Ru reference point to obtain the transport subscription information and the binding information of the logical/physical port address to an assigned IP address.

8.2.3 Mobility management and control function (MMCF)

The MMCF provides IP-based terminal mobility in the control plane of the transport stratum. Details are in [ITU-T Y.2018].

8.2.4 Management of Performance Measurement (MPM)

The MPM provides the management functionality of performance measurement information. Details are in [ITU-T Y.2173].

8.2.5 Resource and admission control functions

8.2.5.1 Overview

Tables 1 and 2 summarize the elementary resource and admission control functions, respectively for PD-FE and TRC-FE. In the following descriptions, technology dependent functions are functions that require specific knowledge of the link-layer technology in use. Technology independent functions are functions that do not require specific knowledge of the link-layer technology in use.

Table 1 – PD-FE elementary functions

Acronym	Function	Description
FDP	Final decision point	Makes the final admission decisions (including priority considerations) in terms of network resources and admission control, based upon requests from the SCF.
QMTI	QoS and priority mapping – technology independent	Maps the service QoS requirements and priority received from the SCF to network QoS parameters (e.g., ITU-T Y.1541 class [b-ITU-T Y.1541]) and priority.
GC	Gate control	Controls the opening and closing of a gate.
IPMC	IP packet marking control	Decides on the packet marking and remarking of IP flows.
NAPTC	NAPT control and NAT traversal	Controls network address translation for both near-end NA(P)T and far-end NA(P)T.
RLC	Rate limiting control	Decides on the bandwidth limit of flows (e.g., for policing).
FWMS	Firewall working mode selection	Selects the working mode of the firewall based on the related service information.
CNPS	Core network path selection	Chooses the core network ingress and/or egress path at the network boundary based on the service information and technology-independent policy rules.
NS	Network selection	Locates core networks and the PE-FE that are involved to enforce the final admission decisions.

Table 2 – TRC-FE elementary functions

Acronym	Function	Description
QMTD	QoS mapping – technology dependent	Maps the network QoS parameters to transport (technology-dependent) QoS parameters.
TDDP	Technology dependent decision point	Makes technology-dependent and resource-based admission decisions for both unicast and multicast.
NTM	Network topology maintenance	Collects and maintains the transport network topology information for both unicast and multicast.
NRM	Network resource maintenance	Collects and maintains the transport resource status information for both unicast and multicast.
ERC	Element resource control	Controls the QoS-related resources in the transport elements at the aggregate level (e.g., VLAN, VPN, LSP).
NOTE – The ERC is for further study.		

8.2.5.2 Policy decision functional entity (PD-FE)

The PD-FE handles the QoS resource requests received from the SCF via the Rs reference point or from the PE-FE via the Rw reference point. The PD-FE contains the following functions:

- Final decision point (FDP): This function first checks the QoS resource request based on service information, network policy rules and transport subscription information, and then interacts with the TRC-FE via the Rt reference point to detect and determine the requested QoS resource within the involved access and/or core transport networks.
 - The FDP makes the final admission decision for media flows of a given service based on network policy rules, service information, transport subscription information, and decision on resource availability.
 - The FDP indicates the loss of connectivity: It informs the SCF that the connectivity of the transport resource previously granted is lost. The SCF may request the PD-FE to relinquish all resources associated with the resource control session.
- QoS mapping – technology independent (QMTI): This function maps the service QoS parameters and priority received from the SCF via the Rs reference point to network QoS parameters (e.g., ITU-T Y.1541 class) and priority based on the network policy rules.
- Gate control (GC): This function controls the PE-FE to install and enforce the final admission decisions via the Rw reference point (e.g., opening or closing the gate). The action to pass or drop IP packets is based on a set of IP gates (packet classifiers, e.g., IPv4 5-tuple) and transport interface identification information (e.g., VLAN/VPN ID) as needed.
- IP packet marking control (IPMC): This function takes decisions on packet marking and remarking of flows. The marking may consider the priority of the flow and traffic engineering parameters.
- NAPT control and NAT traversal (NAPTC): This function interacts with the PE-FE and the SCF to provide the address binding information for NAPT control and NAT traversal as needed.
- Rate limiting control (RLC): This function makes decisions on the bandwidth limits of flows (e.g., for policing).
- Firewall working mode selection (FWMS): This function selects the working mode of the firewall based on the service information. Four packet inspection modes could be identified (static packet filtering, dynamic packet filtering, stateful inspection, deep packet inspection, see also clause 8.2.6.1).

- Core network path selection (CNPS): This function chooses the core network ingress and/or egress path for a media flow based on the service information and technology independent policy rules at the involved PD-FE.
- Network selection (NS): This function locates core networks that are involved to offer the requested QoS resource. It locates the PE-FE instances that are involved to enforce the final admission decisions.

The PD-FE is required to make the final policy decisions based on the service information (e.g., service type, flow description, bandwidth, priority), transport network information (e.g., resource admission result, network policy rules) and transport subscription information (e.g., maximum upstream/downstream capacity). The policy decision is required to provide sufficient information to make the PE-FE perform the resource control operation (e.g., gate opening/closing, bandwidth allocation/rate limiting, packet marking, traffic policing/shaping, NAPT and address latching). The policy decisions may be composed of flow ID, IP addresses, bandwidth, gate status, time/volume limit or traffic descriptor.

The PD-FE can be stateful or stateless depending on the complexity of the specific network environment, application characteristics and deployment architecture.

- The stateless PD-FE only maintains the transaction state information, e.g., state held for the duration of a request-response operation. In order to be stateless, the PD-FE is required to generate the resource control session information for each resource control request from the SCF, which can be stored in the SCF, TRC-FE or PE-FE and used to retrieve the state information together with pertinent information flows.
- The stateful PD-FE may maintain a variety of resource control session information within the PD-FE, such as the session duration, the resource control session information (e.g., the association between the SCF and the PD-FE, the PD-FE and the TRC-FE, the PD-FE and the PE-FE), the resource reservation limit (e.g., time limit/volume limit), resource reservation status (i.e., authorized, reserved, or committed) and physical/logical connection ID.

8.2.5.3 Transport resource control functional entity (TRC-FE)

TRC-FE is responsible for transport technology dependent resource control as follows:

- Resource status monitoring and network information collection
The TRC-FE collects and maintains the network information and resource status information. The resource status information may be specific to the resource based admission control scheme being used by TRC-FE, i.e., whether it is accounting, out-of-band measurements, in-band measurements, or reservation-based.
- Resource based admission control
On receipt of the resource request from the PD-FE, the TRC-FE is required to perform resource based admission control based on the QoS and priority requirements received from the PD-FE (e.g., bandwidth and ITU-T Y.1541 class), in conjunction with the resource utilization information and transport dependent policy rules, and is required to update the resource status and return the result to the PD-FE.
- Transport dependent policy control
Transport dependent policy rules are a set of rules specific to a transport sub-network and technology. The TRC-FE ensures that a request from the PD-FE matches the transport specific policy rules (e.g., access link policy rules, core transport network policy rules), as multiple PD-FEs can request resources from the same TRC-FE. The TRC-FE is required to coordinate the resource requests from PD-FEs and take into account transport dependent policy rules to decide if the resource requests can be supported (e.g., usage/constraints of particular transport QoS class and total capacity).

The TRC-FE provides the following basic functions:

- QoS mapping – technology dependent (QMTD): This function maps the network QoS parameters and classes received from the PD-FE via the Rt reference point to transport (technology dependent) QoS parameters and classes based on specific transport policy rules, and accommodating the diversity of transport technologies.
 - When mapping network QoS parameters to transport (technology dependent) QoS parameters, TRC-FE considers the underlying transport technology. A set of network QoS parameters may be mapped to different sets of transport (technology dependent) QoS parameters based on transport technologies. The TRC-FE has knowledge of the QoS related features of the underlying transport network and map the network QoS parameters to the best matching transport (technology dependent) QoS parameters for given transport technology. The mapping policy rules need to be provided by network operators.
 - Technology dependent decision point (TDDP): This function receives and responds to the QoS resource request from the PD-FE via the Rt reference point and/or from another TRC-FE via Rp reference point for both unicast and multicast. This function detects and determines the availability of requested QoS resource based on the network topology and resource status information, as well the transport subscription information in access networks. It may make path selection between ingress and egress points within its purview of a sub-domain to satisfy the QoS resource requirements. If the requested resource is available, this function updates the resource status to include the new application request and responds to the PD-FE and/or another TRC-FE with a positive answer (e.g., resource available); otherwise, it responds to the PD-FE and/or another TRC-FE with a negative answer (e.g., resource unavailable).
 - Network topology maintenance (NTM): This function collects and maintains the transport network topology information (including unicast and multicast) from transport functions via the Rc reference point. It is possible that the topology information is configured and tracked locally in the TRC-FE. In this case, the Rc reference point is not needed. Note that the reference point that allows the TRC-FE to collect the topology information from the NMS is for further study.
 - Network resource maintenance (NRM): This function collects and maintains the transport resource status information (including unicast and multicast) from transport functions via the Rc reference point. It is possible that the resource information is configured and tracked locally in the TRC-FE. In this case, the Rc reference point is not needed. Note that the reference point that allows the TRC-FE to collect the resource information from the NMS is for further study.
 - Element resource control (ERC): This function controls the QoS-related resources in the intermediate transport elements at the aggregate level (e.g., VLAN, VPN, LSP). Note that the ERC is for further study.

The implementation of the TRC-FE in various access networks may be different according to access transport technologies and corresponding QoS mechanisms in the data plane. The implementation of the TRC-FE may be different in various core networks according to core transport technologies and corresponding QoS mechanisms in the data plane.

Multiple TRC-FE instances can be interconnected in the same core transport network, and one or more of those instances may be co-located with transport functions (for example, MTCF and MRF), in support of different types of admission control (for example, multicast admission control). The TRC-FE instance that is directly connected to the PD-FE is called top-tier TRC-FE. The TRC-FE instance that is connected to top-tier TRC-FE and co-located with transport functions is called co-located TRC-FE. The following operation modes are supported by the TRC-FE and the Rp reference point:

- **Outsourcing mode**

The co-located TRC-FE makes the resource admission decision for both unicast and multicast services; the top-tier TRC-FE queries the co-located TRC-FE for resource admission in the relevant network segment. The outsourcing mode can be performed at either media flow level or aggregate level. The outsourcing mode is suitable for the dynamic resource approach, i.e., the resources are fully shared by unicast and multicast.

- **Designating mode**

The co-located TRC-FE performs resource admission control for unicast and/or multicast services respectively within the pre-provisioned threshold of aggregate resources; the top-tier TRC-FE is entitled to adjust the threshold of aggregate resources based on the resource utilization or upon the request of co-located TRC-FE. The designating mode can only be performed at the aggregate level. The designating mode is suitable for adjustable resource approach, i.e., the dedicated resources are provisioned to unicast and multicast services.

- **Reporting mode**

The co-located TRC-FE makes the resource admission decision for multicast services and the top-tier TRC-FE makes the resource admission decision for unicast services. Based on the predefined provider's policy, the co-located TRC-FE reports the resource status information to the top-tier TRC-FE. The co-located TRC-FE and top-tier TRC-FE interact with each other to maintain the consistency of the resource status information. The granularity of interaction between top-tier TRC-FE and co-located TRC-FE can be either at per session level. Note that this mode is required to follow a restricted procedure such as shown in Appendix IV. The reporting mode is suitable for dynamic resource approach, i.e., the resources are fully shared by unicast and multicast.

Further detailed mechanisms are described in Appendix IV.

Appendix II elaborates on the TRC-FE over different transport technologies.

Examples of methods for detecting and determining resource availability in TRC-FE: refer to Appendix III.

8.2.6 Transport functions

Note that the transport functions described in the following clauses only pertain to the entities interacting with the RACF.

8.2.6.1 Policy enforcement functional entity (PE-FE)

The PE-FE enforces the network policy rules instructed by the PD-FE on a per-subscriber and per-IP flow basis. It is recommended that the PD-FE be able to perform the following functions based on flow information such as classifier (e.g., IPv4 5-tuple) and flow direction, as well as transport interface identification information (e.g., VLAN/VPN ID, LSP label) as needed. The functions of the PE-FE include:

- **Opening and closing gate:** enabling or disabling packet filtering for an IP media flow.
A gate is unidirectional, associated with a media flow in either the upstream or downstream direction. When a gate is open, all of the packets associated with the flow are allowed to pass through; when a gate is closed, all of the packets associated with the flow are blocked and dropped.
- **Rate limiting and bandwidth allocation.**
- **Traffic classification and marking.**
- **Traffic policing and shaping.**
- **Mapping of IP-layer QoS information onto link layer QoS information based on predefined static policy rules (e.g., setting 802.1p priority values).**

- Network address and port translation.
- Media relay (i.e., address latching) for NAT traversal.
- Collecting and reporting resource usage information (e.g., start-time, end-time, and octets of sent data).
- Packet-filtering-based firewall: inspecting and dropping packets based on predefined static security policy rules and gates installed by the PD-FE.

There are four packet inspection modes for packet-filtering-based firewall:

- static packet filtering: inspecting packet header information and dropping packets based on static security policy rules. This is the default packet inspection mode applied for all flows;
- dynamic packet filtering: inspecting packet header information and dropping packets based on static security policy rules and dynamic gate status;
- stateful inspection: inspecting packet header information as well as TCP/UDP connection state information and dropping packets based on static security policy rules and dynamic gate status;
- deep packet inspection: inspecting packet header information, TCP/UDP connection state information and the content of payload together, and dropping packets based on static security policy rules and dynamic gate status.

8.2.6.2 CPN gateway policy decision functional entity (CGPD-FE)

The CGPD-FE makes decisions in the CPN gateway regarding network resource and admission control. In particular, the CGPD-FE provides gate control functionality, i.e., dynamic NAT and firewall functions at the boundary between the CPN gateway and the NGN.

A detailed definition of the CGPD-FE is for further study.

8.2.6.3 CPN Gateway policy enforcement functional entity (CGPE-FE)

The CGPE-FE enforces the network policy rules and the transport resource policy rules instructed by the PD-FE for upstream traffic on a per-subscriber and per-flow basis. It performs the following functions based on flow information such as classifier (e.g., IPv4 5-tuple) and flow direction, as well as transport interface identification information (e.g., VLAN, ATM VPC/VPI) as needed:

- Opening and closing gate: enabling or disabling packet filtering for an media flow.
A gate is unidirectional, associated with a media flow in either the upstream or downstream direction. When a gate is open, all of the packets associated with the flow are allowed to pass through; when a gate is closed, all of the packets associated with the flow are blocked and dropped.
- Rate limiting and bandwidth allocation.
- Traffic classification and marking.
- Traffic policing and shaping.
- Mapping of IP-layer QoS information onto link layer QoS information based on predefined static policy rules (e.g., setting 802.1p priority values).
- Collecting and reporting resource usage information (e.g., start-time, end-time, and octets of sent data).

8.2.6.4 Transport resource enforcement functional entity (TRE-FE)

The TRE-FE enforces the transport resource policy rules instructed by the TRC-FE at the technology-dependent aggregate level (e.g., VLAN, VPN and MPLS). It is recommended that the TRE-FE be able to perform the functions based only on transport link information (e.g.,

VLAN/VPN ID, and LSP label). For example a TRE-FE may be used to modify the bandwidth associated with an LSP, or to set ATM traffic management parameters such as cell rate or burst size.

Note that the detailed requirements for TRE-FE are different for different transport technologies. These requirements are specified in other related Recommendations (e.g., the MPLS-related specifics are specified in [b-ITU-T Y.2174]).

8.3 Mechanisms

8.3.1 Selection mechanisms

In order to transfer the resource control requests between relevant functional entities (such as between the SCF and the PD-FE, the PD-FE and the TRC-FE, the PD-FE and the PE-FE, the TRC-FE and the TRC-FE, or the PD-FE and the PD-FE), two operations are performed: discovery and selection.

Discovery mechanism

A functional entity discovers the communicating parties by the following mechanisms:

- Static mechanism: A functional entity may obtain the topology and connectivity information of all relevant communicating parties from statically configured location information, which includes either the IP address or the fully qualified domain name (FQDN). This information would be retrieved through, for example, the DNS.
- Dynamic mechanism: A functional entity may formulate the topology and connectivity information of all relevant communicating parties and update the information automatically.

In this Recommendation, the static mechanism is mandatory and the dynamic mechanism is optional.

Selection mechanism

A functional entity selects a specific instance from the list of communicating parties that are discovered. The information such as the type of service and a set of service attributes, globally unique IP addresses or the end user's identifier can be used to identify the specific communicating party.

The PD-FE identifier, resource control session identifier, and globally unique IP address information (or transport subscriber identifier) are required by pertinent reference points (such as Rs, Rw, Rt, Ri, Rd and Rp) in support of a selection mechanism.

8.3.2 Binding mechanisms

The RACF is required to use one of the following mechanisms for binding the media flow QoS request with the policy decision information in support of policy enforcement in the PE-FE when transport signalling is applied to pull the policy decision information from the PD-FE:

- 1) Authorization token: The PD-FE generates an authorization token upon resource request from the SCF. The authorization token contains the fully qualified domain name of the PD-FE and a resource control session ID in the PD-FE, which allows the PD-FE to uniquely identify the resource request.
- 2) Source address of media flow (e.g., globally unique IP address): When neither near-end NAPT nor far-end NAPT is deployed between the CPE and the SCF, the end user globally unique IP address is used for the binding. Otherwise, the source address of the media flow received by the access gateway is required to be used for the binding. The fully qualified domain name of the PD-FE and the resource control session ID can be derived based on the source address of the media flow.



- 3) Source address of media flow and other filters (e.g., media flow classifier): When multiple simultaneous media flows are provisioned in a session, the source address may not be adequate to identify a unique binding; other filters such as the port number of source address, destination address and port number, and protocol number may be used with the source address for the binding. The fully qualified domain name of the PD-FE and the session ID are derived based on the source address of media flow and other applied filter information.
- 4) Transport subscriber identifier: When the transport subscription information is needed by the RACF for policy decision and resource control, the transport subscriber identifier may be used for accessing the subscription profile in the NACF directly.

9 Reference points

NOTE – By default, all information components in an information flow defined in clause 9 are to be considered "mandatory" unless they are explicitly identified as being "optional."

9.1 Reference point Rs

The Rs reference point allows QoS resource request information needed for QoS resource authorization and reservation to be exchanged between the PD-FE and the SCF. Either the push or pull mode may be used. The Rs reference point is required to be able to support resource control for both fixed and mobile networks, and is recommended to support NAPT/firewall control and NAT traversal at the PE-FE as needed.

The Rs reference point may operate as an intra-domain or an inter-domain reference point.

9.1.1 Functional requirements

9.1.1.1 Resource control functional requirements

The Rs reference point provides the ability for the SCF to make requests:

- for resource authorization and reservation for a media flow;
- for QoS handling;
- for priority handling;
- for gate control of a media flow;
- to insert the NAPT function and request address mapping information;
- for dynamic firewall working mode selection;
- for resource usage information.

In addition, the SCF can request notification of events.

9.1.1.2 Resource control session processing functional requirements

To assure the reliability and performance of resource control session operations across the Rs reference point, the following capabilities are required:

Overload control: The Rs reference point is required to provide the capability to support overload control for preventing the overflow of information messages exchanged between the SCF and the PD-FE.

Synchronization and audit: The Rs reference point is required to provide the capability to support synchronization and audit of the resource control session status in support of recovery and operational information statistics and auditing.

Session state maintenance: When a stateful PD-FE is used, it is required to be able to maintain the session state using either soft-state or hard-state approaches. The reservation holding time specifies the time limitation in support of abnormal recovery. When a stateless PD-FE is used, the resource control session information passed by the SCF or PE-FE can be used to derive the session state and relevant information.

9.1.2 Information exchange requirements

This clause provides a brief description of the information exchange requirements for the Rs reference point.

Request-response transactions: The reference point is required to allow the SCF to request a transaction to be performed by the PD-FE and get a response (that can be correlated with the request) in return.

Notifications: The reference point is required to support the notification of asynchronous events (from the PD-FE to the SCF).

Reliable delivery: The reference point is required to provide reliable delivery of messages.

Capabilities: The SCF is required to be able to determine the capabilities of appropriate PD-FE instance when requesting resources and other transport plane functions.

Security: The Rs is required to support the authentication between the SCF and the PD-FE such that requests to the PD-FE from unauthenticated sources will not be performed and such that the SCF can verify the source of notifications sent from the PD-FE. Refer to clause 11 for other security requirements.

One-to-many/many-to-one: Two modes are required to be supported: 1) One-to-many mode: a SCF is required to be able to communicate with multiple PD-FEs; 2) Many-to-one mode, multiple SCF instances are required to be able to make requests to a given PD-FE. Only a single SCF will make a request to a given PD-FE for a particular session.

Granularity of resource control: The Rs reference point is required to support resource control operations (including resource authorization, reservation, commitment, modification and termination) at different levels of granularity. A single resource control request may combine one or several media flows from a single application session, or from a single SCF, or from a provider domain.

For example,

- The change of any individual media flow within an existing resource control session invokes the operation of resource modification to that media flow.
- The failure of any individual elements (e.g., transport link failure) invokes the operation of resource termination to all affected media flows.

Level of resource control: The Rs reference point is required to support the resources control for the media flow level.

NOTE – Rs resource control for aggregate level is outside the scope of this Recommendation.

9.1.3 Information components

The information components exchanged across the Rs reference point are categorized as follows:

9.1.3.1 Resource control processing information components

The information components for resource control request processing (e.g., discovery, binding, overload control and state maintenance) are described in Table 3.

Table 3 – Resource control processing information components (Rs)

Information component	Description
SCF identifier	A unique identifier for different instances of the SCF within the same administrative domain of a single requester.
Resource control session identifier	An identifier for the session, which may be composed of multiple media flows for which the resource reservation requests are sent to the RACF. The identifier has to be unique within the same SCF instance.
Globally unique IP address information (Optional, Note 1)	A set of IP address information used for locating the access network in which the CPE is requesting the transport resource.
– Unique IP address	The IP address for identifying the CPE.
– Address realm	The addressing domain of the IP address (e.g., Subnet prefix or VPN ID).
Transport subscriber identifier (Optional, Note 1)	A globally unique identifier for the CPE requesting the transport resource. This identifier can be used for locating the transport subscription information for the CPE.
Resource requester identifier	An identifier for the requester (i.e., the owner of the SCF (e.g., a service provider)) of resource control service. It is unique over the requesters sending requests for the resource control to the same RACF domain.
Resource request priority (Optional)	The indication of the importance of a resource control request. It can be used for processing simultaneous requests by the PD-FE based on the priority level.
Reservation holding time (Optional)	The value of time interval for which the resource is reserved, which can be initiated by an SCF based on the service requirement and/or granted by a PD-FE based on the network policy decision. The PD-FE is required to release the session when the holding time has expired.
Invitation indication (Optional)	The indication of invitation. It represents the current service is provided by invitation. In this case, the PD-FE makes the policy decisions based on the resource availability and network policy rules.
Resource control session information (Optional)	The record of the resource control session information. This is used for deriving the session state and other information (e.g., association of the SCF and the PD-FE) and only has a local significance between the PD-FE and the SCF. This component is only applicable when a stateless PD-FE is deployed.
NOTE 1 – One of the globally unique IP addresses or transport subscriber identifiers is recommended to be present. NOTE 2 – Only the optional component is explicitly indicated. The use of each information component (i.e., mandatory or optional) also refers to the specific information flows in clause 9.1.4. NOTE 3 – How the SCF obtains the information of transport subscriber ID is an issue for service stratum functionality.	

9.1.3.2 QoS resource information components

The QoS resource information sub-components for media session and media flows are described in Table 4.

Table 4 – QoS resource information sub-components (Rs)

Information component	Description
Media profile	A set of information sub-components for a media session, which may be composed of data flows and control flows (e.g., RTP and RTCP flows for a VoIP call). The sub-components in a media profile can be represented by a wildcard as needed.
– Media number	An identifier for a media session (e.g., ordinal number of the position of the "m=" line in the SDP).
– Type of service	Indication of service type for the media data flow (e.g., voice, video telephony, or streaming video).
– Application class of service (Optional)	The application service class for the media (e.g., first class) is of local significance between the resource request client (i.e., the owner of SCF) and the owner of the PD-FE, and is to be converted by the PD-FE to a network class of service (e.g., ITU-T Y.1541 class for performance requirement) based on SLA and network policy rules.
– Media priority (Optional)	Information for priority handling (e.g., TDR/emergency telecommunications service (ETS)).
– Restoration indication (Optional)	It is used to indicate whether the QoS of a request can be restored or not. If the QoS of the existing session has been downgraded, the SCF can indicate to the RACF to check whether the QoS of this session can be restored or not.
– Downgraded indication (Optional)	It is used to indicate whether the QoS of an existing session has been downgraded or not. In the roaming scenario, the requester (the home RACF) informs the visited RACF whether the QoS of the current session has been downgraded or not.
– Downgradability indication (Optional)	It is used to indicate whether the QoS of an incoming or existing session is downgradable or not.
– Media flow description	A set of sub-components of individual or a group of media flows within a media session.

The information sub-components of the media flow description are described in Table 5.

Table 5 – Media flow description sub-components (Rs)

Information component	Description
Media flow description	A set of sub-components of individual media flows or a group of media flows within a media session. The sub-components of a media flow description can be represented by a wildcard as needed.
– Flow direction (in->out, out->in, bidirectional)	Direction of the media flow, where "in" refers to inside the core network so that "out->in" refers to the direction towards the core network.
– Flow number	An identifier for the individual media flow within a media session.
– Flow status	Instruction and indication of enabled or disabled status for a media flow.
– Protocol version	The version of source and destination unicast network address protocol (e.g., IPv4 or IPv6).

Table 5 – Media flow description sub-components (Rs)

Information component	Description
– IP addresses	The source and destination network addresses.
– Ports	The source and destination port numbers. Port ranges are required to be supported (e.g., two consecutive ports for RTP, RTCP).
– Protocol number	The protocol ID (e.g., UDP, TCP).
– Bandwidth	The requested maximum bandwidth. The upstream and downstream bandwidth is recommended to be provided separately.

9.1.3.3 Authorization token information component

The information component used for binding purposes in the pull mode is described in Table 6.

Table 6 – Authorization token information component (Rs)

Information component	Description
Authorization token (Optional)	A unique identifier used in policy pull mode. The token is requested by the SCF and provided in a response by the PD-FE.

9.1.3.4 Charging correlation information component

This information component provides the resource usage information, see Table 7.

Table 7 – Charging correlation information component (Rs)

Information component	Description
Charging correlation information (Optional)	Charging correlation information, such as charging ID of the SCF and networks, and resource usage information.

9.1.3.5 Resource control action information components

A variety of indicators are used to request a specific resource control action per network event/condition, see Table 8.

Table 8 – Resource control action information components (Rs)

Information component	Description
Resource Reservation Mode	Indication of resource reservation mode (e.g., non-reservation, reservation only or reservation + commitment). In the pull mode of the QoS control scenario, the "non-reservation" option is used. In the push mode, either the "reservation only" or the "reservation + commit" option is used.
Dynamic firewall working mode (Optional)	Service information for dynamic firewall working mode selection (e.g., security level).
Resource Request Result	Indication of the result for a resource request (initiation, modification, release).
Timestamp	The time when the resources were lost.