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

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/.

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

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.

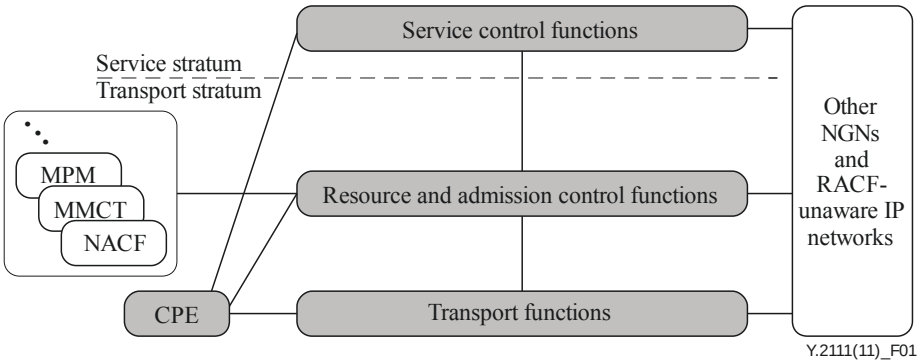


Figure 1 – RACF within the NGN architecture

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.

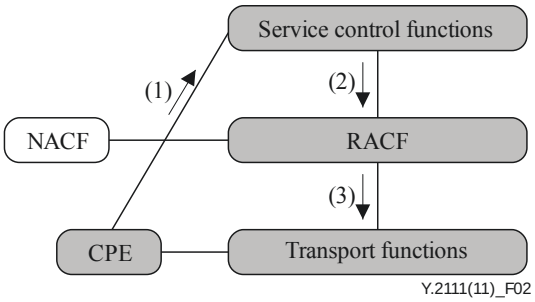


Figure 2 – Flow diagram for scenario 1

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.

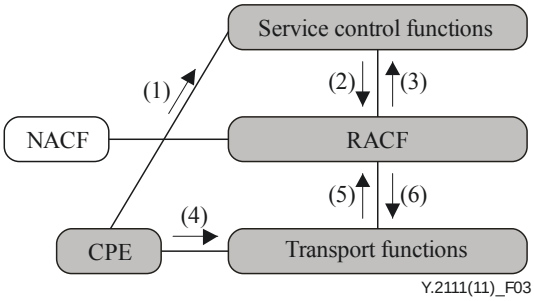


Figure 3 – Flow diagram for scenario 2

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.

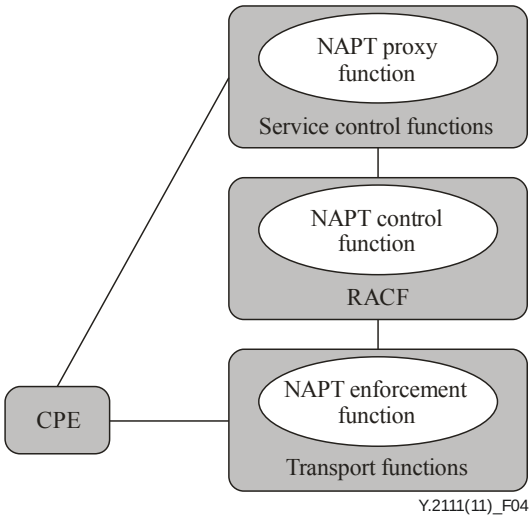


Figure 4 – NAPT and NAT traversal control mechanisms

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.

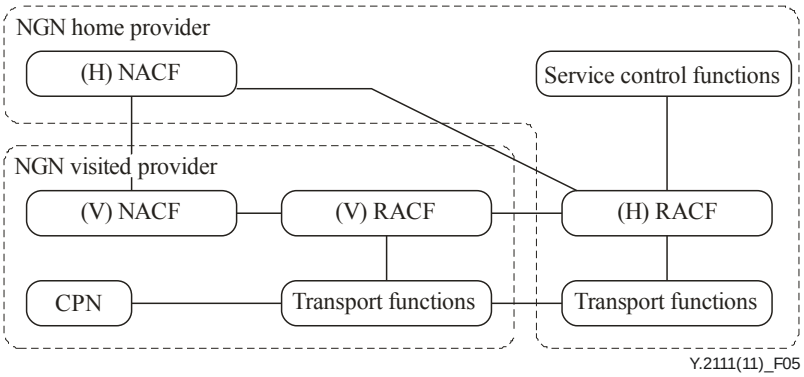


Figure 5 – Inter-operator communications for a nomadicity scenario

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.

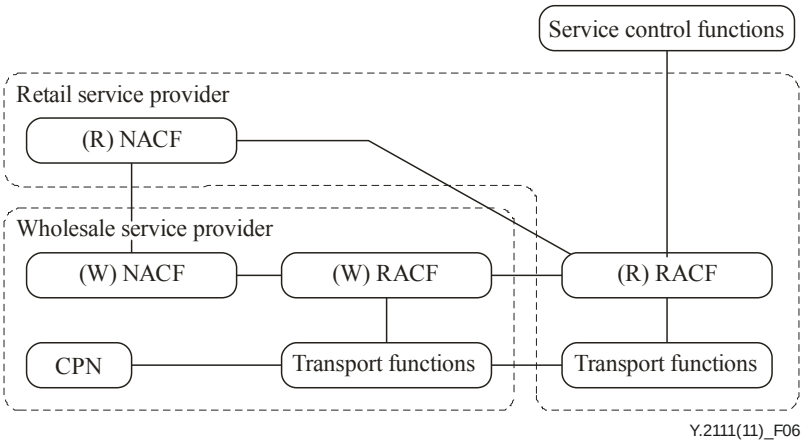


Figure 6 – Inter-operator communications for a wholesale scenario

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.

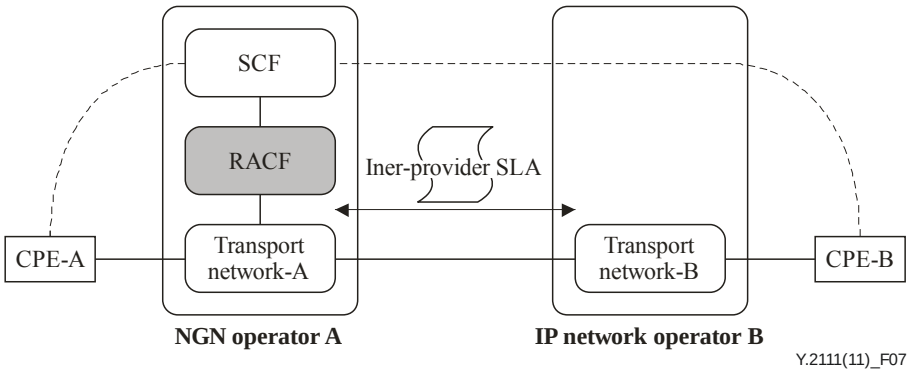


Figure 7 – Inter-operator communication between NGNs and RACF-unaware IP networks

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.

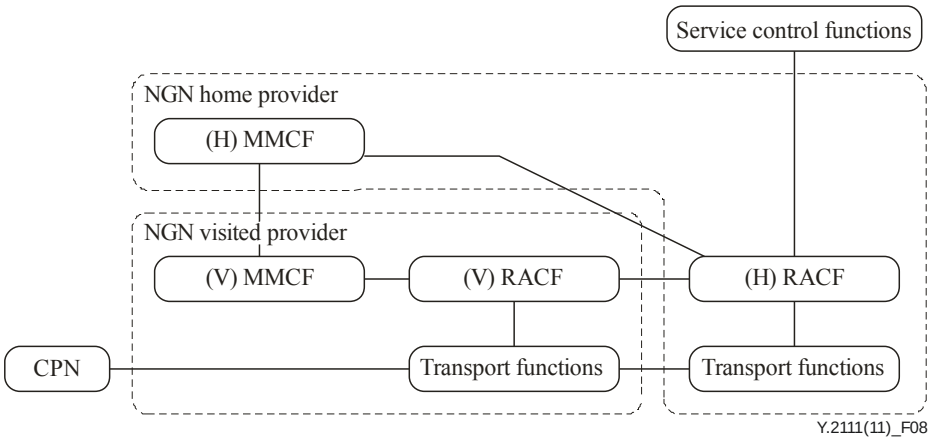


Figure 8 – Inter-operator communication for a handover scenario

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:

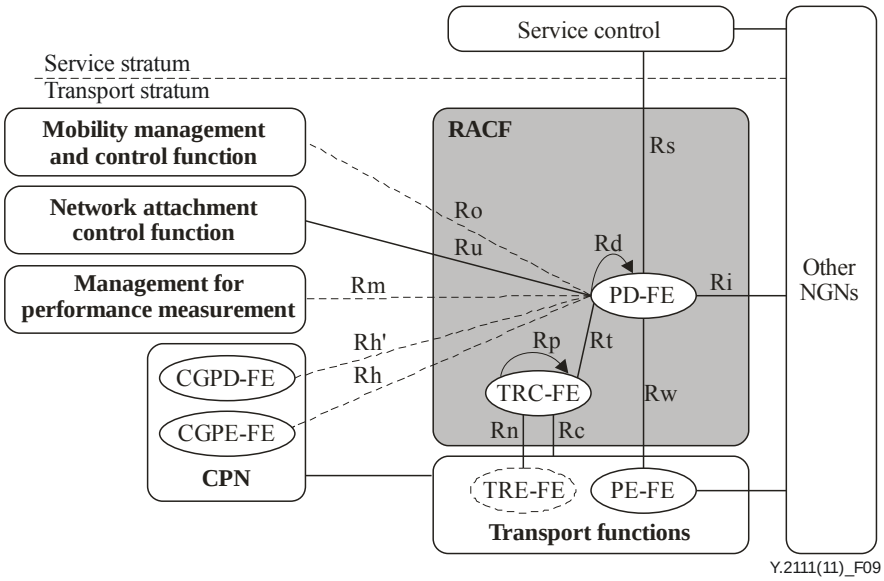
a) The SCF in an RACF-controlled network requests QoS resource authorization and reservation from the RACF according to the service QoS profile.

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



NOTE – Dashed lines mean optional reference points.

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 NAPT 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.

Table 8 – Resource control action information components (Rs)

Information component	Description
Reason	Information describing the cause for an event (e.g., Abort event).
Event notification indication (Optional)	A set of information sub-components indicating the query and notification of a transport event. Note that the listed sub-components may not include all event notifications. Extra events can be added.
– Resource information indicator	Indication of a request for resource information. It is used by the SCF to ask the PD-FE to include the modified service information (such as available bandwidth) in the response message, or is used by the PD-FE to retrieve the original service information when an event occurs (e.g., node failure).
– Transport loss indicator	The SCF's subscription for the notification of the transport loss events, or notification of a transport loss event to the SCF.
– Transport recovery indicator	The SCF's subscription for the transport recovery events, or notification of a transport recovery event.
– Transport release indicator	The SCF's subscription for the transport release events, or notification of a transport release event to the SCF.
NAPT control and NAT traversal Indication (Conditional)	A set of information subcomponents indicating the existence of near-end and/or far-end NAPTs. The events of NAPT control and NAT traversal are not mutually exclusive. They can be used in the same information flow.
– Address translation command	Indication to the SCF for signalling message modification for near-end NAPT. The PD-FE may perform the NAPT control, obtain the address binding information, and request the SCF to modify signalling messages accordingly based on network address hiding policy decision.
– Address binding information request	Indication of the presence of far-end NAT traversal issued by the SCF. The SCF may ask the RACF for the network address and port translation information (e.g., address latching) in support of far-end NAT traversal.
– Address binding information response	Indication to the SCF for the response of address latching for far-end NAT traversal. The PD-FE is required to obtain the NAPT information, generate the address binding information and send it to relevant SCF instance. The SCF is required to modify the message body of application signalling accordingly.

9.1.4 Information flows exchanged over Rs

This clause describes the information flows (namely requests and responses) exchanged over Rs.

9.1.4.1 Resource initiation request

The resource initiation request information flow is sent by the SCF to the PD-FE initiate a resource control session. Depending on the resource reservation mode desired, a single resource initiation request may be used for authorization only or reservation only or commitment only or some combination of the above. It contains the following information components:

- SCF identifier
- Resource control session identifier
- Globally unique IP address information (Optional, see Note)
  - Unique IP address
  - Address realm
- Transport subscriber identifier (Optional, see Note)
- Resource requester identifier
- Resource request priority (Optional)
- Reservation holding time (Optional)
- Invitation indication (Optional)
- Resource control session information (Optional)
- Dynamic firewall working mode (Optional)
- Authorization token (Optional)
- Charging correlation information (Optional)
- Media profile
  - Media number
  - Type of service
  - Application class of service (Optional)
  - Media priority (Optional)
  - Restoration indication (Optional)
  - Downgraded indication (Optional)
  - Downgradability indication (Optional)
  - Media flow description
    - Flow direction
    - Flow number
    - Flow status
    - Protocol version
    - IP addresses
    - Ports
    - Protocol number
    - Bandwidth
- Resource reservation mode
- Event notification indication (Optional)
  - Resource information indicator
  - Transport loss indicator
  - Transport recovery indicator

  - Transport release indicator
- NAPT control and NAT traversal (Conditional)
  - Address binding information request

NOTE – At least of one of the above information components is required to be present.

9.1.4.2 Resource initiation response

The request initiation response information flow is sent by the PD-FE to the SCF to confirm the resource initiation request of the SCF. It contains the following information components:

- SCF identifier
- Resource control session identifier
- Reservation holding time (Optional)
- Resource control session information (Optional)
- Resource request result
- Authorization token (Optional)
- Media profile (Optional)
  - Media number
  - Type of service
  - Application class of service (Optional)
  - Media priority (Optional)
  - Restoration indication (Optional)
  - Downgraded indication (Optional)
  - Downgradability indication (Optional)
  - Media flow description
    - Flow direction
    - Flow number
    - Flow status
    - Protocol version
    - IP addresses
    - Ports
    - Protocol number
    - Bandwidth
- NAPT control and NAT traversal (Conditional)
  - Address translation command
  - Address binding information response

9.1.4.3 Resource modification request

The resource modification request information flow is sent by the SCF to the PD-FE to request the modification of the resources assigned to an established session. The session state can be retrieved with the resource control session information provided by the SCF if a stateless PD-FE is used. It contains the following information components:

- SCF identifier
- Resource control session identifier
- Resource requester identifier

- Resource request priority (Optional)
- Reservation holding time (Optional)
- Invitation indication (Optional)
- Resource control session information (Optional)
- Dynamic firewall working mode (Optional)
- Charging correlation information (Optional)
- Media profile
  - Media number
  - Type of service
  - Application class of service (Optional)
  - Media priority (Optional)
  - Restoration indication (Optional)
  - Downgraded indication (Optional)
  - Downgradability indication (Optional)
  - Media flow description
    - Flow direction
    - Flow number
    - Flow status
    - Protocol version
    - IP addresses
    - Ports
    - Protocol number
    - Bandwidth
- Resource reservation mode
- Event notification indication (Optional)
  - Resource information indicator
  - Transport loss indicator
  - Transport recovery indicator
  - Transport release indicator
- NAPT control and NAT traversal (Conditional)
  - Address binding information request

9.1.4.4 Resource modification response

The resource modification response information flow is sent by the PD-FE to the SCF to confirm that the resource modification request made by the SCF has been received and to indicate the result. The information within this flow is the same as that in the resource initiation response information flow.

9.1.4.5 Resource action request

The resource action request information flow is sent by the PD-FE to the SCF as needed to request a specific resource control action (e.g., retrieving the resource information) for an established session. It contains the following information components:

- SCF identifier

- Resource control session identifier
- Resource control session information (Optional)
- Dynamic firewall working mode (Optional)
- Charging correlation information (Optional)
- Media profile
  - Media number
  - Type of service
  - Application class of service (Optional)
  - Media priority (Optional)
  - Restoration indication (Optional)
  - Downgraded indication (Optional)
  - Downgradability indication (Optional)
  - Media flow description
    - Flow direction
    - Flow number
    - Flow status
    - Protocol version
    - IP addresses
    - Ports
    - Protocol number
    - Bandwidth
- Event notification indication (Optional)
  - Resource information indicator
  - Transport loss indicator
  - Transport recovery indicator
  - Transport release indicator
- NAPT control and NAT traversal (Conditional)
  - Address translation command
  - Address binding information response

9.1.4.6 Resource action response

The resource action response information flow is sent by the SCF to the PD-FE to confirm that the request for the specific action has been received and to provide the requested service information. It contains the following information components:

- SCF identifier
- Resource control session identifier
- Resource requester identifier
- Resource request priority (Optional)
- Resource control session information (Optional)
- Dynamic firewall working mode (Optional)
- Charging correlation information (Optional)
- Media profile (Optional)

  - Media number
  - Type of service
  - Application class of service (Optional)
  - Media priority (Optional)
  - Restoration indication (Optional)
  - Downgraded indication (Optional)
  - Downgradability indication (Optional)
  - Media flow description
    - Flow direction
    - Flow number
    - Flow status
    - Protocol version
    - IP addresses
    - Ports
    - Protocol number
    - Bandwidth
- Event notification indication (Optional)
  - Resource information indicator
  - Transport loss indicator
  - Transport recovery indicator
  - Transport release indicator
- NAPT control and NAT traversal (Conditional)
  - Address binding information Request

9.1.4.7 Resource notification

The resource notification information flow is sent by the PD-FE to notify the SCF of transport resource events. It contains the following information components:

- SCF identifier
- Resource control session identifier
- Resource control session information (Optional)
- Dynamic firewall working mode (Optional)
- Charging correlation information (Optional)
- Media profile
  - Media number
  - Type of service
  - Application class of service (Optional)
  - Media priority (Optional)
  - Restoration indication (Optional)
  - Downgraded indication (Optional)
  - Downgradability indication (Optional)
  - Media flow description
    - Flow direction

        - Flow number
        - Flow status
        - Protocol version
        - IP addresses
        - Ports
        - Protocol number
        - Bandwidth
- Event notification indication
    - Resource information indicator
    - Transport loss indicator
    - Transport recovery indicator
    - Transport release indicator

NOTE – The use of this information flow for the notification of resource usage information is for further study.

9.1.4.8 Resource release request

The resource release request information flow is sent by the SCF to the PD-FE to request the release of resources assigned to an established session or individual media flow. The resource release can be resource control session based, flow-based, and a wildcard is used to indicate the release of all of sessions related to this client. When a request is received, all of the relevant resources are released including the transport event notification settings. It contains the following information components:

- SCF identifier
- Resource control session identifier
- Resource requester identifier
- Resource request priority (Optional)
- Resource control session information (Optional)
- Dynamic firewall working mode (Optional)
- Charging correlation information (Optional)
- Media profile
    - Media number
    - Type of service
    - Application class of service (Optional)
    - Media priority (Optional)
    - Restoration indication (Optional)
    - Downgraded indication (Optional)
    - Downgradability indication (Optional)
    - Media flow description
        - Flow direction
        - Flow number
        - Flow status
        - Protocol version
        - IP addresses

- Ports
- Protocol number
- Bandwidth

9.1.4.9 Resource release response

The resource release response information flow is sent by the PD-FE to the SCF to confirm that the resource release request has been received and to indicate the results. It contains the following information components:

- SCF identifier
- Resource control session identifier
- Resource request priority (Optional)
- Resource control session information (Optional)
- Resource request result

9.1.4.10 Abort resource request

The abort resource request information flow is sent by the PD-FE to the SCF to indicate the loss of all resources for the established session to the SCF. It contains the following information components:

- SCF identifier
- Resource control session identifier
- Resource requester identifier
- Resource control session information (Optional)
- Timestamp
- Reason

9.1.4.11 Abort resource response

The abort resource response is sent by the SCF to the PD-FE to confirm a resource abort request. It contains the following information components:

- SCF identifier
- Resource control session identifier
- Resource control session information (Optional)

9.2 Reference point Rw

The Rw reference point allows the final admission decisions to be installed (either pushed or pulled) to the PE-FE from the PD-FE. This reference point is required to be able to support resource control for both fixed and mobile access networks and is recommended to support NAPT/firewall control and NAT traversal at the PE-FE as needed.

The Rw reference point is an intra-domain reference point.

9.2.1 Functional requirements

9.2.1.1 Resource control functional requirements

The Rw reference point allows the PD-FE to push the admission decisions to the PE-FE, and also allows the PE-FE to request the admission decisions when path-coupled resource reservation mechanisms are in use. The PD-FE may specify:

- Resources to be reserved and/or committed for media flows.
- QoS handling such as packet marking and policing to use.

- Gate control (opening/closing) for a media flow.
- The insertion of a NAPT function, requesting the necessary address mapping information.
- Resource usage information request and report for a media flow.
- Dynamic firewall working mode selection for a media flow.
- Technology independent core network ingress/egress path information for a media flow.

In addition, the PD-FE can request notification of events and may receive a request from the PE-FE to verify the resource reservation that it receives from the CPE.

Note that the NAPT function may be contained within the same or a different information flow from the function providing bandwidth reservation. The Rw reference point is recommended to allow for this flexibility.

9.2.1.2 Resource control session processing functional requirements

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

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

Synchronization and audit: The Rw 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.

9.2.2 Information exchange requirements

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

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

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

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

Capabilities: The PD-FE is required to be able to determine capabilities when requesting resources and other transport plane functions from the PE-FE.

Security: The Rw is recommended to support the authentication between the PD-FE and PE-FE such that requests to the PE-FE from unauthenticated sources will not be performed and such that the PD-FE can verify the source of notifications sent from the PE-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 PD-FE is required to be able to communicate with multiple PE-FEs; 2) Many-to-one mode, multiple PD-FEs are required to be able to make requests to a given PE-FE.

For either mode, only a single PD-FE is required to make a request to a given PE-FE for a particular session.

Granularity of resource control: The Rw reference point is required to support resource control requests at different levels of granularity.

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

9.2.3 Information components

The majority of the information components at the Rw reference point are similar to those at Rs. However, the value and meaning may be changed in the PD-FE due to the operator's policy decision and QoS mapping. In addition, some components are not applicable and some new parameters are needed at Rw.

9.2.3.1 Resource control processing information components

The resource control processing information components at Rw are described in Table 9.

Table 9 – Resource control processing information components (Rw)

Information component	Description
PD-FE identifier	A unique identifier for different instances of PD-FE within the same administrative domain of a single network operator.
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 PE-FE. The identifier has to be unique within the same PD-FE instance.
Resource requester identifier (Optional, Note 2)	An identifier for the requester (i.e., the owner of the SCF (e.g., a service provider)) of a 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 PE-FE based on the priority level.
Reservation holding time (Optional, Note 3)	The value of the time interval for which the resource is reserved, which can be initiated by the SCF based on the service requirement and/or granted by the PD-FE based on the network policy decision. The PD-FE is required to release the session when the holding time has expired.
Resource control session information (Optional, Note 4)	The record of the resource control session information. This is used for deriving the session state and other information (e.g., association of the PD-FE and the PE-FE) and only has a local significance between the PD-FE and pertinent parties. This component is only applicable when a stateless PD-FE is deployed.
NOTE 1 – 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 9.2.4. NOTE 2 – The resource requester identifier may be used to assist the PD-FE in identifying the unique relationship between the resource control session and the requester of the SCF. NOTE 3 – Reservation holding time may be used by the PE-FE to assist the PD-FE in monitoring the resource control session timeout and/or state. NOTE 4 – When a stateless PD-FE is in use, the PD-FE identifier is required to be inserted in the resource control session information component and sent to pertinent entities (e.g., PE-FE or TRC-FE).	

9.2.3.2 QoS resource information components

The QoS resource information sub-components for media sessions and media flows are described in Table 10.

Table 10 – QoS resource information sub-components (Rw)

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).
– Media number	An identifier for a media session (e.g., ordinal number of the position of the "m=" line in the SDP).
– Network class of service (Optional)	Represents the network service class subscribed by a CPE (e.g., Premium, Gold, Silver, and Regular). It may include the QoS performance class (e.g., ITU-T Y.1541 class). This parameter is only of local significance for a single operator owning the transport resource, which can be mapped from an application CoS issued by the SCF based on network policy rules and the SLA and can be used for the transport resource control and authorization of transport subscription.
– Media priority (Optional)	Information for priority handling (e.g., TDR/ETS).
– Path selection information (Optional)	The technology independent core network ingress/egress path information at the PE-FE for a media flow (e.g., VPN ID).
– Media flow description	A set of sub-components of individual or a group of media flows within a media session.
Physical connection identifier (Optional)	A local identifier for physical connection of the access transport network that the CPE is attached to (e.g., IP address of the PE-FE device, and media access control (MAC) address or Link ID and physical port ID). It is the same as defined at the Ru reference point.
Logical connection identifier (Optional)	A local identifier for logical connection of the access transport network to which the CPE is connected (e.g., ATM VPI/VCI, PPP, MPLS label, GTP tunnel or logical port). It can be used by the PE-FE to identify the layer 2 connection in pertinent network devices for a particular CPE requesting the access transport resource. It is the same as defined at the Ru reference point.
NOTE – The application class of service and the type of service are mapped into the network class of service and relevant media flow description sub-components (e.g., IP QoS handling class and traffic descriptor).	

The information describing sub-components of the media flow are in Table 11.

Table 11 – Media flow description sub-components (Rw)

Information component	Description
Media flow description	A set of parameters for the individual media flow within a media session.
– 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.

Table 11 – Media flow description sub-components (Rw)

Information component	Description
– Flow number	An identifier for the individual media flow within a media session.
– Gate status	Instruction and indication of open or closed status of the gate for a media flow or a group of media flows. The PD-FE is required to perform the gate control based on the flow status received from the SCF.
– Protocol version	The version of the source and destination unicast network address protocol (e.g., IPv4 or IPv6).
– 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.
– IP QoS handling class (Optional)	A QoS parameter for IP packet marking and handling in the PE-FE (e.g., IPv4 differentiated services code point (DSCP) and IPv6 traffic class). It can be derived from the service information, network CoS and network policy rules.
– Traffic descriptor (Optional)	The description of the flow characteristics (e.g., peak data rate, sustainable data rate, and maximum burst size as specified in [b-ITU-T Y.1221]).

9.2.3.3 Authorization token information component

Table 12 – Authorization token information component (Rw)

Information component	Description
Authorization token (Optional)	A unique identifier used in policy pull mode. The token is produced by the PD-FE and may be sent back by the PE-FE to the PD-FE for the re-authorization of the resource request in the pull mode.
NOTE – Only applicable to policy pull mode as an optional binding method.	

9.2.3.4 Charging correlation information component

Table 13 – Charging correlation information component (Rw)

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

9.2.3.5 Resource control action information components

Table 14 – Resource control action information components (Rw)

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.
Reason	Information describing the cause for an event (e.g., Abort event).
Event notification indication (Optional)	A set of information sub-components indicating the query and notification of a transport event. Note that listed sub-components may not include all event notifications. Extra events can be added.
– Resource information indicator	Indication of a request for resource information. It is used by the PD-FE to ask the PE-FE to include the modified resource information (such as available bandwidth) in the response message, or is used by the PE-FE to retrieve the policy decision information when an event occurs (e.g., node failure).
– Transport loss indicator	The PD-FE's subscription for the notification of the transport loss events, or notification of a transport loss event to the PD-FE.
– Transport recovery indicator	The PD-FE's subscription for the transport recovery events, or notification of a transport recovery event to the PD-FE.
– Transport release indicator	The PD-FE's subscription for the transport release events, or notification of a transport release event to the PD-FE.
NAPT control and NAT traversal indication (Conditional)	A set of information sub-components indicating the existence of near-end and/or far-end NAPTs. The events of NAPT control and NAT traversal are not mutually exclusive. They can be used in the same information flow.
– Address translation command	Indication to the PD-FE for signalling message modification for near-end NAPT. The PE-FE may perform the NAPT enforcement, and ask the PD-FE to request the SCF to modify signalling messages accordingly based on network address hiding policy decision.
– Address binding information request	Indication of the presence of far-end NAT traversal issued by the PD-FE. The PD-FE may ask the PE-FE for the network address and port translation information (e.g., address latching) in support of far-end NAT traversal.

Table 14 – Resource control action information components (Rw)

Information component	Description
– Address binding information response	Indication to the PD-FE for the response of address latching for far-end NAT traversal. The PE-FE is required to obtain the NAPT information, generate the address binding information and send it to relevant PD-FE instance. The PD-FE is required to ask the relevant SCF instance to modify the message body of application signalling accordingly.

9.2.4 Information flows exchanged over Rw

This clause describes the information flows (namely requests and responses) exchanged over Rw.

9.2.4.1 Resource initiation request

The resource initiation request information flow is sent by the PD-FE to the PE-FE to initiate a resource control session. Depending on the resource reservation mode desired, a single resource initiation request may be used for reservation only or reservation and commitment. The session state can be derived through resource control session information provided by the PD-FE if a stateless PE-FE is used. It contains the following information components:

- PD-FE identifier
- Resource control session identifier
- Resource requester identifier (Optional)
- Resource request priority (Optional)
- Reservation holding time (Optional)
- Resource control session information (Optional)
- Dynamic firewall working mode (Optional)
- Charging correlation information (Optional)
- Media profile
  - Media number
  - Network class of service (Optional)
  - Media priority (Optional)
  - Path selection information (Optional)
  - Media flow description
    - Flow direction
    - Flow number
    - Gate status
    - Protocol version
    - IP addresses
    - Ports
    - Protocol number
    - Bandwidth
    - IP QoS handling class (Optional)
    - Traffic descriptor (Optional)

- Physical connection identifier (Optional)
- Logical connection identifier (Optional)
- Resource reservation mode (Optional)
- Event notification indication (Optional)
  - Resource information indicator
  - Transport loss indicator
  - Transport recovery indicator
  - Transport release indicator
- NAPT control and NAT traversal (Conditional)
  - Address binding information request

9.2.4.2 Resource initiation response

The resource initiation response information flow is sent by the PE-FE to the PD-FE to confirm the resource initiation request. It contains the following information components:

- PD-FE identifier
- Resource control session identifier
- Resource requester identifier (Optional)
- Reservation holding time (Optional)
- Resource control session information (Optional)
- Resource request result
- Media profile (Optional)
  - Media number
  - Network class of service (Optional)
  - Media priority (Optional)
  - Media flow description
    - Flow direction
    - Flow number
    - Gate status
    - Protocol version
    - IP addresses
    - Ports
    - Protocol number
    - Bandwidth
    - IP QoS handling class (Optional)
    - Traffic descriptor (Optional)
- NAPT control and NAT traversal (Conditional)
  - Address translation command
  - Address binding information response

9.2.4.3 Resource modification request

The resource modification request information flow is sent by the PD-FE to the PE-FE to request the resource modification of an established session. It contains the following information components:

- PD-FE identifier
- Resource control session identifier
- Resource requester identifier (Optional)
- Resource request priority (Optional)
- Reservation holding time (Optional)
- Dynamic firewall working mode (Optional)
- Charging correlation information (Optional)
- Media profile
  - Media number
  - Network class of service (Optional)
  - Media priority (Optional)
  - Path selection information (Optional)
  - Media flow description
    - Flow direction
    - Flow number
    - Gate status
    - Protocol version
    - IP addresses
    - Ports
    - Protocol number
    - Bandwidth
    - IP QoS handling class (Optional)
    - Traffic descriptor (Optional)
- Physical connection identifier (Optional)
- Logical connection identifier (Optional)
- Resource reservation mode
- Event notification indication (Optional)
  - Resource information indicator
  - Transport loss indicator
  - Transport recovery indicator
  - Transport release indicator
- NAPT control and NAT traversal (Optional)
  - Address binding information request

9.2.4.4 Resource modification response

The resource modification response information flow is sent by the PE-FE to the PD-FE to confirm the resource modification request. The information components are the same as those in the resource initiation response.

9.2.4.5 Resource action request

The resource action request information flow is sent by the PE-FE to the PD-FE to request a specific resource control action (e.g., retrieving the resource information). It contains the following information components:

- PD-FE identifier
- Resource control session identifier
- Resource requester identifier (Optional)
- Resource control session information (Optional)
- Authorization token (Optional)
- Dynamic firewall working mode (Optional)
- Media profile (Optional)
  - Media number
  - Network class of service (Optional)
  - Media priority (Optional)
  - Path selection information (Optional)
  - Media flow description
    - Flow direction
    - Flow number
    - Gate status
    - Protocol version
    - IP addresses
    - Ports
    - Protocol number
    - Bandwidth
    - IP QoS handling class (Optional)
    - Traffic descriptor (Optional)
- Physical connection identifier (Optional)
- Logical connection identifier (Optional)
- Resource reservation mode
- Event notification indication (Optional)
  - Resource information indicator
  - Transport loss indicator
  - Transport recovery indicator
  - Transport release indicator
- NAPT control and NAT traversal (Conditional)
  - Address translation command
  - Address binding information response

9.2.4.6 Resource action response

The resource action response information flow is sent by the PD-FE to the PE-FE as needed to confirm the request of the specific action and provide the service information. It contains the following information components:

- PD-FE identifier
- Resource control session identifier
- Resource requester identifier (Optional)
- Resource request priority (Optional)
- Resource control session information (Optional)
- Authorization token (Optional)
- Dynamic firewall working mode (Optional)
- Charging correlation information (Optional)
- Media profile (Optional)
  - Media number
  - Network class of service (Optional)
  - Media priority (Optional)
  - Path selection information (Optional)
  - Media flow description
    - Flow direction
    - Flow number
    - Gate status
    - Protocol version
    - IP addresses
    - Ports
    - Protocol number
    - Bandwidth
    - IP QoS handling class (Optional)
    - Traffic descriptor (Optional)
- Physical connection identifier (Optional)
- Logical connection identifier (Optional)
- Resource reservation mode
- Event notification indication (Optional)
  - Resource information indicator
  - Transport loss indicator
  - Transport recovery indicator
  - Transport release indicator
- NAPT control and NAT traversal (Conditional)
  - Address binding information request

9.2.4.7 Resource notification

The resource notification information flow is sent by the PE-FE to notify the PD-FE of the transport resource events. It contains the following information components:

- PD-FE identifier
- Resource control session identifier
- Resource requester identifier (Optional)
- Resource control session information (Optional)
- Dynamic firewall working mode (Optional)
- Charging correlation information (Optional)
- Media profile
  - Media number
  - Network class of service (Optional)
  - Media priority (Optional)
  - Media flow description
    - Flow direction
    - Flow number
    - Gate status
    - Protocol version
    - IP addresses
    - Ports
    - Protocol number
    - Bandwidth
    - IP QoS handling class (Optional)
    - Traffic descriptor (Optional)
- Event notification indication
  - Resource information indicator
  - Transport loss indicator
  - Transport recovery indicator
  - Transport release indicator

9.2.4.8 Resource decision request

The resource decision request information flow is sent by the PE-FE to the PD-FE to request the authorization and relevant policy decision information in the policy pull mode in the initial and modification phases. It contains the following information components:

- PD-FE identifier
- Resource control session identifier
- Resource requester identifier (Optional)
- Resource request priority (Optional)
- Authorization token (Optional)
- Dynamic firewall working mode (Optional)
- Media profile
  - Media number

  - Network class of service (Optional)
  - Media priority (Optional)
  - Path selection information (Optional)
  - Media flow description
    - Flow direction
    - Flow number
    - Gate status
    - Protocol version
    - IP addresses
    - Ports
    - Protocol number
    - Bandwidth
    - IP QoS handling class (Optional)
    - Traffic descriptor (Optional)
- Physical connection identifier (Optional)
- Logical connection identifier (Optional)
- Resource reservation mode
- NAPT control and NAT traversal (Conditional)
  - Address translation command
  - Address binding information response

9.2.4.9 Resource decision response

The resource decision response information flow is sent by the PD-FE to authorize the request and provide the information to the PE-FE in the policy pull mode in the initial and modification phases. It contains the following information components:

- PD-FE identifier
- Resource control session identifier
- Resource requester identifier (Optional)
- Resource request priority (Optional)
- Resource control session information (Optional)
- Authorization token (Optional)
- Dynamic firewall working mode (Optional)
- Charging correlation information (Optional)
- Media profile
  - Media number
  - Network class of service (Optional)
  - Media priority (Optional)
  - Path selection information (Optional)
  - Media flow description
    - Flow direction
    - Flow number
    - Gate status

        - Protocol version
        - IP addresses
        - Ports
        - Protocol number
        - Bandwidth
        - IP QoS handling class (Optional)
        - Traffic descriptor (Optional)
- Physical connection identifier (Optional)
- Logical connection identifier (Optional)
- Resource reservation mode
- Event notification indication (Optional)
  - Resource information indicator
  - Transport loss indicator
  - Transport recovery indicator
  - Transport release indicator
- NAPT control and NAT traversal (Conditional)
  - Address binding information request

9.2.4.10 Resource release request

The resource release request information flow is sent by the PD-FE to the PE-FE to request the resource release for an established session or individual media flow. It contains the following information components:

- PD-FE identifier
- Resource control session identifier
- Resource requester identifier (Optional)
- Resource control session information (Optional)
- Media profile (Optional)
  - Media number
  - Network class of service (Optional)
  - Media priority (Optional)
  - Dynamic firewall working mode (Optional)
  - Media flow description
    - Flow direction
    - Flow number
    - Gate status
    - Protocol version
    - IP addresses
    - Ports
    - Protocol number
    - Bandwidth
    - IP QoS handling class (Optional)
    - Traffic descriptor (Optional)

- Physical connection identifier (Optional)
- Logical connection identifier (Optional)
- Event notification indication (Optional)
  - Resource information indicator
  - Transport loss indicator
  - Transport recovery indicator
  - Transport release indicator
- NAPT control and NAT traversal (Conditional)
  - Address binding information request

9.2.4.11 Resource release response

The resource release response information flow is sent by the PE-FE to the PD-FE to confirm the resource release request. It contains the following information components:

- PD-FE identifier
- Resource control session identifier
- Resource requester identifier (Optional)
- Resource control session information (Optional)
- Resource request result

9.2.4.12 Abort resource request

The abort resource request information flow is sent by the PE-FE to the PD-FE to indicate the loss of all resources for the established session. It contains the following information components:

- PD-FE identifier
- Resource control session identifier
- Resource requester identifier (Optional)
- Resource control session information (Optional)
- Authorization token (Optional)
- Timestamp
- Reason

9.2.4.13 Abort resource response

The abort resource response information flow is sent by the PD-FE to confirm the resource abort request. It contains the following information components:

- PD-FE identifier
- Resource control session identifier
- Resource requester identifier (Optional)
- Resource control session information (Optional)

9.3 Reference point Rc

NOTE – The details of Rc reference point are for further study.

The Rc reference point allows the TRC-FE to collect the network topology and resource status information of an access or a core network. It is relevant to a transport functional entity at the network boundary or inside the network. Note that the Rc reference point may be connected to any instances of transport functions as needed, including the PE-FE, TRE-FE and other functional entities in the transport stratum defined in [ITU-T Y.2012], to obtain the relevant information.

The Rc reference point is an intra-domain reference point.

9.3.1 Functional requirements

The Rc reference point provides the ability for the TRC-FE to request all transport elements within its purview to:

- Collect the network topology information.
- Collect the resource status information.

In addition, the TRC-FE can request notification of events (e.g., link or port failure) from a transport element to update the resource status information.

9.3.2 Information exchange requirements

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

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

Notifications: The reference point is required to allow the notification of asynchronous events (from a transport element to the TRC-FE).

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

Capabilities: The TRC-FE is required to be able to determine capabilities when requesting resources and other transport plane functions from a transport element.

Security: All messages between the TRC-FE and transport elements are recommended to be authenticated so that requests to the transport elements from unauthenticated sources will not be performed and thus notifications sent from the transport elements to the TRC-FE can be ensured to come from an authenticated source.

9.3.3 Information exchanged

The resource status information is recommended to include pre-provisioned resources for applications and amount of actual traffic using the resources.

The resource status information is specific to the L2/L3 transport technologies of a network.

This information may be specific to each traffic class in the transport functions if different traffic classes are supported.

The resource status information may be specific to the resource-related admission control scheme being used by the TRC-FE, i.e., whether it is accounting, out-of-band measurements, in-band measurements, or reservation-based. Note that the TRC-FE can employ more than one resource-related admission control method simultaneously and use the relevant information based on the applicable method.

9.3.4 Information components

This clause describes the information components exchanged across the Rc reference point.

Note that some requirements for Rc are specific to transport technologies. These requirements are specified in other related Recommendations (e.g., [b-ITU-T Y.2174]).

9.3.4.1 Resource status information components

The resource status information components at Rc are described in Table 15.

NOTE – Performance attributes other than bandwidth (e.g., one-way delay, delay variation, and packet loss ratio) are for further study. In general, performance information can be provided by the management of performance measurement as defined in [ITU-T Y.2173] to the RACF. The related details are also for further study.

Table 15 – Resource status information components (Rc)

Information component	Description
Transport FE identifier	A unique identifier for different instances of transport functional entities within the same administrative domain of a single network operator.
Transport resource identifier	A local identifier for a transport resource such as a port, link or connection. Examples of a connection include ATM VP/VC, MPLS LSP, and VLAN. The physical connection identifier and logical connection identifier may be used to derive this transport identifier in certain scenarios, e.g., access network.
Transport class of service (Optional)	It represents the transport service class of the connection. Multiple transport service classes may be included in a connection.
Bandwidth	Available bandwidth of a relevant link or connection. The upstream and downstream bandwidth is recommended to be provided separately. It is optional to specify bandwidth for each class of service.

9.4 Reference point Ru

The Ru reference point allows the PD-FE to interact with the NACF for checking on CPE transport subscription information and the binding information of the logical/physical port address to an assigned IP address.

The Ru reference point is an intra-domain reference point.

9.4.1 Functional requirements

9.4.1.1 Resource control functional requirements

The Ru reference point provides the ability for the RACF to access the user profile for:

- Retrieving the configuration information in order to locate the access transport network for a transport subscriber.
- Retrieving access transport network subscription information in order to perform resource based admission control.

9.4.1.2 Resource control session processing functional requirements

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

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

Synchronization and audit: The Ru 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.

9.4.2 Information exchange requirements

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

Request-response transactions: The reference point is required to allow the PD-FE to request a transaction to be performed by the NACF 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 NACF to the PD-FE).

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

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

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

Many-to-one: Many-to-one mode, multiple PD-FE instances is required to be able to make requests to a given NACF. Only a single PD-FE will make a request to a given NACF for a particular session.

9.4.3 Information components

The information components consist of those in Tables 16 to 18.

Table 16 – Access transport resource subscriber information components (Ru)

Information component	Description
Globally unique IP address information	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	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.
Physical connection identifier (Optional)	A local identifier for physical connection of access transport network that the CPE is attached to (e.g., IP address of a PE-FE device, and MAC address or Link ID and physical port).

Table 16 – Access transport resource subscriber information components (Ru)

Information component	Description
Logical connection identifier	A local identifier for logical connection of access transport network to which the CPE is connected (e.g., ATM VPI/VCI, PPP, MPLS Label, GTP Tunnel and logical port). It can be used to locate the layer 2 connection and pertinent network devices for a particular CPE requesting the access transport resource.
Type of access transport network (Optional)	The type of access network to which the CPE is attached.

Table 17 – Default access transport resource configuration information sub-components (Ru)

Information component	Description
Default configuration (Optional)	
– Default access control list	The list of destination IP addresses, ports, prefixes and port ranges allowed to cut through by default.
– Default upstream bandwidth	The maximum bandwidth that can be used for the upstream connections by default.
– Default downstream bandwidth	The maximum bandwidth that can be used for the downstream connections by default.

Table 18 – Access transport resource subscription information sub-components (Ru)

Information component	Description
Transport resource subscription (Optional)	
– Network class of service	Represents the network service class subscribed by a CPE (e.g., Premium, Gold, Silver, Regular). It may include the QoS performance class (e.g., ITU-T Y.1541 class). This parameter is only of local significance for a single operator owning the transport resource, which can be mapped from application CoS issued by the SCF based on network policy rules and SLA and can be used for the transport resource control and authorization of transport subscription.
– Subscribed upstream bandwidth	The maximum bandwidth subscribed by a CPE for the upstream connections.
– Subscribed downstream bandwidth	The maximum amount of bandwidth subscribed by a CPE for the downstream connections.
– Level of priority	The maximum level of priority permitted for any reservation request.
– Time slot (Optional)	Time slot represents the specific time period. User may subscribe different QoS parameters during different Time Slot.

Table 18 – Access transport resource subscription information sub-components (Ru)

Information component	Description
Remaining quota (Optional, Note)	Remaining quota is defined as volume of user plane traffic allowed to be used. It represents an upper limit for the bandwidth quota for per user.
NOTE – The remaining quota is updated after the RACF reports the remaining quota allowance to the NACF. The reporting mechanism for the remaining quota from the RACF to the NACF is for further study.	

9.4.4 Information flows exchanged over Ru

The Ru reference point is recommended to allow information flows (namely requests and responses) to be exchanged as follows:

- The profile information is pushed by the NACF to the PD-FE.
- The profile information is pulled by the PD-FE from the NACF.
- The resource utilization information is pushed by the PD-FE to the NACF.

The PD-FE and the NACF are recommended to use one of two selection mechanisms, either the local static configuration or dynamic discovery, based on a globally unique IP address and/or transport subscriber identifier to locate the respective communicating entities (i.e., PD-FE → NACF, or NACF → PD-FE).

The following information flows are recommended to be exchanged through the Ru reference point:

9.4.4.1 Transport resource information request

The transport resource information request information flow is sent by the PD-FE to the NACF to request the access transport network profile information. A globally unique IP address information and/or transport subscriber identifier is recommended to be used to discover the NACF and identify the user profile using the static configuration or dynamic discovery approaches. It contains the following information components:

- Globally unique IP address information (Optional, see Note)
  - Unique IP address
  - Address realm
- Transport subscriber identifier (Optional, see Note)
- Remaining quota (Optional)

NOTE – One of them is required to be present.

9.4.4.2 Transport resource information response

The transport resource information response information flow is sent by the NACF to the PD-FE to provide the access transport network profile information during either a new resource initiation request from the SCF or the network failure recovery procedure. It contains the following information components:

- Globally unique IP address information (Optional, see Note)
  - Unique IP address
  - Address realm
- Transport subscriber identifier (Optional, see Note)
- Physical connection identifier (Optional)
- Logical connection identifier

- Type of access transport network (Optional)
- Transport resource subscription (Optional)
  - Network class of service
  - Subscribed upstream bandwidth
  - Subscribed downstream bandwidth
  - Level of priority
  - Time slot (Optional)
- Remaining quota (Optional)

NOTE – One of them is required to be present.

9.4.4.3 Transport resource information indication

The transport resource information indication information flow is sent by the NACF to the PD-FE to push the access transport network profile information when an IP address assigned to a subscriber or the relevant profile is changed after the profile information has been sent to the PD-FE. It contains the following information components:

- Globally unique IP address information (Optional, see Note)
  - Unique IP address
  - Address realm
- Transport subscriber identifier (Optional, see Note)
- Physical connection identifier (Optional)
- Logical connection identifier
- Type of access transport network (Optional)
- Transport resource subscription (Optional)
  - Network class of service
  - Subscribed upstream bandwidth
  - Subscribed downstream bandwidth
  - Level of priority
  - Time slot (Optional)
- Remaining quota (Optional)
- Default configuration (Optional)
  - Default access control list
  - Default upstream bandwidth
  - Default downstream bandwidth

NOTE – One of them is required to be present.

9.4.4.4 Transport resource release notification

The transport resource release notification information flow is sent by the NACF to notify the PD-FE to remove the resource profile information from local repository when the assigned IP address is released (e.g., DHCP leased timer expiry or a release of the access transport resources). It contains the following information components:

- Globally unique IP address information (Optional, see Note)
  - Unique IP address
  - Address realm

- Transport subscriber identifier (Optional, see Note)

NOTE – One of them is required to be present.

9.4.4.5 Resource utilization information notification

The resource utilization information notification information flow, is sent by the PD-FE to notify the NACF to report the remaining quota for the subscribers. It contains the following information components:

- Globally unique IP address information (Optional, see Note)
  - Unique IP address
  - Address realm
- Transport subscriber identifier (Optional, see Note)
- Remaining quota (Optional)

NOTE – One of them is required to be present.

9.5 Reference point Rt

The Rt reference point allows the PD-FE to interact with the TRC-FE to detect and determine the requested QoS resource in the involved access network and core network for media flows along the media flow path. In addition, it can relay the access network information from the NACF to the TRC-FE through the PD-FE.

The Rt reference point is an intra-domain reference point.

9.5.1 Functional requirements

9.5.1.1 Resource control functional requirements

The Rt reference point provides the ability for the PD-FE to request the TRC-FE entities in the involved networks to detect and determine the requested QoS resource for a given media flow. The PD-FE may also request that the TRC-FE provides the path selection information for a given flow in the core network.

9.5.1.2 Resource control session processing functional requirements

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

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

Synchronization and audit: The Rt 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.

9.5.2 Information exchange requirements

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

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

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

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

Capabilities: The PD-FE is required to be able to determine capabilities when requesting resources and other transport plane functions from the TRC-FE.

Security: The Rt is recommended to support the authentication between the PD-FE and TRC-FE such that requests to the TRC-FE from unauthenticated sources will not be performed and such that the PD-FE can verify the source of notifications sent from the TRC-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 PD-FE is required to be able to communicate with multiple TRC-FEs; 2) Many-to-one mode, multiple PD-FEs are required to be able to make requests to a given TRC-FE.

Granularity of resource control: The Rt reference point is required to support resource control requests at different levels of granularity.

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

NOTE – Rt resource control at the aggregate level is for further study.

9.5.3 Information components

The majority of the information components at the Rt reference point are similar to those at Rs. However, the value and meaning may be changed in the PD-FE due to the network policy rules and QoS mapping. In addition, some components are not applicable and some new information components are needed at Rt.

9.5.3.1 Resource control processing information components

The resource control processing information components at Rt are as described in Table 19.

Table 19 – Resource control processing information components (Rt)

Information component	Description
PD-FE identifier	A unique identifier for different instances of PD-FE within the same administrative domain of a single network operator.
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 TRC-FE. The identifier has to be unique within the same PD-FE 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)	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.

Table 19 – Resource control processing information components (Rt)

Information component	Description
Resource requester identifier (Optional, Note 2)	An identifier for the requester (i.e., the owner of the SCF (e.g., a service provider)) of a 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 TRC-FE based on the priority level.
Reservation holding time (Optional, Note 3)	The value of time interval for which the resource is reserved, which can be initiated by the SCF based on the service requirement and/or granted by the PD-FE based on the network policy decision. The PD-FE is required to release the session when the holding time has expired.
Resource control session information (Optional, Note 4)	The record of the resource control session information. This is used for deriving the session state and other information (e.g., association of the PD-FE and TRC-FE) and only has a local significance between the PD-FE and pertinent parties. This component is only applicable when a stateless PD-FE is deployed.
NOTE 1 – 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 9.5.4. NOTE 2 – The resource requester identifier may be used to assist PD-FE in identifying the unique relationship between the resource control session and the requester of the SCF. NOTE 3 – Reservation holding time may be used by the PE-FE to assist the PD-FE in monitoring the resource control session timeout and/or state. NOTE 4 – When a stateless PD-FE is in use, the PD-FE identifier is required to be inserted in the resource control session information component and sent to pertinent entities (e.g., PE-FE or TRC-FE).	

9.5.3.2 QoS resource information components

The QoS resource information sub-components for media session and media flows are described in Table 20.

Table 20 – QoS resource information sub-components (Rt)

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).
– 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).

Table 20 – QoS resource information sub-components (Rt)

Information component	Description
– Network class of service (Optional)	Represents the network service class subscribed by a CPE (e.g., Premium, Gold, Silver, and Regular). It may include the QoS performance class (e.g., ITU-T Y.1541 class). This parameter is only of local significance for a single operator owning the transport resource, which can be mapped from application CoS issued by the SCF based on network policy rules and SLA and can be used for the transport resource control and authorization of transport subscription.
– Media priority (Optional)	Information for priority handling (e.g., TDR/ETS).
– Ingress identifier (Optional)	The IP address of the ingress PE-FE where the involved flow enters a sub-domain.
– Egress identifier (Optional)	The IP address of the egress PE-FE where the involved flow leaves a sub-domain.
– Performance state (Optional)	Estimated performance level of the local domain, to be compared with desired network performance requirement (e.g., ITU-T Y.1541 class).
– Path selection information (Optional)	For requests, the technology independent core network ingress/egress path information at the PE-FE for a media flow (e.g., VPN ID). For responses, it may also be the path selection information for the media flow within the core network.
– Media flow description	A set of sub-components of individual or a group of media flows within a media session.
Physical connection identifier (Optional)	A local identifier for physical connection of the access transport network that the CPE is attached to (e.g., IP address of a PE-FE device, and MAC address or Link ID and physical port ID). It is the same as defined at the Ru reference point.
Logical connection identifier (Optional)	A local identifier for logical connection of the access transport network to which the CPE is connected (e.g., ATM VPI/VCI, PPP, MPLS Label, GTP Tunnel or logical port). It can be used by the PE-FE to identify the layer 2 connection in pertinent network devices for a particular CPE requesting the access transport resource. It is the same as defined at the Ru reference point.
Type of access transport network (Optional)	The type of access network to which the CPE is attached.
Transport resource subscription (Optional)	
– Network class of service	Represents the network service class subscribed by a CPE (e.g., Premium, Gold, Silver, Regular). It may include the QoS performance class (e.g., ITU-T Y.1541 class). This parameter is only of local significance for a single operator owning the transport resource, which can be mapped from application CoS issued by the SCF based on network policy rules and SLA and can be used for the transport resource control and authorization of transport subscription.
– Subscribed upstream bandwidth	The maximum bandwidth subscribed by a CPE for the upstream connections.

Table 20 – QoS resource information sub-components (Rt)

Information component	Description
– Subscribed downstream bandwidth	The maximum amount of bandwidth subscribed by a CPE for the downstream connections.
– Level of priority	The maximum level of priority permitted for any reservation request.
NOTE – The application class of service and the type of service are mapped into the network class of service and relevant media flow description sub-components (e.g., IP QoS handling class and traffic descriptor).	

The information sub-components of the media flow description are described in Table 21.

Table 21 – Media flow description sub-components (Rt)

Information component	Description
Media flow description	A set of parameters for the individual media flow within a media session.
– 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).
– 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.
– IP QoS handling class (Optional)	A QoS parameter for IP packet marking and handling in the PE-FE (e.g., IPv4 DSCP and IPv6 traffic class). It can be derived from the service information, network CoS and network policy rules.
– Traffic descriptor (Optional)	The description of the flow characteristics (e.g., peak data rate, sustainable data rate, and maximum burst size as specified in [b-ITU-T Y.1221]).

9.5.3.3 Authorization token information component

This component is not applicable.

9.5.3.4 Charging correlation information component

This component is not applicable.

9.5.3.5 Resource control action information components

Table 22 – Resource control action information components (Rt)

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.
Resource request result	Indication of the result for a resource request (initiation, modification, release).
Timestamp	The time when the resources were lost.
Reason	Information describing the cause for an event (e.g., Abort event).
Event notification indication (Optional)	A set of information sub-components indicating the query and notification of a transport event. Note that the listed sub-components may not include all event notifications. Extra events can be added.
– Resource information indicator	Indication of a request for resource information. It is used by the PD-FE to ask the TRC-FE to include the resource information (such as available bandwidth) in the response message, or is used by TRC-FE to retrieve the processed service information when an event occurs (e.g., node failure).
– Transport loss indicator	The PD-FE's subscription for the notification of the transport loss events, or notification of a transport loss event to the PD-FE.
– Transport recovery indicator	The PD-FE's subscription for the transport recovery events, or notification of a transport recovery event to the PD-FE.
– Transport release indicator	The PD-FE's subscription for the transport release events, or notification of a transport release event to the PD-FE.

9.5.4 Information flows exchanged over Rt

This clause describes the information flows (namely requests and responses) exchanged over Rt.

9.5.4.1 Resource initiation request

The resource initiation request information flow is sent by the PD-FE to the TRC-FE to request the transport resource control (e.g., resource admission and decision). It contains the following information components:

- PD-FE identifier
- Resource control session identifier
- Globally unique IP address information (Optional, see Note)
  - Unique IP address
  - Address realm
- Transport subscriber identifier (Optional, see Note)
- Resource requester identifier (Optional)
- Resource request priority (Optional)
- Reservation holding time (Optional)

- Resource control session information (Optional)
- Media profile
  - Media number
  - Type of service (Optional)
  - Network class of service (Optional)
  - Media priority (Optional)
  - Ingress identifier (Optional)
  - Egress identifier (Optional)
  - Path selection information (Optional)
  - Media flow description
    - Flow direction
    - Flow number
    - Flow status
    - Protocol version
    - IP addresses
    - Ports
    - Protocol number
    - Bandwidth
    - IP QoS handling class (Optional)
    - Traffic descriptor (Optional)
- Physical connection identifier (Optional)
- Logical connection identifier (Optional)
- Type of access transport network (Optional)
- Transport resource subscription (Optional)
  - Network class of service
  - Subscribed upstream bandwidth
  - Subscribed downstream bandwidth
  - Level of priority
- Event notification indication (Optional)
  - Resource information indicator
  - Transport loss indicator
  - Transport recovery indicator
  - Transport release indicator

NOTE – One of them is required to be present.

9.5.4.2 Resource initiation response

The resource initiation response information flow is sent by the TRC-FE to the PD-FE to confirm the resource initiation request. It contains the following information components:

- PD-FE identifier
- Resource control session identifier
- Resource requester identifier (Optional)
- Reservation holding time (Optional)

- Resource control session information (Optional)
- Resource request result
- Media profile (Optional)
  - Media number
  - Type of service (Optional)
  - Network class of service (Optional)
  - Media priority (Optional)
  - Ingress identifier (Optional)
  - Egress identifier (Optional)
  - Path selection information (Optional)
  - Performance state (Optional)
  - Media flow description
    - Flow direction
    - Flow number
    - Flow status
    - Protocol version
    - IP addresses
    - Ports
    - Protocol number
    - Bandwidth
    - IP QoS handling class (Optional)
    - Traffic descriptor (Optional)

9.5.4.3 Resource modification request

The resource modification request information flow is sent by the PD-FE to the TRC-FE to request the resource modification of an established session. The session state can be provided via resource control session information if a stateless TRC-FE is used. It contains the following information components:

- PD-FE identifier
- Resource control session identifier
- Resource requester identifier (Optional)
- Resource request priority (Optional)
- Reservation holding time (Optional)
- Resource control session information (Optional)
- Media profile
  - Media number
  - Type of service (Optional)
  - Network class of service (Optional)
  - Media priority (Optional)
  - Ingress identifier (Optional)
  - Egress identifier (Optional)
  - Path selection information (Optional)

  - Media flow description
    - Flow direction
    - Flow number
    - Flow status
    - Protocol version
    - IP addresses
    - Ports
    - Protocol number
    - Bandwidth
    - IP QoS handling class (Optional)
    - Traffic descriptor (Optional)
- Physical connection identifier (Optional)
- Logical connection identifier (Optional)
- Type of access transport network (Optional)
- Transport resource subscription (Optional)
  - Network class of service
  - Subscribed upstream bandwidth
  - Subscribed downstream bandwidth
  - Level of priority
- Event notification indication (Optional)
  - Resource information indicator
  - Transport loss indicator
  - Transport recovery indicator
  - Transport release indicator

9.5.4.4 Resource modification response

The resource modification response information flow is sent by the TRC-FE to the PD-FE to confirm the resource modification request. The information components are the same as those in the resource initiation response.

9.5.4.5 Resource action request

The resource action request information flow is sent by the TRC-FE to the PD-FE as needed to request a specific resource control action (e.g., retrieving the information). It contains the following information components:

- PD-FE identifier
- Resource control session identifier
- Resource requester identifier (Optional)
- Resource control session information (Optional)
- Media profile
  - Media number
  - Type of service (Optional)
  - Network class of service (Optional)
  - Media priority (Optional)

  - Ingress identifier (Optional)
  - Egress identifier (Optional)
  - Path selection information (Optional)
  - Media flow description
    - Flow direction
    - Flow number
    - Flow status
    - Protocol version
    - IP addresses
    - Ports
    - Protocol number
    - Bandwidth
    - IP QoS handling class (Optional)
    - Traffic descriptor (Optional)
- Physical connection identifier (Optional)
- Logical connection identifier (Optional)
- Type of access transport network (Optional)
- Transport resource subscription (Optional)
  - Network class of service
  - Subscribed upstream bandwidth
  - Subscribed downstream bandwidth
  - Level of priority
- Event notification indication (Optional)
  - Resource information indicator
  - Transport loss indicator
  - Transport recovery indicator
  - Transport release indicator

9.5.4.6 Resource action response

The resource action response information flow is sent by the PD-FE to the TRC-FE as needed to confirm the request of the specific action and provide the service information. It contains the following information components:

- PD-FE identifier
- Resource control session identifier
- Resource requester identifier (Optional)
- Resource control session information (Optional)
- Media profile
  - Media number
  - Type of service (Optional)
  - Network class of service (Optional)
  - Media priority (Optional)
  - Ingress identifier (Optional)

  - Egress identifier (Optional)
  - Path selection information (Optional)
  - Performance state (Optional)
  - Media flow description
    - Flow direction
    - Flow number
    - Flow status
    - Protocol version
    - IP addresses
    - Ports
    - Protocol number
    - Bandwidth
    - IP QoS handling class (Optional)
    - Traffic descriptor (Optional)
- Physical connection identifier (Optional)
- Logical connection identifier (Optional)
- Type of access transport network (Optional)
- Transport resource subscription (Optional)
  - Network class of service
  - Subscribed upstream bandwidth
  - Subscribed downstream bandwidth
  - Level of priority
- Event notification indication (Optional)
  - Resource information indicator
  - Transport loss indicator
  - Transport recovery indicator
  - Transport release indicator

9.5.4.7 Resource notification

The resource notification information flow is sent by the TRC-FE to notify the PD-FE of the transport resource events. It contains the following information components:

- PD-FE identifier
- Resource control session identifier
- Resource requester identifier (Optional)
- Resource control session information (Optional)
- Dynamic firewall working mode (Optional)
- Media profile
  - Media number
  - Type of service (Optional)
  - Network class of service (Optional)
  - Media priority (Optional)
  - Ingress identifier (Optional)

  - Egress identifier (Optional)
  - Path selection information (Optional)
  - Media flow description
    - Flow direction
    - Flow number
    - Flow status
    - Protocol version
    - IP addresses
    - Ports
    - Protocol number
    - Bandwidth
    - IP QoS handling class (Optional)
    - Traffic descriptor (Optional)
- Event notification indication (Optional)
  - Resource information indicator
  - Transport loss indicator
  - Transport recovery indicator
  - Transport release indicator

9.5.4.8 Resource release request

The resource release request information flow is sent by the PD-FE to the TRC-FE to request the resource release for an established session or individual media flow. The session state can be provided via resource control session information if a stateless TRC-FE is used. It contains the following information components:

- PD-FE identifier
- Resource control session identifier
- Resource requester identifier (Optional)
- Resource control session information (Optional)
- Media profile (Optional)
  - Media number
  - Type of service (Optional)
  - Network class of service (Optional)
  - Media priority (Optional)
  - Ingress identifier (Optional)
  - Egress identifier (Optional)
  - Path selection information (Optional)
  - Media flow description
    - Flow direction
    - Flow number
    - Flow status
    - Protocol version
    - IP addresses

    - Ports
    - Protocol number
    - Bandwidth
    - IP QoS handling class (Optional)
    - Traffic descriptor (Optional)
- Physical connection identifier (Optional)
- Logical connection identifier (Optional)
- Type of access transport network (Optional)
- Transport resource subscription (Optional)
  - Network class of service
  - Subscribed upstream bandwidth
  - Subscribed downstream bandwidth
  - Level of priority
- Event notification indication (Optional)
  - Resource information indicator
  - Transport loss indicator
  - Transport recovery indicator
  - Transport release indicator

9.5.4.9 Resource release response

The resource release response information flow is sent by the TRC-FE to the PD-FE to confirm the resource release request. It contains the following information components:

- PD-FE identifier
- Resource control session identifier
- Resource requester identifier (Optional)
- Resource control session information (Optional)
- Resource request result

9.5.4.10 Abort resource request

The abort resource request information flow is sent by the TRC-FE to the PD-FE to indicate the loss of all resources for the established session. It contains the following information components:

- PD-FE identifier
- Resource control session identifier
- Resource requester identifier (Optional)
- Resource control session information (Optional)
- Timestamp
- Reason

9.5.4.11 Abort resource response

The abort resource response message is sent by the PD-FE to the TRC-FE to confirm a resource abort request. It contains the following information components:

- PD-FE identifier
- Resource control session identifier

- Resource requester identifier (Optional)
- Resource control session information (Optional)

9.6 Reference point Rp

The Rp reference point allows the interaction between the TRC-FE instances within the same administrative domain for resource admission control of unicast, multicast or both.

The Rp reference point is an intra-domain reference point.

9.6.1 Functional requirements

9.6.1.1 Resource control functional requirements

When an operator's core network consists of multiple sub-domains, it is an option to deploy multiple TRC-FE instances in each sub-domain. In this case, the TRC-FE instances communicate with each other through Rp.

In addition, the Rp reference point can be used between top-tier TRC-FE instance and co-located TRC-FE instance using one of operation modes defined in clause 8.2.5.3: outsourcing mode and designating mode.

9.6.1.2 Resource control session processing functional requirements

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

Overload control: The Rp reference point is required to provide the capability to support overload control for preventing the overflow of information messages exchanged between TRC-FE instances.

Synchronization and audit: The Rp 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.

9.6.2 Information exchange requirements

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

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

Notifications: The reference point is required to allow the notification of asynchronous events (from a TRC-FE to another TRC-FE).

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

Capabilities: A TRC-FE is required to be able to determine capabilities when requesting resources and other transport plane functions from another TRC-FE.

Security: The Rp is recommended to support the authentication between the instances of TRC-FEs such that requests to the TRC-FE from unauthenticated sources will not be performed and such that the TRC-FE can verify the source of notifications sent from another TRC-FE. Refer to clause 11 for other security requirements.

Granularity of resource control: The Rp reference point is required to support resource control requests at different levels of granularity.

Level of resource control: The Rp reference point is required to support the resources control at media flow level and/or aggregate level according to the deployed resource control mode as described in clause 7.1.1.

9.6.3 Information components

9.6.3.1 Resource control processing information components

The information components for request processing, described in Table 23 below, provide the information used for discovery, binding, flow control (overload control) and state maintenance.

Table 23 – Resource control processing information components (Rp)

Information component	Description
TRC-FE identifier	A unique identifier for different instances of the TRC-FE within the same administrative domain of a single network operator.
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 TRC-FE. The identifier has to be unique within the same PD-FE instance.
Reservation holding time (Optional)	The value of time interval for which the resource is reserved, which can be initiated by the SCF, based on the service requirement and/or granted by the PD-FE, based on the network policy decision. The PD-FE is required to release the session when the holding time has expired.
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 TRC-FE instances) and only has a local significance between the pertinent TRC-FE instances. This component is only applicable when a stateless PD-FE is deployed.

9.6.3.2 QoS resource information components

The QoS resource information sub-components for media session, media flows and aggregate resource are described in Table 24.

Table 24 – QoS resource information sub-components (Rp)

Information component	Description
Media profile (Conditional)	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).
– 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).

Table 24 – QoS resource information sub-components (Rp)

Information component	Description
– Network class of service (Optional)	Represents the network service class subscribed by a CPE (e.g., Premium, Gold, Silver, Regular). It may include the QoS performance class (e.g., ITU-T Y.1541 class). This parameter is only of local significance for a single operator owning the transport resource, which can be mapped from application CoS issued by the SCF based on network policy rules and SLA and can be used for the transport resource control and authorization of transport subscription.
– Media priority (Optional)	Information for priority handling (e.g., TDR/ETS).
– Ingress identifier (Optional)	The IP address of the ingress PE-FE where the involved flow enters a sub-domain.
– Egress identifier (Optional)	The IP address of the egress PE-FE where the involved flow leaves a sub-domain.
– Path selection information (Optional)	For requests, the technology independent core network ingress/egress path information at the PE-FE for a media flow (e.g., VPN ID). For responses, it may also be the path selection information for the media flow within the core network.
– Media flow description	A set of sub-components of individual or a group of media flows within a media session.
Physical access ID (Optional)	The identifier of the physical access to which the user equipment is connected.
Logical access ID (Optional)	The identifier of the logical access used by the attached user equipment. In the xDSL case, the Logical Access ID may explicitly contain the identifier of VP and/or VC carrying the traffic.
Aggregate resource profile (Conditional)	The aggregate resource description.

The information sub-components of the media flow description are described in Table 25.

Table 25 – Media flow description sub-components (Rp)

Information component	Description
Media flow description	A set of parameters for the individual media flow within a media session.
– 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).
– 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).

Table 25 – Media flow description sub-components (Rp)

Information component	Description
– Bandwidth	The requested maximum bandwidth. The upstream and downstream bandwidth is recommended to be provided separately.
– IP QoS handling class (Optional)	A QoS parameter for IP packet marking and handling in the PE-FE (e.g., IPv4 DSCP and IPv6 traffic class). It can be derived from the service information, network CoS and network policy rules.
– Traffic descriptor (Optional)	The description of the flow characteristics (e.g., peak data rate, sustainable data rate, and maximum burst size as specified in [b-ITU-T Y.1221]).

The information sub-components of the aggregate resource profile are described in Table 26.

Table 26 – Aggregate resource profile sub-components (Rp)

Information component	Description
Aggregate resource profile (Conditional)	The description of an aggregate resource.
– Direction (Optional)	Direction of the requested bulk resources.
– Physical access ID (Optional, see Note)	The identifier of the physical access to which the user equipment is connected.
– Logical access ID (Optional, see Note)	The identifier of the logical access used by the attached user equipment. For example, in the xDSL case, the Logical Access ID corresponds to the identifier of VP and/or VC carrying the traffic.
– Physical aggregation ID (Optional, see Note)	The identifier of the physical resource in the aggregation network.
– Logical aggregation ID (Optional, see Note)	The identifier of the logical resource in the aggregation network.
– Bandwidth	The maximum requested data rate.
– QoS class (Optional)	A QoS class parameter for requested resources (e.g., 802.1p).
– Traffic descriptor (Optional)	The description of the resource characteristics (e.g., peak data rate, sustainable data rate, and maximum burst size (e.g., as specified in [b-ITU-T Y.1221])).
NOTE – Either physical/logical access IDs or physical/logical aggregation connection IDs may be present in the Aggregate Resource Profile.	

9.6.3.3 Authorization token information component

This component is not applicable.

9.6.3.4 Charging correlation information component

This component is not applicable.

9.6.3.5 Resource control action information components

Table 27 – Resource control action information components (Rp)

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.
Resource request result	Indication of the result for a resource request (initiation, modification, release).
Timestamp	The time when the resources were lost.
Reason	Information describing the cause for an event (e.g., Abort event).
Event notification indication (Optional)	A set of information sub-components indicating the query and notification of a transport event. Note that listed sub-components may not include all event notifications. Extra events can be added.
– Resource information indicator	Indication of a request for resource information. It is used by the TRC-FE instance to ask the pertinent TRC-FE instances to include the resource information (such as available bandwidth) in the response message, or is used by TRC-FE to retrieve the processed service information when an event occurs (e.g., node failure).
– Transport loss indicator	The TRC-FE's subscription for the notification of the transport loss events, or notification of a transport loss event to TRC-FE.
– Transport recovery indicator	The TRC-FE's subscription for the transport recovery events, or notification of a transport recovery event to TRC-FE.
– Transport release indicator	The TRC-FE's subscription for the transport release events, or notification of a transport release event to TRC-FE.

9.6.4 Information flows exchanged over Rp

This clause describes the information flows (namely requests and responses) exchanged over Rp.

9.6.4.1 Resource initiation request

One TRC-FE instance may request another TRC-FE instance in the downstream sub-network to check the availability of the requested QoS resource and update the resource status information for outsourcing mode. The request, i.e., information flow, communicates the following information:

- TRC-FE identifier
- Resource control session identifier
- Resource requester identifier (Optional)
- Reservation holding time (Optional)
- Resource control session information (Optional)
- Physical access ID (Optional)
- Logical access ID (Optional)
- Media profile (Conditional, see Note 1)
  - Media number

  - Type of service (Optional)
  - Network class of service (Optional)
  - Media priority (Optional)
  - Ingress identifier (Optional)
  - Egress identifier (Optional)
  - Path selection information (Optional)
  - Media flow description
    - Flow direction
    - Flow number
    - Flow status
    - Protocol version
    - IP addresses
    - Ports
    - Protocol number
    - Bandwidth
    - IP QoS handling class (Optional)
    - Traffic descriptor (Optional)
- Aggregate resource profile (Conditional, see Note 1)
  - Direction (Optional)
  - Physical access ID (Optional, see Note 2)
  - Logical access ID (Optional, see Note 2)
  - Physical aggregation ID (Optional, see Note 2)
  - Logical aggregation ID (Optional, see Note 2)
  - Bandwidth
  - QoS class (Optional)
  - Traffic descriptor (Optional)
- Event notification indication (Optional)
  - Resource information indicator
  - Transport loss indicator
  - Transport recovery indicator
  - Transport release indicator

NOTE 1 – Depending on the level of requested resources, either media description or aggregate resource profile may be present.

NOTE 2 – Either physical/logical access IDs or physical/logical aggregation connection IDs may be present in the aggregate resource profile.

9.6.4.2 Resource initiation response

One TRC-FE instance may respond to another TRC-FE instance in the upstream sub-network to confirm the resource initiation request. The response, i.e., information flow, communicates the following information:

- TRC-FE identifier
- Resource control session identifier

- Resource requester identifier (Optional)
- Reservation holding time (Optional)
- Resource control session information (Optional)
- Resource request result
- Physical access ID (Optional)
- Logical access ID (Optional)
- Media profile (Optional)
  - Media number
  - Type of service (Optional)
  - Network class of service (Optional)
  - Media priority (Optional)
  - Ingress identifier (Optional)
  - Egress identifier (Optional)
  - Path selection information (Optional)
  - Media flow description
    - Flow direction
    - Flow number
    - Flow status
    - Protocol version
    - IP addresses
    - Ports
    - Protocol number
    - Bandwidth
    - IP QoS handling class (Optional)
    - Traffic descriptor (Optional)
- Aggregate resource profile (Optional)
  - Direction (Optional)
  - Physical access ID (Optional)
  - Logical access ID (Optional)
  - Physical aggregation ID (Optional)
  - Logical aggregation ID (Optional)
  - Bandwidth
  - QoS class (Optional)
  - Traffic descriptor (Optional)

9.6.4.3 Resource modification request

One TRC-FE may request another TRC-FE in the downstream sub-network to check the availability of the modified requested QoS resource and update the resource status information for outsourcing mode. The request, i.e., information flow, communicates the following information:

- TRC-FE identifier
- Resource control session identifier
- Resource requester identifier (Optional)

- Reservation holding time (Optional)
- Resource control session information (Optional)
- Physical access ID (Optional)
- Logical access ID (Optional)
- Media profile (Conditional, see Note 1)
  - Media number
  - Type of service (Optional)
  - Network class of service (Optional)
  - Media priority (Optional)
  - Ingress identifier (Optional)
  - Egress identifier (Optional)
  - Path selection information (Optional)
  - Media flow description
    - Flow direction
    - Flow number
    - Flow status
    - Protocol version
    - IP addresses
    - Ports
    - Protocol number
    - Bandwidth
    - IP QoS handling class (Optional)
    - Traffic descriptor (Optional)
- Aggregate resource profile (Conditional, see Note 1)
  - Direction (Optional)
  - Physical access ID (Optional, see Note 2)
  - Logical access ID (Optional, see Note 2)
  - Physical aggregation ID (Optional, see Note 2)
  - Logical aggregation ID (Optional, see Note 2)
  - Bandwidth
  - QoS class (Optional)
  - Traffic descriptor (Optional)
- Event notification indication (Optional)
  - Resource information indicator
  - Transport loss indicator
  - Transport recovery indicator
  - Transport release indicator

NOTE 1 – Depending on the level of requested resources, either a media description or an aggregate resource profile may be present.

NOTE 2 – Either physical/logical access IDs or physical/logical aggregation connection IDs may be present in the aggregate resource profile.

9.6.4.4 Resource modification response

One TRC-FE instance may respond to another TRC-FE instance in the upstream sub-network to confirm the resource modification request. The information components in the response, i.e., information flow, are the same as those in the resource initiation response.

9.6.4.5 Resource request rejection

A TRC-FE may respond to another TRC-FE in the upstream sub-network that the requested QoS resource is unavailable. The response, i.e., information flow, communicates the following information:

- TRC-FE identifier
- Resource control session identifier
- Resource requester identifier (Optional)
- Resource control session information (Optional)
- Reason

9.6.4.6 Resource unavailable indication

A TRC-FE may notify another TRC-FE in the upstream sub-network that the requested QoS resource is no longer available. The response, i.e., information flow, communicates the following information:

- TRC-FE identifier
- Resource control session identifier
- Resource requester identifier (Optional)
- Resource control session information (Optional)
- Reason

9.6.4.7 Resource release request

One TRC-FE instance may request another TRC-FE instance in the downstream sub-network to release the requested QoS resource. The request, i.e., information flow, communicates the following information:

- TRC-FE identifier
- Resource control session identifier
- Resource requester identifier (Optional)
- Resource control session information (Optional)
- Reason

9.6.4.8 Resource release response

One TRC-FE instance may respond to another TRC-FE instance in the upstream sub-network to report the action taken in response to a resource release request. The response, i.e., information flow, communicates the following information:

- TRC-FE identifier
- Resource control session identifier
- Resource requester identifier (Optional)
- Resource control session information (Optional)
- Reason

9.6.4.9 Aggregate resource allocation request

The aggregate resource allocation request message is used to increase or decrease current aggregate resource allocation that is sent from one TRC-FE to another TRC-FE for the designating model. The aggregate resource allocation request message contains the following components:

- TRC-FE identifier
- Resource control session identifier
- Resource requester identifier (Optional)
- Reservation holding time (Optional)
- Resource control session information (Optional)
- Aggregate resource profile
  - Direction (Optional)
  - Physical access ID (Optional, see Note)
  - Logical access ID (Optional, see Note)
  - Physical aggregation ID (Optional, see Note)
  - Logical aggregation ID (Optional, see Note)
  - Bandwidth
  - QoS class (Optional)
  - Traffic descriptor (Optional)
- Event notification indication (Optional)
  - Resource information indicator
  - Transport loss indicator
  - Transport recovery indicator
  - Transport release indicator

NOTE – Either physical/logical access IDs or physical/logical aggregation connection IDs may be present in the aggregate resource profile.

9.6.4.10 Aggregate resource allocation response

The aggregate resource allocation response message is used to confirm aggregate resource allocation for designating model. The aggregate resource allocation response message contains the following components:

- TRC-FE identifier
- Resource control session identifier
- Resource requester identifier (Optional)
- Reservation holding time (Optional)
- Resource control session information (Optional)
- Resource request result
- Aggregate resource profile (Optional)
  - Direction (Optional)
  - Physical access ID (Optional, see Note)
  - Logical access ID (Optional, see Note)
  - Physical aggregation ID (Optional, see Note)
  - Logical aggregation ID (Optional, see Note)

- Bandwidth
- QoS class (Optional)
- Traffic descriptor (Optional)

NOTE – Either physical/logical access IDs or physical/logical aggregation connection IDs may be present in the aggregate resource profile.

9.6.4.11 Resource notification

One TRC-FE instance may require another TRC-FE instance to notify the transport resource events. The resource notification information flow is sent by a TRC-FE to notify another TRC-FE of the transport resource events. It contains the following information components:

- TRC-FE identifier
- Resource control session identifier
- Resource control session information (Optional)
- Physical access ID (Optional)
- Logical access ID (Optional)
- Media profile (Conditional)
  - Media number
  - Type of service (Optional)
  - Network class of service (Optional)
  - Media priority (Optional)
  - Ingress identifier (Optional)
  - Egress identifier (Optional)
  - Path selection information (Optional)
  - Media flow description
    - Flow direction
    - Flow number
    - Flow status
    - Protocol version
    - IP addresses
    - Ports
    - Protocol number
    - Bandwidth
    - IP QoS handling class (Optional)
    - Traffic descriptor (Optional)
- Aggregate resource profile (Conditional)
  - Direction (Optional)
  - Physical access ID (Optional)
  - Logical access ID (Optional)
  - Physical aggregation ID (Optional)
  - Logical aggregation ID (Optional)
  - Bandwidth
  - QoS class (Optional)

  - Traffic descriptor (Optional)
- Event notification indication (Optional)
  - Resource information indicator
  - Transport loss indicator
  - Transport recovery indicator
  - Transport release indicator

9.7 Reference point Ri

The Ri reference point is an inter-domain reference point. The Ri reference point conveys the information on QoS handling, priority handling and resource usage between domains.

The Ri reference point is used to support inter-operator domain PD-FE communication when the SCF is not capable of interacting with the PD-FE in each domain crossed by the media flow or when no SCF is available. For example, when there are separate access network and core network operators and the SCF only interacts with the core network PD-FE, Ri can be used to request resource and admission control over the access domain.

NOTE – In previous editions, the Ri reference point was applicable only to the nomadicity scenario.

9.7.1 Functional requirements

The functional requirements on Ri are similar to the requirements on Rs, except for the gate control, NAPT and firewall aspects which are not part of the inter-domain exchanges.

In peering relations between operators, the PD-FE instance of each operator may interact with PD-FE instances of other operators.

9.7.1.1 Resource control functional requirements

The Ri reference point provides the ability for the PD-FE to make requests:

- for resource authorization and reservation for a media flow;
- for QoS handling;
- for priority handling;
- for resource usage information.
- In addition, the PD-FE can request notification of events.

9.7.1.2 Resource control session processing functional requirements

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

Overload control: The Ri reference point is required to provide the capability to support overload control for preventing the overflow of information messages exchanged between PD-FEs coming from a different domain.

Synchronization and audit: The Ri 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 other PD-FE or PE-FE can be used to derive the session state and relevant information.

9.7.2 Information exchange requirements

This clause provides the description of the information exchange requirements for the Ri reference point.

Request-response transactions: The reference point is required to allow the PD-FE in one administrative domain to request a transaction to be performed by the peer PD-FE in another administrative domain 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 in the peer administrative domain to the PD-FE in the originating domain).

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

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

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

One-to–many/many-to-one communications: Two modes are required to be supported: 1) One-to-many mode: one PD-FE in a given domain is required to be able to send requests to PD-FEs in multiple peer domains; 2) Many-to-one mode, one PD-FE in a given domain is required to be able to accept requests from a PD-FE in multiple peer domains. Only one PD-FE instance in a single domain will make a request to another PD-FE in the peer domain on behalf of a particular session.

Granularity of resource control: The Ri reference point is required to support resource control requests from one administrative domain to another domain at different levels of granularity, e.g., at the media flow level, application session level, service control function level and the operator level between administrative domains.

Level of resource control: The Ri reference point is required to support resource control from one administrative domain to another domain for the media flow level.

NOTE – Ri resource control at the aggregate level is for further study.

9.7.3 Information components

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

9.7.3.1 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 28.

Table 28 – Resource control processing information components (Ri)

Information component	Description
PD-FE identifier	A unique identifier for different instances of the originating PD-FE in the other 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 peer PD-FE. The identifier has to be unique within the peer RACF instance.
Globally unique IP address information (Optional, Note 1)	A set of IP address information used for locating the network in which the CPE is requesting the transport resource.

Table 28 – Resource control processing information components (Ri)

Information component	Description
– 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 peer PD-FE (e.g., a service network provider)) of a resource control service. It is unique over the requesters sending requests for the resource control to the same original 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 a 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 the peer PD-FE based on the service requirement; and/or granted by the original PD-FE based on the network policy decision. The original PD-FE is required to release the session when the holding time has expired.
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 peer PD-FE and the original PD-FE) and only has a local significance between the original PD-FE and the peer PD-FE. This component is only applicable when a stateless PD-FE is deployed.
NOTE 1 – Either a globally unique IP address or a transport subscriber identifier is required 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 9.7.4. NOTE 3 – How the peer PD-FE obtains the information of transport subscriber ID is an issue for the service stratum functionality.	

9.7.3.2 QoS resource information components

The QoS resource information sub-components for media session and media flows are described in Table 29.

Table 29 – QoS resource information sub-components (Ri)

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).

Table 29 – QoS resource information sub-components (Ri)

Information component	Description
– 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 the SCF peer PD-FE) and the owner of the original PD-FE, and is to be converted by the original PD-FE to the network class of service (e.g., ITU-T Y.1541 class for performance requirement) based on the SLA and network policy rules.
– Media priority (Optional)	Information for priority handling (e.g., TDR/ETS).
– Restoration indication (Optional)	This parameter 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)	This parameter 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)	Indication that the requester permits the allocation of degraded resources in the case where sufficient resource allocation cannot be provided.
– 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 30.

Table 30 – Media flow description sub-components (Ri)

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 local domain, so that "out→in" refers to the direction towards the local domain. (Refine the description off line).
– 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).
– 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).

Table 30 – Media flow description sub-components (Ri)

Information component	Description
– 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.

9.7.3.3 Authorization token information component

The information component used for binding purpose in the pull mode is described in Table 31.

Table 31 – Authorization token information component (Ri)

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

9.7.3.4 Charging correlation information component

This information component provides the resource usage information, see Table 32.

Table 32 – Charging correlation information component (Ri)

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

9.7.3.5 Resource control action information components

A variety of indicators are used to request a specific resource control action per network event/condition, see Table 33.

Table 33 – Resource control action information components (Ri)

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.
Resource request result	Indication of the result for a resource request (initiation, modification, release).
Timestamp	The time when the resources were lost.
Reason	Information describing the cause for an event (e.g., abort event).
Event notification indication (Optional)	A set of information sub-components indicating the query and notification of a transport event. Note that the listed sub-components may not include all event notifications. Extra events can be added.

Table 33 – Resource control action information components (Ri)

Information Component	Description
– Resource information indicator	Indication of a request for resource information. It is used by the peer PD-FE to ask the original PD-FE to include the modified service information (such as available bandwidth) in the response message, or is used by the PD-FE to retrieve the original service information when an event occurs (e.g., node failure).
– Transport loss indicator	The peer PD-FE's subscription for the notification of the transport loss events, or notification of a transport loss event to the SCF peer PD-FE.
– Transport recovery indicator	The peer PD-FE's subscription for the transport recovery events, or notification of a transport recovery event.
– Transport release indicator	The peer PD-FE's subscription for the transport release events, or notification of a transport release event to the SCF peer PD-FE.
NAPT control and NAT traversal indication (Conditional)	A set of information sub-components indicating the existence of near-end and/or far-end NAPTs. The events of NAPT control and NAT traversal are not mutually exclusive. They can be used in the same information flow.
– Address translation command	Indication to the SCF for a signalling message modification for near-end NAPT. The PD-FE may perform the NAPT control, obtain the address binding information, and request the SCF to modify signalling messages accordingly based on network address hiding policy decision.
– Address binding information request	Indication of the presence of far-end NAT traversal issued by the SCF. The SCF may ask the RACF for the network address and port translation information (e.g., address latching) in support of far-end NAT traversal.

9.7.4 Information flows exchanged over Ri

This clause describes the information flows (namely requests and responses) exchanged over Ri.

9.7.4.1 Resource initiation request

The resource initiation request information flow is sent by the PD-FE to the peer PD-FE to initiate a resource control session. Depending on the resource reservation mode desired, a single resource initiation request may be used for authorization only (including only user subscription profile based authorization) or reservation only or commitment only or some combination of the above. It contains the following information components:

- PD-FE identifier
- Resource control session identifier
- Globally unique IP address information (Optional, see Note)
  - Unique IP address
  - Address realm
- Transport subscriber identifier (Optional, see Note)
- Resource requester identifier

- Resource request priority (Optional)
- Reservation holding time (Optional)
- Resource control session information (Optional)
- Authorization token (Optional)
- Charging correlation information (Optional)
- Media profile
  - Media number
  - Type of service
  - Application class of service (Optional)
  - Media priority (Optional)
  - Restoration indication (Optional)
  - Downgraded indication (Optional)
  - Downgradability indication (Optional)
  - Media flow description
    - Flow direction
    - Flow number
    - Flow status
    - Protocol version
    - IP addresses
    - Ports
    - Protocol number
    - Bandwidth
- Resource reservation mode
- Event notification indication (Optional)
  - Resource information indicator
  - Transport loss indicator
  - Transport recovery indicator
  - Transport release indicator
- NAPT control and NAT traversal (Conditional)
  - Address binding information request

NOTE – One of these is required to be present.

9.7.4.2 Resource initiation response

The request initiation response information flow is sent by the PD-FE to the peer PD-FE to confirm the resource initiation request of the peer PD-FE. The request initiation response may carry the initial policy rule (e.g., network class of service, bandwidth, level of priority and charging correlation information) made by the peer PD-FE. It contains the following information components:

- PD-FE identifier
- Resource control session identifier
- Reservation holding time (Optional)
- Resource control session information (Optional)

- Resource request result
- Authorization token (Optional)
- Charging correlation information (Conditional, see NOTE)
- Media profile (Conditional, see NOTE)
  - Media number
  - Type of service
  - Application class of service (Optional)
  - Media priority (Optional)
  - Restoration indication (Optional)
  - Downgraded indication (Optional)
  - Downgradability indication (Optional)
  - Media flow description
    - Flow direction
    - Flow number
    - Flow status
    - Protocol version
    - IP addresses
    - Ports
    - Protocol number
    - Bandwidth
  - NAPT control and NAT traversal (Conditional)
  - Address translation command
  - Address binding information response

NOTE – The condition is that the resource initiation response supports the nomadicity scenario of the SCF interacting with the NGN visited provider.

9.7.4.3 Resource modification request

The resource modification request information flow is sent by the original PD-FE to the peer PD-FE to request the modification of the resources assigned to an established session. The session state can be retrieved with the resource control session information provided by the SCF peer PD-FE if a stateless PD-FE is used. It contains the following information components:

- PD-FE identifier
- Resource control session identifier
- Resource requester identifier
- Resource request priority (Optional)
- Reservation holding time (Optional)
- Resource control session information (Optional)
- Charging correlation information (Optional)
- Media profile
  - Media number
  - Type of service
  - Application class of service (Optional)

  - Media priority (Optional)
  - Restoration indication (Optional)
  - Downgraded indication (Optional)
  - Downgradability indication (Optional)
  - Media flow description
    - Flow direction
    - Flow number
    - Flow status
    - Protocol version
    - IP addresses
    - Ports
    - Protocol number
    - Bandwidth
- Resource reservation mode
- Event notification indication (Optional)
  - Resource information indicator
  - Transport loss indicator
  - Transport recovery indicator
  - Transport release indicator
- NAPT control and NAT traversal (Conditional)
  - Address binding information request

9.7.4.4 Resource modification response

The resource modification response information flow is sent by the peer PD-FE to the original PD-FE to confirm that the resource modification request made by the original PD-FE has been received and indicate the result. The information within this flow is the same as that in the resource initiation response information flow.

9.7.4.5 Resource action request

The resource action request information flow is sent by the peer PD-FE to the original PD-FE as needed to request a specific resource control action (e.g., retrieving the resource information) for an established session. It contains the following information components:

- PD-FE identifier
- Resource control session identifier
- Resource control session information (Optional)
- Charging correlation information (Optional)
- Media profile
  - Media number
  - Type of service
  - Application class of service (Optional)
  - Media priority (Optional)
  - Restoration indication (Optional)
  - Downgraded indication (Optional)

  - Downgradability indication (Optional)
  - Media flow description
    - Flow direction
    - Flow number
    - Flow status
    - Protocol version
    - IP addresses
    - Ports
    - Protocol number
    - Bandwidth
- Event notification indication (Optional)
  - Resource information indicator
  - Transport loss indicator
  - Transport recovery indicator
  - Transport release indicator
  - Address binding information response
- NAPT control and NAT traversal (Conditional)
  - Address translation command
  - Address binding information response

9.7.4.6 Resource action response

The resource action response information flow is sent by the original PD-FE to the peer PD-FE to confirm that the request for the specific action has been received and to provide the requested service information. It contains the following information components:

- PD-FE identifier
- Resource control session identifier
- Resource requester identifier
- Resource request priority (Optional)
- Resource control session information (Optional)
- Charging correlation information (Optional)
- Media profile (Optional)
  - Media number
  - Type of service
  - Application class of service (Optional)
  - Media priority (Optional)
  - Restoration indication (Optional)
  - Downgraded indication (Optional)
  - Downgradability indication (Optional)
  - Media flow description
    - Flow direction
    - Flow number
    - Flow status

        - Protocol version
        - IP addresses
        - Ports
        - Protocol number
        - Bandwidth
- Event notification indication (Optional)
    - Resource information indicator
    - Transport loss indicator
    - Transport recovery indicator
    - Transport release indicator
- NAPT control and NAT traversal (Conditional)
    - Address binding information request

9.7.4.7 Resource notification

The resource notification information flow is sent by the peer PD-FE to notify the original PD-FE of transport resource events. It contains the following information components:

- PD-FE identifier
- Resource control session identifier
- Resource control session information (Optional)
- Charging correlation information (Optional)
- Media profile
    - Media number
    - Type of service
    - Application class of service (Optional)
    - Media priority (Optional)
    - Restoration indication (Optional)
    - Downgraded indication (Optional)
    - Downgradability indication (Optional)
    - Media flow description
        - Flow direction
        - Flow number
        - Flow status
        - Protocol version
        - IP addresses
        - Ports
        - Protocol number
        - Bandwidth
- Event notification indication
    - Resource information indicator
    - Transport loss indicator
    - Transport recovery indicator
    - Transport release indicator

NOTE – The use of this information flow for the notification of resource usage information is for further study.

9.7.4.8 Resource release request

The resource release request information flow is sent by the original PD-FE to the peer PD-FE to request the release of resources assigned to an established session or individual media flow. The resource release can be resource control session based, flow-based, and a wildcard is used to indicate the release of all of sessions related to this client. When a request is received, all of the relevant resources are released including the transport event notification settings. It contains the following information components:

- PD-FE identifier
- Resource control session identifier
- Resource requester identifier
- Resource request priority (Optional)
- Resource control session information (Optional)
- Charging correlation information (Optional)
- Media profile
  - Media number
  - Type of service
  - Application class of service (Optional)
  - Media priority (Optional)
  - Restoration indication (Optional)
  - Downgraded indication (Optional)
  - Downgradability indication (Optional)
  - Media flow description
    - Flow direction
    - Flow number
    - Flow status
    - Protocol version
    - IP addresses
    - Ports
    - Protocol number
    - Bandwidth

9.7.4.9 Resource release response

The resource release response information flow is sent by the peer PD-FE to the original PD-FE to confirm the resource release request has been received and indicate the results. It contains the following information components:

- PD-FE identifier
- Resource control session identifier
- Resource request priority (Optional)
- Resource control session information (Optional)
- Resource request result

9.7.4.10 Abort resource request

The abort resource request information flow is sent by the peer PD-FE to the original PD-FE to indicate the loss of all resources for the established session. It contains the following information components:

- PD-FE identifier
- Resource control session identifier
- Resource requester identifier
- Resource control session information (Optional)
- Timestamp
- Reason

9.7.4.11 Abort resource response

The abort resource response is sent by the original PD-FE to the peer PD-FE to confirm a resource abort request. It contains the following information components:

- PD-FE identifier
- Resource control session identifier
- Resource control session information (Optional)

9.8 Reference point Rd

The PD-FE is required to provide a single point of contact to the SCF over Rs. For scalability in larger domains, multiple instances of PD-FE may be deployed, each one handling a subset of the PE-FEs. As a result the PD-FE instance that receives a request over the Rs reference point may not be able to directly reach the PE-FE concerned. Hence the instances of PD-FE need to inter-communicate over Rd. Note that multiple instances of PD-FE may be deployed without using the Rd reference point, e.g., where all PE-FE instances are directly reachable from a given PD-FE instance, or where the SCF directly sends the request to the PD-FE instance handling the PE-FE concerned.

The Rd reference point is an intra-domain reference point.

9.8.1 Functional requirements

The functional requirements on Rd are similar to the requirements on Rs except for the security requirements that are not applicable to intra-domain operations. Rd needs to support conveying only partial information related to specific functions of the PD-FE.

The functional requirements on Rd are similar to the requirements on Rs and Ri except for:

- The gate control, NAPT and firewall aspects which are optional.
- The security requirements that are not applicable to intra-domain operation.

Rd needs to support conveying only partial information related to specific functions of the PD-FE.

9.8.1.1 Resource control functional requirements

The Rd reference point provides the ability for the PD-FE to make requests:

- for resource authorization and reservation for a media flow;
- for QoS handling;
- for priority handling;

and optionally:

- for gate control of a media flow;

- to insert NAPT function and request address mapping information;
- for dynamic firewall working mode selection;

for resource usage information.

In addition, the PD-FE can request notification of events.

9.8.1.2 Resource control session processing functional requirements

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

Overload control: The Rd reference point is required to provide the capability to support overload control for preventing the overflow of information messages exchanged between PD-FEs belonging to the same domain.

Synchronization and audit: The Rd 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 other PD-FE or PE-FE can be used to derive the session state and relevant information.

9.8.2 Information exchange requirements

This clause provides the description of the information exchange requirements for the Rd reference point.

Request-response transactions: The reference point is required to allow the PD-FE in one administrative domain to request a transaction to be performed by the peer PD-FE in another administrative domain 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 in the peer administrative domain to the PD-FE in the originating domain).

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

Capabilities: The PD-FE is required to be able to determine capabilities when requesting resources and other transport functions.

One-to–many/many-to-one communications: Two modes are required to be supported: 1) One-to-many mode: one PD-FE in a given domain is required to be able to send requests to the PD-FEs in multiple peer domains; 2) Many-to-one mode, one PD-FE in a given domain is required to be able to accept the requests from the PD-FE in multiple peer domains. Only one PD-FE instance in a single domain will make a request to another PD-FE in the peer domain on behalf of a particular session.

Granularity of resource control: The Rd reference point is required to support resource control requests from one administrative domain to another domain at different levels of granularity, e.g., at the media flow level, application session level, service control function level and the operator level between administrative domains.

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

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

9.8.3 Information components

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

9.8.3.1 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 34.

Table 34 – Resource control processing information components (Rd)

Information component	Description
PD-FE identifier	A unique identifier for different instances of the RACF 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 peer PD-FE. The identifier has to be unique within the same PD-FE instance.
Globally unique IP address information (Optional, Note 1)	A set of IP address information used for locating the 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 peer PD-FE (e.g., a Network Provider)) of a 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 a 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 a peer PD-FE based on the service requirement and/or granted by the original PD-FE based on the network policy decision. The original PD-FE is required to release the session when the holding time has expired.

Table 34 – Resource control processing information components (Rd)

Information component	Description
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 a peer PD-FE and the original PD-FE) and only has a local significance between the original PD-FE and the peer PD-FE. This component is only applicable when a stateless PD-FE is deployed.
NOTE 1 – Either a globally unique IP address or a transport subscriber identifier is required 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 9.8.4. NOTE 3 – How the peer PD-FE obtains the information of transport subscriber ID is an issue for service stratum functionality.	

9.8.3.2 QoS resource information components

The QoS resource information sub-components for media session and media flows are described in Table 35.

Table 35 – QoS resource information sub-components (Rd)

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 peer PD-FE) and the owner of the original PD-FE, and is to be converted by the original PD-FE to a network class of service (e.g., ITU-T Y.1541 class for performance requirement) based on the SLA and network policy rules.
– Media priority (Optional)	Information for priority handling (e.g., TDR/ETS).
– 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 36.

Table 36 – Media flow description sub-components (Rd)

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).
– 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.

9.8.3.3 Authorization token information component

The information component used for binding purpose in the pull mode is described in Table 37.

Table 37 – Authorization token information component (Rd)

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

9.8.3.4 Charging correlation information component

This information component provides the resource usage information, see Table 38.

Table 38 – Charging correlation information component (Rd)

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

9.8.3.5 Resource control action information components

A variety of indicators are used to request a specific resource control action per network event/condition, see Table 39.

Table 39 – Resource control action information components (Rd)

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.
Reason	Information describing the cause for an event (e.g., Abort event).
Event notification indication (Optional)	A set of information sub-components indicating the query and notification of a transport event. Note that the listed sub-components may not include all event notifications. Extra events can be added.
– Resource information indicator	Indication of a request for resource information. It is used by the peer PD-FE to ask the original PD-FE to include the modified service information (such as available bandwidth) in the response message, or is used by the PD-FE to retrieve the original service information when an event occurs (e.g., node failure).
– Transport loss indicator	The peer PD-FE's subscription for the notification of the transport loss events, or notification of a transport loss event to the peer PD-FE.
– Transport recovery indicator	The peer PD-FE's subscription for the transport recovery events, or notification of a transport recovery event.
– Transport release indicator	The peer PD-FE's subscription for the transport release events, or notification of a transport release event to the peer PD-FE.
NAPT control and NAT traversal indication (Optional)	A set of information sub-components indicating the existence of near-end and/or far-end NAPTs. The events of NAPT control and NAT traversal are not mutually exclusive. They can be used in the same information flow.
– Address translation command	Indication to the peer PD-FE for signalling message modification for near-end NAPT. The original PD-FE may perform the NAPT control, obtain the address binding information, and request the peer PD-FE to modify signalling messages accordingly based on network address hiding policy decision.
– Address binding information request	Indication of the presence of far-end NAT traversal issued by the peer PD-FE. The peer PD-FE may ask the original PD-FE for the network address and port translation information (e.g., address latching) in support of far-end NAT traversal.

Table 39 – Resource control action information components (Rd)

Information component	Description
– Address binding information response	Indication to the peer PD-FE for the response of address latching for far-end NAT traversal. The original PD-FE is required to obtain the NAPT information, generate the address binding information and send it to relevant SCF instance. The SCF is required to modify the message body of application signalling accordingly.

9.8.4 Information flows exchanged over Rd

This clause describes the information flows (namely requests and responses) exchanged over Rd.

9.8.4.1 Resource initiation request

The resource initiation request information flow is sent by the PD-FE to the peer PD-FE to initiate a resource control session. Depending on the resource reservation mode desired, a single resource initiation request may be used for authorization only or reservation only or commitment only or some combination of the above. It contains the following information components:

- PD-FE identifier
- Resource control session identifier
- Globally unique IP address information (Optional, see NOTE)
  - Unique IP address
  - Address realm
- Transport subscriber identifier (Optional, see NOTE)
- Resource requester identifier
- Resource request priority (Optional)
- Reservation holding time (Optional)
- Resource control session information (Optional)
- Dynamic firewall working mode (Optional)
- Authorization token (Optional)
- Charging correlation information (Optional)
- Media profile
  - Media number
  - Type of service
  - Application class of service (Optional)
  - Media priority (Optional)
  - Media flow description
    - Flow direction
    - Flow number
    - Flow status
    - Protocol version
    - IP addresses
    - Ports

        - Protocol number
        - Bandwidth
- Resource reservation mode
- Event notification indication (Optional)
- Resource information indicator
- Transport loss indicator
- Transport recovery indicator
- Transport release indicator
- NAPT control and NAT traversal (Optional)
    - Address binding information request

NOTE – One of these is required to be present.

9.8.4.2 Resource initiation response

The request initiation response information flow is sent by the PD-FE to the peer PD-FE to confirm the resource initiation request of the peer PD-FE. It contains the following information components:

- PD-FE identifier
- Resource control session identifier
- Reservation holding time (Optional)
- Resource control session information (Optional)
- Resource request result
- Authorization token (Optional)
- Media profile (Optional)
    - Media number
    - Type of service
    - Application class of service (Optional)
    - Media priority (Optional)
    - Media flow description
        - Flow direction
        - Flow number
        - Flow status
        - Protocol version
        - IP addresses
        - Ports
        - Protocol number
        - Bandwidth
- NAPT control and NAT traversal (Optional)
    - Address translation command
    - Address binding information response

9.8.4.3 Resource modification request

The resource modification request information flow is sent by the PD-FE to the peer PD-FE to request the modification of the resources assigned to an established session. The session state can be retrieved with the resource control session information provided by the peer PD-FE if a stateless PD-FE is used. It contains the following information components:

- PD-FE identifier
- Resource control session identifier
- Resource requester identifier
- Resource request priority (Optional)
- Reservation holding time (Optional)
- Resource control session information (Optional)
- Dynamic firewall working mode (Optional)
- Charging correlation information (Optional)
- Media profile
  - Media number
  - Type of service
  - Application class of service (Optional)
  - Media priority (Optional)
  - Media flow description
    - Flow direction
    - Flow number
    - Flow status
    - Protocol version
    - IP addresses
    - Ports
    - Protocol number
    - Bandwidth
- Resource reservation mode
- Event notification indication (Optional)
  - Resource information indicator
  - Transport loss indicator
  - Transport recovery indicator
  - Transport release indicator
- NAPT control and NAT traversal (Optional)
  - Address binding information request

9.8.4.4 Resource modification response

The resource modification response information flow is sent by the PD-FE to the peer PD-FE to confirm that the resource modification request made by the peer PD-FE has been received and indicate the result. The information within this flow is the same as that in the resource initiation response information flow.

9.8.4.5 Resource action request

The resource action request information flow is sent by the PD-FE to the peer PD-FE as needed to request a specific resource control action (e.g., retrieving the resource information) for an established session. It contains the following information components:

- PD-FE identifier
- Resource control session identifier
- Resource control session information (Optional)
- Dynamic firewall working mode (Optional)
- Charging correlation information (Optional)
- Media profile
  - Media number
  - Type of service
  - Application class of service (Optional)
  - Media priority (Optional)
  - Media flow description
    - Flow direction
    - Flow number
    - Flow status
    - Protocol version
    - IP addresses
    - Ports
    - Protocol number
    - Bandwidth
- Event notification indication (Optional)
  - Resource information indicator
  - Transport loss indicator
  - Transport recovery indicator
  - Transport release indicator
  - Address binding information response
- NAPT control and NAT traversal (Optional)
  - Address translation command
  - Address binding information response

9.8.4.6 Resource action response

The resource action response information flow is sent by the PD-FE to the peer PD-FE to confirm that the request for the specific action has been received and to provide the requested service information. It contains the following information components:

- PD-FE identifier
- Resource control session identifier
- Resource requester identifier
- Resource request priority (Optional)
- Resource control session information (Optional)

- Dynamic firewall working mode (Optional)
- Charging correlation information (Optional)
- Media profile (Optional)
  - Media number
  - Type of service
  - Application class of service (Optional)
  - Media priority (Optional)
  - Media flow description
    - Flow direction
    - Flow number
    - Flow status
    - Protocol version
    - IP addresses
    - Ports
    - Protocol number
    - Bandwidth
- Event notification indication (Optional)
  - Resource information indicator
  - Transport loss indicator
  - Transport recovery indicator
  - Transport release indicator
- NAPT control and NAT traversal (Optional)
  - Address binding information request

9.8.4.7 Resource notification

The resource notification information flow is sent by the PD-FE to notify the peer PD-FE of transport resource events. It contains the following information components:

- PD-FE identifier
- Resource control session identifier
- Resource control session information (Optional)
- Dynamic firewall working mode (Optional)
- Charging correlation information (Optional)
- Media profile
  - Media number
  - Type of service
  - Application class of service (Optional)
  - Media priority (Optional)
  - Media flow description
    - Flow direction
    - Flow number
    - Flow status
    - Protocol version

        - IP addresses
        - Ports
        - Protocol number
        - Bandwidth
- Event notification indication
    - Resource information indicator
    - Transport loss indicator
    - Transport recovery indicator
    - Transport release indicator

NOTE – The use of this information flow for the notification of resource usage information is for further study.

9.8.4.8 Resource release request

The resource release request information flow is sent by the PD-FE to the peer PD-FE to request the release of resources assigned to an established session or individual media flow. The resource release can be resource control session based, flow-based, and a wildcard is used to indicate the release of all of sessions related to this client. When a request is received, all of the relevant resources are released including the transport event notification settings. It contains the following information components:

- PD-FE identifier
- Resource control session identifier
- Resource requester identifier
- Resource request priority (Optional)
- Resource control session information (Optional)
- Dynamic firewall working mode (Optional)
- Charging correlation information (Optional)
- Media profile
    - Media number
    - Type of service
    - Application class of service (Optional)
    - Media priority (Optional)
    - Media flow description
        - Flow direction
        - Flow number
        - Flow status
        - Protocol version
        - IP addresses
        - Ports
        - Protocol number
        - Bandwidth

9.8.4.9 Resource release response

The resource release response information flow is sent by the PD-FE to the peer PD-FE to confirm the resource release request has been received and indicate the results. It contains the following information components:

- PD-FE identifier
- Resource control session identifier
- Resource request priority (Optional)
- Resource control session information (Optional)
- Resource request result

9.8.4.10 Abort resource request

The abort resource request information flow is sent by the PD-FE to the peer PD-FE to indicate the loss of all resources for the established session to the peer PD-FE. It contains the following information components:

- PD-FE identifier
- Resource control session identifier
- Resource requester identifier
- Resource control session information (Optional)
- Timestamp
- Reason

9.8.4.11 Abort resource response

The abort resource response is sent by the PD-FE to the peer PD-FE to confirm a resource abort request. It contains the following information components:

- PD-FE identifier
- Resource control session identifier
- Resource control session information (Optional)

9.9 Reference point Rn

The TRC-FE performs element resource control and applies the resulted decisions to the TRE-FE through the Rn reference point at the aggregate level.

Note that the detailed requirements for Rn 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]).

9.10 Reference point Rh

The Rh reference point allows the final admission decisions to be installed (either pushed or pulled) to the CGPE-FE from the PD-FE. The corresponding procedures are shown in Appendix V.

The Rh reference point is an intra-domain reference point.

9.10.1 Functional requirements

9.10.1.1 Resource control functional requirements

The Rh reference point allows the PD-FE to push the policy decisions to the CGPE-FE, and also allows the CGPE-FE to request the admission decisions. The PD-FE is required to specify:

- Resources to be reserved and/or committed for media flows.

- QoS handling such as packet marking and policing to use.
- Gate control (opening/closing) for a media flow.
- Resource usage information request and report for a subscriber.

9.10.1.2 Resource control session processing functional requirements

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

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

Synchronization and audit: The Rh 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 CGPE-FE can be used to derive the session state and relevant information.

9.10.2 Information exchange requirements

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

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

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

Reliable delivery: The reference point may provide reliable delivery of messages.

Capabilities: The PD-FE is required to be able to determine capabilities when requesting resources and other transport plane functions from the CGPE-FE.

Security: The Rh is recommended to support the authentication between the PD-FE and CGPE-FE such that requests to the CGPE-FE from unauthenticated sources will not be performed and such that the PD-FE can verify the source of notifications sent from the CGPE-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 PD-FE is required to be able to communicate with multiple CGPE-FEs; 2) Many-to-one mode, multiple PD-FEs are required to be able to make requests to a given CGPE-FE.

For either mode, only a single PD-FE is required to make a request to a given CGPE-FE for a particular session.

Granularity of resource control: The Rh reference point is required to support resource control requests at different levels of granularity.

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

9.10.3 Information components

The majority of the information components at the Rh reference point are similar to those at Rw. However, the value and meaning may be changed in the PD-FE due to the operator's policy decision and QoS mapping. In addition, some components are not applicable and some new parameters are needed at Rh. Appendix VIII provides a detailed comparison of the Rw and Rh reference point.

9.10.3.1 Resource control processing information components

The resource control processing information components at Rh are described in Table 40.

Table 40 – Resource control processing information components (Rh)

Information component	Description
PD-FE identifier	A unique identifier for different instances of PD-FE within the same administrative domain of a single network operator.
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 CGPE-FE. The identifier has to be unique within the same PD-FE instance.
Resource requester identifier (Optional, Note 2)	An identifier for the requester (i.e., the owner of 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 CGPE-FE based on the priority level.
Reservation holding time (Optional, Note 3)	The value of time interval for which the resource is reserved, which can be initiated by SCF based on the service requirement and/or granted by PD-FE based on the network policy decision. The PD-FE shall release the session when the holding time has expired.
Resource control session information (Optional, Note 4)	The record of the resource control session information. This is used for deriving the session state and other information (e.g., association of PD-FE and CGPE-FE) and only has a local significance between the PD-FE and pertinent parties. This component is only applicable when a stateless PD-FE is deployed.
NOTE 1 – 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 9.10.4. NOTE 2 – The resource requester identifier may be used to assist the PD-FE in identifying the unique relationship between the resource control session and requester of the SCF. NOTE 3 – Reservation holding time may be used by the CGPE-FE to assist the PD-FE in monitoring the resource control session timeout and/or state. NOTE 4 – When a stateless PD-FE is in use, the PD-FE identifier shall be inserted in the resource control session information component and sent to pertinent entities (e.g., CGPE-FE or TRC-FE).	

9.10.3.2 QoS resource information components

The QoS resource information sub-components for media session and media flows are described in Table 41.

Table 41 – QoS resource information sub-components (Rh)

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).
– Media number	An identifier for a media session (e.g., ordinal number of the position of the "m=" line in the SDP).
– Network class of service (Optional)	Represents the network service class subscribed by a CPE (e.g., Premium, Gold, Silver, and Regular). It may include the QoS performance class (e.g., ITU-T Y.1541 class). This parameter is only of local significance for a single operator owning the transport resource, which can be mapped from application CoS issued by the SCF based on network policy rules and SLA and can be used for the transport resource control and authorization of transport subscription.
– Media priority (Optional)	Information for priority handling (e.g., TDR/ETS).
– Media flow description	A set of sub-components of individual or a group of media flows within a media session.
NOTE – The application class of service and the type of service are mapped into the network class of service and relevant media flow description sub-components (e.g., IP QoS handling class and traffic descriptor).	

The information sub-components of the media flow description are described in Table 42.

Table 42 – Media flow description sub-components (Rh)

Information component	Description
Media flow description	A set of parameters for the individual media flow within a media session.
– 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.
– Gate status	Instruction and indication of open or closed status of the gate for a media flow or a group of media flows. The PD-FE shall perform the gate control based on the flow status received from the SCF.
– Protocol version	The version of source and destination unicast network address protocol (e.g., IPv4 or IPv6).
– IP addresses	The source and destination network addresses.
– Ports	The source and destination port numbers. Port ranges shall 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 should be provided separately.

Table 42 – Media flow description sub-components (Rh)

Information component	Description
– IP QoS handling class (Optional)	A QoS parameter for IP packet marking and handling in CGPE-FE (e.g., IPv4 DSCP and IPv6 traffic class). It can be derived from the service information, network CoS and network policy rules.
– L2 QoS handling class (Optional)	A QoS parameter for L2 packet marking and handling in CGPE-FE (e.g., 802.1p). It can be derived from the network QoS parameters and transport subscription information by PD-FE.
–Traffic descriptor (Optional)	The description of the flow characteristics (e.g., peak data rate, sustainable data rate, and maximum burst size as specified in [b-ITU-T Y.1221]).

9.10.3.3 Resource control action information components

The resource control action information sub-components for media session and media flows are described in Table 43.

Table 43 – Resource control action information components (Rh)

Information component	Description
Resource reservation mode	Indication of resource reservation mode (e.g., non-reservation, reservation only or reservation + commitment). In the push mode, either the "reservation only" or the "reservation + commit" option is used.
Resource request result	Indication of the result for a resource request (initiation, modification, release).
Timestamp	The time when the resources were lost.
Reason	Information describing the cause for an event (e.g., Abort event).
Event notification indication (Optional)	A set of information sub-components indicating the query and notification of a transport event. Note that listed sub-components may not include all event notifications. Extra events can be added.
– Resource information indicator	Indication of a request for resource information. It is used by the PD-FE to ask the CGPE-FE to include the modified resource information (such as available bandwidth) in the response message, or is used by the CGPE-FE to retrieve the policy decision information when an event occurs (e.g., node failure).
– Transport loss indicator	The PD-FE's subscription for the notification of the transport loss events, or notification of a transport loss event to the PD-FE.
– Transport recovery indicator	The PD-FE's subscription for the transport recovery events, or notification of a transport recovery event to the PD-FE.
– Transport release indicator	The PD-FE's subscription for the transport release events, or notification of a transport release event to the PD-FE.

9.10.4 Information flows exchanged over Rh

This clause describes the information flows (namely requests and responses) exchanged over Rh.

9.10.4.1 Resource initiation request

The resource initiation request information flow is sent by the PD-FE to the CGPE-FE to initiate a resource control session. Depending on the resource reservation mode desired. A single resource initiation request may be used for reservation only or reservation and commitment. The session state can be derived through resource control session information provided by the PD-FE if a stateless CGPE-FE is used. It contains the following information components:

- PD-FE identifier
- Resource control session identifier
- Resource requester identifier (Optional)
- Resource request priority (Optional)
- Reservation holding time (Optional)
- Resource control session information (Optional)
- Media profile
  - Media number
  - Network class of service (Optional)
  - Media priority (Optional)
  - Media flow description
    - Flow direction
    - Flow number
    - Gate status
    - Protocol version
    - IP addresses
    - Ports
    - Protocol number
    - Bandwidth
    - IP QoS handling class (Optional)
    - L2 QoS handling class (Optional)
    - Traffic descriptor (Optional)
- Resource reservation mode (Optional)
  - Resource information indicator
  - Transport loss indicator
  - Transport recovery indicator
  - Transport release indicator

9.10.4.2 Resource initiation response

The resource initiation response information flow is sent by the CGPE-FE to the PD-FE to confirm the resource initiation request. It contains the following information components:

- PD-FE identifier
- Resource control session identifier
- Resource requester identifier (Optional)

- Reservation holding time (Optional)
- Resource control session information (Optional)
- Resource request result
- Media profile (Optional)
  - Media number
  - Network class of service (Optional)
  - Media priority (Optional)
  - Media flow description
    - Flow direction
    - Flow number
    - Gate status
    - Protocol version
    - IP addresses
    - Ports
    - Protocol number
    - Bandwidth
    - IP QoS handling class (Optional)
    - Traffic descriptor (Optional)

9.10.4.3 Resource modification request

The resource modification request information flow is sent by the PD-FE to the CGPE-FE to request the resource modification of an established session. It contains the following information components:

- PD-FE identifier
- Resource control session identifier
- Resource requester identifier (Optional)
- Resource request priority (Optional)
- Reservation holding time (Optional)
- Media profile
  - Media number
  - Network class of service (Optional)
  - Media priority (Optional)
  - Media flow description
    - Flow direction
    - Flow number
    - Gate status
    - Protocol version
    - IP addresses
    - Ports
    - Protocol number
    - Bandwidth
    - IP QoS handling class (Optional)

        - Traffic descriptor (Optional)
- Resource reservation mode
- Event notification indication (Optional)
    - Resource information indicator
    - Transport loss indicator
    - Transport recovery indicator
    - Transport release indicator

9.10.4.4 Resource modification response

The resource modification response information flow is sent by CGPE-FE to PD-FE to confirm the resource modification request. The information components are the same as those in the resource initiation response.

9.10.4.5 Resource action request

The resource action request information flow is sent by the CGPE-FE to the PD-FE to request a specific resource control action (e.g., retrieving the resource information). It contains the following information components:

- PD-FE identifier
- Resource control session identifier
- Resource requester identifier (Optional)
- Resource control session information (Optional)
- Media profile (Optional)
    - Media number
    - Network class of service (Optional)
    - Media priority (Optional)
    - Media flow description
        - Flow direction
        - Flow number
        - Gate status
        - Protocol version
        - IP addresses
        - Ports
        - Protocol number
        - Bandwidth
        - IP QoS handling class (Optional)
        - Traffic descriptor (Optional)
- Resource reservation mode
- Event notification indication (Optional)
    - Resource information indicator
    - Transport loss indicator
    - Transport recovery indicator
    - Transport release indicator

9.10.4.6 Resource action response

The resource action response information flow is sent by the PD-FE to the CGPE-FE as needed to confirm the request of the specific action and provide the service information. It contains the following information components:

- PD-FE identifier
- Resource control session identifier
- Resource requester identifier (Optional)
- Resource request priority (Optional)
- Resource control session information (Optional)
- Media profile (Optional)
  - Media number
  - Network class of service (Optional)
  - Media priority (Optional)
  - Media flow description
    - Flow direction
    - Flow number
    - Gate status
    - Protocol version
    - IP addresses
    - Ports
    - Protocol number
    - Bandwidth
    - IP QoS handling class (Optional)
    - Traffic descriptor (Optional)
- Resource reservation mode
- Event notification indication (Optional)
  - Resource information indicator
  - Transport loss indicator
  - Transport recovery indicator
  - Transport release indicator

9.10.4.7 Resource notification

The resource notification information flow is sent by the CGPE-FE to notify the PD-FE of the transport resource events. It contains the following information components:

- PD-FE identifier
- Resource control session identifier
- Resource requester identifier (Optional)
- Resource control session information (Optional)
- Media profile
  - Media number
  - Network class of service (Optional)
  - Media priority (Optional)

  - Media flow description
    - Flow direction
    - Flow number
    - Gate status
    - Protocol version
    - IP addresses
    - Ports
    - Protocol number
    - Bandwidth
    - IP QoS handling class (Optional)
    - Traffic descriptor (Optional)
- Event notification indication
  - Resource information indicator
  - Transport loss indicator
  - Transport recovery indicator
  - Transport release indicator

9.10.4.8 Resource release request

The resource release request information flow is sent by the PD-FE to the CGPE-FE to request the resource release for an established session or individual media flow. It contains the following information components:

- PD-FE identifier
- Resource control session identifier
- Resource requester identifier (Optional)
- Resource control session information (Optional)
- Media profile (Optional)
  - Media number
  - Network class of service (Optional)
  - Media priority (Optional)
  - Media flow description
    - Flow direction
    - Flow number
    - Gate status
    - Protocol version
    - IP addresses
    - Ports
    - Protocol number
    - Bandwidth
    - IP QoS handling class (Optional)
    - Traffic descriptor (Optional)
- Event notification indication (Optional)
  - Resource information indicator

– Transport loss indicator
– Transport recovery indicator
– Transport release indicator

9.10.4.9 Resource release response

The resource release response information flow is sent by CGPE-FE to the PD-FE to confirm the resource release request. It contains the following information components:

- PD-FE identifier
- Resource control session identifier
- Resource requester identifier (Optional)
- Resource control session information (Optional)
- Resource request result

9.10.4.10 Abort resource request

The abort resource request information flow is sent by CGPE-FE to PD-FE to indicate the loss of all resources for the established session. It contains the following information components:

- PD-FE identifier
- Resource control session identifier
- Resource requester identifier (Optional)
- Resource control session information (Optional)
- Timestamp
- Reason

9.10.4.11 Abort resource response

The abort resource response information flow is sent by the PD-FE to confirm the resource abort request. It contains the following information components:

- PD-FE identifier
- Resource control session identifier
- Resource requester identifier (Optional)
- Resource control session information (Optional)

9.11 Reference point Rm

The Rm reference point allows the PD-FE to collect the measured and analysed performance-related information of an access or core network. It also allows the PD-FE to provide specific media-flow information for their resource status information collection. The Rm reference point is an intra-domain reference point.

9.11.1 Functional requirements

The Rm reference point is required to carry the following information:

- Measurement and analysis reports for MPM applications within the same NGN provider domain.
- Acknowledgement for the reports transfer receipt.
- The description of media flows information for the report specified by the MPM applications.

9.11.2 Information exchange requirements

This clause specifies the information exchange requirements for the Rm reference point.

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

Notifications: The reference point must allow the notification of asynchronous events (from an MPM to the PD-FE).

Reliable delivery: The reference point should provide reliable delivery of messages.

One-to-many/many-to-one: Two modes may be supported: 1) One-to-many mode, a PD-FE communicates with multiple MPMs; 2) Many-to-one mode, multiple PD-FEs make requests to a given MPM.

Security: All messages between the PD-FE and the MPM must be authenticated so that requests to the MPM from unauthenticated sources will not be performed and thus notifications sent from the MPM to the PD-FE can be ensured to come from an authenticated source.

9.11.3 Information components

The network performance information components at Rm are described in Table 44.

Table 44 – Resource status information components (Rm)

Information component	Description
PD-FE identifier	A unique identifier for different instances of PD-FE within the same administrative domain of a single network operator.
Report identifier	A unique identifier for a performance report from the MPM. It is used as the pointer to the actual report.
Transport resource identifier	A local identifier for a transport resource such as port, link or connection. Examples of a connection include ATM VP/VC, MPLS LSP, and VLAN. The physical collection identifier and logical collection identifier should be used to derive this transport identifier in certain scenarios, e.g., access network.
Media flow description	A set of parameters for the individual media flow within a media session.
– 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.
– Protocol version	The version of source and destination unicast network address protocol (e.g., IPv4 or IPv6).
– IP addresses	The source and destination network addresses.
– Ports	The source and destination port numbers. Port ranges shall be supported (e.g., two consecutive ports for RTP, RTCP).
– Protocol number	The protocol ID (e.g., UDP, TCP).
– VLAN ID	The VLAN ID.
– MPLS LSP ID	The MPLS LSP ID.

Table 44 – Resource status information components (Rm)

Information component	Description
Report	Performance report content per media flow.
– one-way delay	One-way delay of a media flow.
– one-way delay variation	One-way delay variation of a media flow.
– loss ratio	Loss ratio of a media flow.
– media flow bandwidth	Bandwidth of a media flow.
– link bandwidth	Bandwidth of a link that this media flow belongs.

9.12 Reference point Ro

The Ro reference point allows the MMCF to query the PD-FE to verify whether resources are available to serve the user prior to handover. It also allows the MMCF to provide address binding information to the PD-FE for reserving QoS resources.

The Ro reference point is an intra-domain reference point.

Note that the detailed requirements for Ro are specified in clause 6.5.8 of [ITU-T Y.2018].

9.12.1 Functional requirements

9.12.1.1 Resource control functional requirements

The Ro reference point allows the MMCF to make requests:

- for verification of resource availability;
- for resource re-provisioning.

9.12.1.2 Resource control session processing functional requirements

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

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

Synchronization and audit: The Ro reference point is required to provide the capability to support the 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.

9.12.2 Information exchange requirements

This clause provides the description of the information exchange requirements for the Ro reference point.

Request-response transactions: The reference point is required to allow the MMCF 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 not required to allow the notification of asynchronous events.

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

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

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

One-to-many/many-to-one: One-to-many mode is required to be supported: a PD-FE is required to be able to communicate with multiple MMCFs. Many-to-one mode is not required to be supported since the PD-FE makes no request to the MMCF.

Granularity of resource control: The Ro reference point is required to support resource control requests at different levels of granularity.

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

9.12.3 Information components

The information components exchanged across the Ro reference point are described in Table 45.

Table 45 – Resource control action information components (Ro)

Information component	Description
Transport subscriber identifier	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.
Candidate attachment point list	A list of attachment points, suggesting the new access networks to which handover initiation will be considered. The access networks towards the top of the list are preferred over those towards the bottom of the list.
Status	The status notified to the MMCF. For the verification of resource availability, it specifies whether requested resources are available or not for each candidate link. For the resource re-provisioning, it specifies the status of operation.
Persistent IP address information	A set of IP address information used for locating the mobile UE.
– Unique IP address	The IP address allocated to the attached mobile UE.
– Address realm	The addressing domain in which the IP address is significant.
Temporary IP address information	A set of IP address information used for locating the access network to which the UE is attached.
– Unique IP address	The IP address allocated to the attached mobile UE.
– Address realm	The addressing domain in which the IP address is significant.
Operation type	Indication of the resource reservation operation type: resource reservation or resource release.
Gateway address (optional)	The address of the anchor point.

Table 45 – Resource control action information components (Ro)

Information component	Description
Resource availability time	The value of the time interval for which the resources are available. For each candidate network, the resources can be reserved for particular time intervals in advance, based on the service requirement. The resources are available for time intervals which have not been reserved. 'Resource availability time' contains a starting point and a period.

9.12.4 Information flows exchanged over the Ro

This clause describes the information flows (namely requests and responses) exchanged over the Ro.

9.12.4.1 Available resource query request

The available resource query request information flow is sent by the MMCF to the PD-FE to verify that resources are available to serve the user, prior to handover. It contains the following information components:

- Transport subscriber identifier
- Candidate attachment point list

9.12.4.2 Available resource query response

The available resource query response information flow is sent by the PD-FE to the MMCF to confirm the status of the checked user. It contains the following information components:

- Transport subscriber identifier
- Status
- Resource availability time

9.12.4.3 Resource re-provisioning request

The resource re-provisioning request information flow is sent by the MMCF to the PD-FE to reserve session QoS resources by providing address binding information, and to release QoS resources on the old path once handover is complete. It contains the following information components:

- Persistent IP address information
  - Unique IP address
  - Address realm
- Transport subscriber identifier (mandatory if meets the conditions in the NOTE)
- Temporary IP address information
  - Unique IP address
  - Address realm
- Operation type
- Gateway address (Optional)

NOTE – Transport subscriber identifier is required if either a persistent or temporary address is private.

9.12.4.4 Resource re-provisioning response

The resource re-provisioning response information flow is sent by the PD-FE to the MMCF to confirm the status of the reservation operation. It contains the following information components:

- Transport subscriber identifier
- Persistent IP address information
  - Unique IP address
  - Address realm
- Status

9.13 Reference point Rh'

The Rh' reference point conveys the information on QoS handling, priority handling and resource usage between the PD-FE and the CGPD-FE.

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

Note that the detailed requirement for Rh' is for further study.

9.14 Domain scope of the reference points

The following table describes the domain scope of the reference points.

Table 46 – Reference points and domain scope

Reference point	Inter-domain	Intra-domain
Rs	X	X
Rw		X
Rc		X
Rp		X
Rt		X
Ru		X
Rd		X
Ri	X	
Rh		X
Rn		X
Rm		X
Ro		X
Rh'	X	X
NOTE – In this Recommendation, each reference point may correspond to an interface.		

10 Procedures

This clause defines basic procedures triggered by a single event (e.g., a session initiation request). These basic procedures could be further composed into any possible composite procedures triggered by a series of events.

10.1 Procedures for QoS control

10.1.1 SCF-requested QoS control procedures

Scenario 1, described in clause 7.1 uses the SCF-requested QoS resource reservation mechanism, i.e., the SCF sends RACF a resource initiation request to invoke the QoS resource authorization and reservation. The RACF will push the admission control decisions into the network nodes (e.g., border gateway, edge node or access node) if the resource request is authorized and admitted.

10.1.1.1 Basic procedures

10.1.1.1.1 QoS resource reservation procedure

The SCF-requested QoS resource reservation procedure is illustrated in Figure 10. It is initiated by a resource initiation request from the SCF.

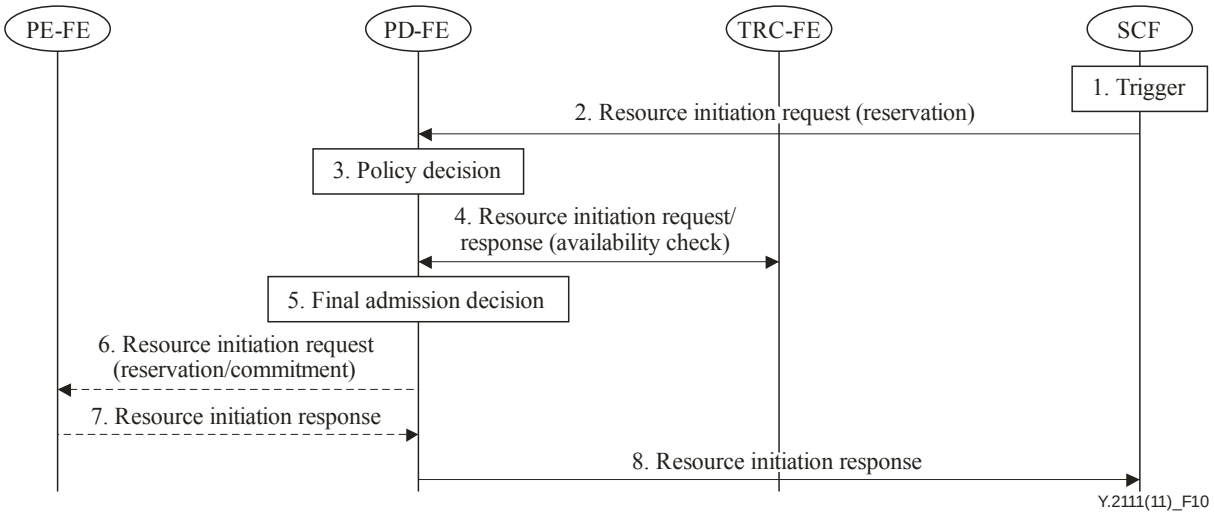


Figure 10 – SCF-requested QoS resource reservation procedure

1) A resource initiation request (reservation) (RIR (reservation)) is usually triggered by a service establishment event or an internal action in the SCF. An example event is that a service signalling message is received at or generated by the SCF.

2) The SCF determines or derives the QoS requirement parameters (such as bandwidth, class of service) for the media flows of a given service. It then sends an RIR (reservation) with the media flow description and its QoS parameters to the PD-FE across the Rs reference point for QoS resource authorization and reservation.

3) On receipt of the RIR (reservation), the PD-FE is required to authorize the required QoS resources for the media flow. The PD-FE checks if the media flow description and the required QoS resources are consistent with network policy rules held in the PD-FE and the transport subscription information held in the NACF.

4) The PD-FE positions and determines which access networks and core networks are involved for the media flow. If there are TRC-FE instances in an involved network, the PD-FE sends an RIR (availability check) to one of the TRC-FE instances registered in the PD-FE to check resource availability in the involved network. If there are multiple TRC-FE instances in the involved network, they communicate with each other to determine if the required QoS resource is available from edge to edge in the involved network. The TRC-FE instance which received the RIR (availability check) is required to send a resource initiation response (RIP) back to the PD-FE. When multiple TRC-FE instances are present in the form of distributed hierarchical structure, the top tier TRC-FE instance forwards the request to other TRC-FE instances in case those instances are in control of resources referenced in the request (i.e., the top tier TRC-FE has delegated resources to other TRC-FE instances).

In this case the top tier TRC-FE makes the final resource admission decision based on the results of resource admission from all other instances.

5) The PD-FE makes the final admission decisions based on the results of steps (3) and (4). If the media flow is not admitted, the PD-FE sends an RIP with the rejection reason back to the SCF.

6) The PD-FE determines whether this service request requires sending a request to the PE-FE. If needed, the PD-FE sends an RIR to install the final admission decisions in the PE-FE.

   The RIR from the PD-FE may request the admission decisions to be enforced immediately (i.e., RIR (reservation + commitment)), or may request the installation of admission decisions only (i.e., resource initiation request (reservation only)) and await a separate RIR (commitment) later for gate opening and resource allocation. The detailed procedure for the separate RIR (commitment) is described in clause 10.1.1.1.3.

7) The PE-FE installs (and enforces) the final admission decisions sent from the PD-FE and sends an RIP back to the PD-FE.

8) The PD-FE sends an RIP back to the SCF.

10.1.1.1.2 QoS resource reservation procedure for a nomadicity/wholesale scenario

The SCF-requested QoS resource reservation procedure for a nomadicity/wholesale scenario is illustrated in Figure 11 that is initiated by a resource initiation request from the home SCF. The home/retail PD-FE authorizes the request, and finds that the required resources belong to the visited/wholesale network. Then the home/retail PD-FE (PD-FE(H)) sends the request to the visited/wholesale PD-FE (PD-FE(V)).

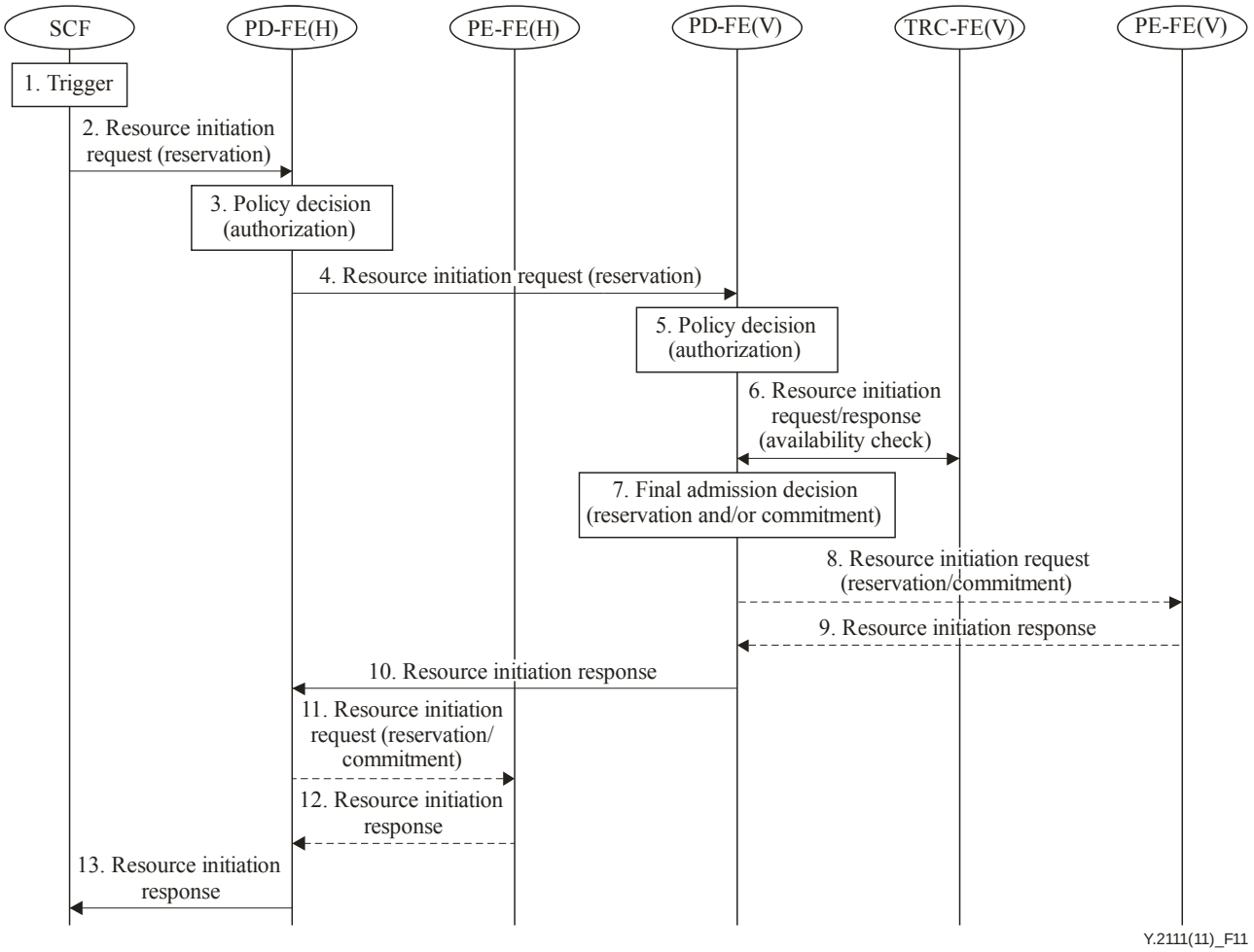


Figure 11 – SCF-requested QoS resource reservation procedure for a nomadicity/wholesale scenario

1) A resource initiation request (reservation) (RIR (reservation)) is usually triggered by a service establishment event or an internal action in the SCF. An example event is that a service signalling message is received at or generated by the SCF.

2) The SCF determines or derives the QoS requirement parameters (such as bandwidth, class of service) for the media flows of a given service. It then sends an RIR (reservation) with the media flow description and its QoS parameters to the PD-FE(H) across the Rs reference point for QoS resource authorization and reservation.

3) On receipt of the RIR (reservation), the PD-FE(H) authorizes the required QoS resources for the media flow. The PD-FE(H) checks if the media flow description and the required QoS resources are consistent with network policy rules held in the PD-FE(H) and the transport subscription information held in the NACF. If successful, the PD-FE(H) makes the initial policy decisions based on the transport subscription information, network policy rules and service information.

4) As the PD-FE(H) does not own the resources in the transport network, the RIR is sent further to the PD-FE(V).

5) On receipt of the RIR (reservation), the PD-FE(V) authorizes the required QoS resources for the media flow. The PD-FE(V) checks if the media flow description and the required QoS resources are consistent with network policy rules held in the PD-FE(V).

6) The PD-FE(V) positions and determines which access networks and core networks are involved for the media flow. The PD-FE(V) sends an RIR (availability check) to the TRC-FE(V) to check resource availability in the involved network.

7) The PD-FE(V) makes the final admission decisions based on the results of steps (5) and (6). If the media flow is not admitted, the PD-FE(V) sends an RIP with the rejection reason back to the PD-FE(H).

8) The PD-FE(V) determines whether this service request requires sending a request to the PE-FE(V). If needed, the PD-FE(V) sends an RIR to install the final admission decisions in the PE-FE(V).

9) The PE-FE(V) installs (and enforces) the final admission decisions sent from the PD-FE(V) and sends an RIP back to the PD-FE(V).

10) The PD-FE(V) sends an RIP back to the PD-FE(H).

11) The PD-FE(H) determines whether this service request requires sending a request to the PE-FE(H). If needed, the PD-FE(H) sends an RIR to install the admission decisions in the PE-FE(H).

12) The PE-FE(H) installs (and enforces) the admission decisions sent from the PD-FE(H) and sends an RIP back to the PD-FE(H).

13) The PD-FE(H) sends an RIP back to the SCF.

Note that nomadicity can be supported through inter-SCF communication without the involvement of the Ri reference point.

Another SCF-requested QoS resource reservation procedure for nomadicity scenario is illustrated in Figure 12 that is initiated by a resource initiation request from the visited SCF. The PD-FE(V) performs the admission control based on the resources available, and its own network policy rules. As the NGN visited provider cannot obtain the access user profile, the PD-FE(V) sends the request to the PD-FE(H) for authorization.

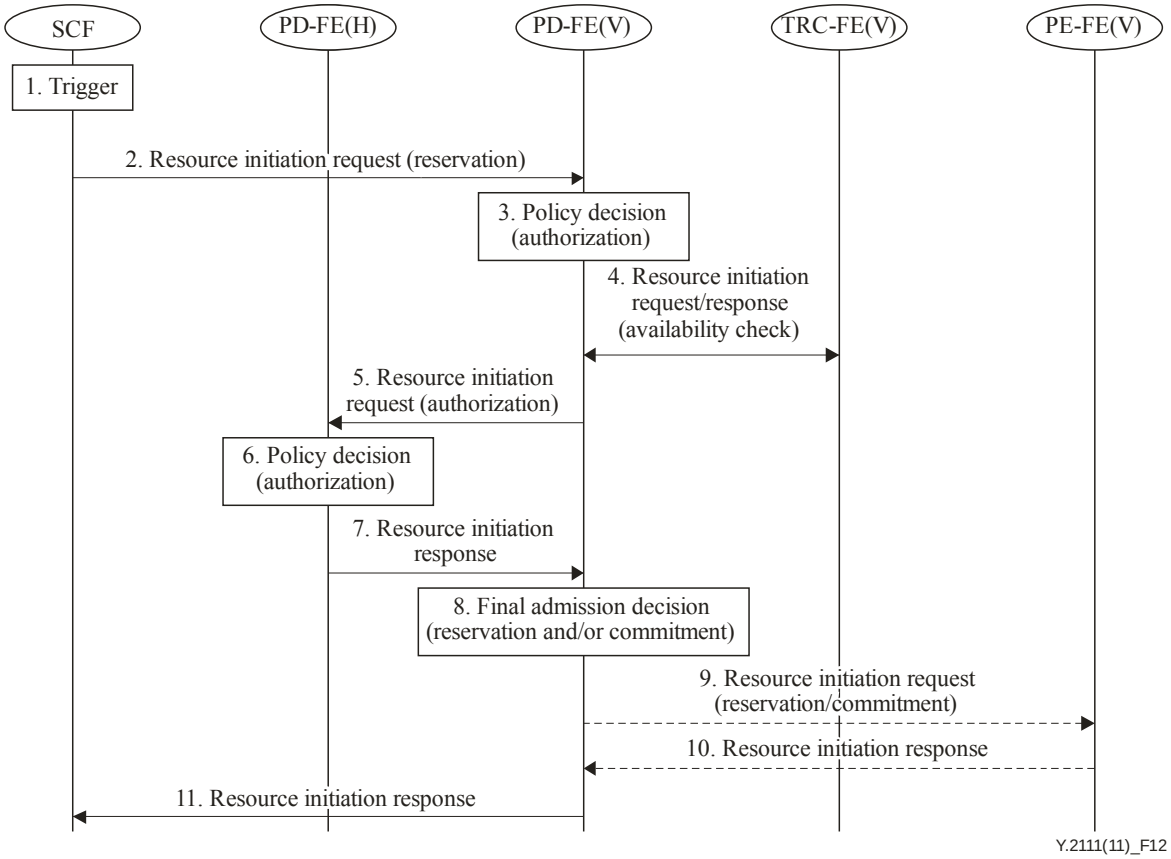


Figure 12 – SCF-requested QoS resource reservation procedure for nomadicity scenario 2

1) A resource initiation request (reservation) (i.e., RIR (reservation)) is usually triggered by a service establishment event or an internal action in the SCF. An example event is that a service signalling message is received at or generated by the SCF.

2) The SCF determines or derives the QoS requirement parameters (such as bandwidth, class of service) for the media flows of a given service. It then sends an RIR (reservation) with the media flow description and its QoS parameters to the PD-FE(V) across the Rs reference point for QoS resource authorization and reservation.

3) On receipt of the RIR (reservation), the PD-FE(V) authorizes the required QoS resources for the media flow. The PD-FE(V) checks if the media flow description and the required QoS resources are consistent with network policy rules held in the PD-FE(V).

4) The PD-FE(V) positions and determines which access networks and core networks are involved for the media flow. The PD-FE(V) sends an RIR (availability check) to the TRC-FE(V) to check resource availability in the involved network.

5) As the PD-FE(V) does not own the access user profile, the RIR is sent on further to the PD-FE(H).

6) On receipt of the RIR (reservation), the PD-FE(H) authorizes the required QoS resources for the media flow. The PD-FE(H) checks if the media flow description and the required QoS resources are consistent with network policy rules held in the PD-FE(H) and the transport subscription information held in the NACF. If successful, the PD-FE(H) makes the initial policy decisions based on the transport subscription information, network policy rules and service information.

7) After authorization, an RIP is sent to the PD-FE(V) including the initial policy decisions from the PD-FE(H).

8) The PD-FE(V) makes the final admission decisions based on the results of steps (4) and (7).

9) The PD-FE(V) may send an RIR to install the final admission decisions in the PE-FE(V).

10) The PE-FE(V) installs (and enforces) the final admission decisions sent from the PD-FE(V) and sends an RIP back to the PD-FE(V).

11) The PD-FE(V) sends an RIP back to the SCF.

10.1.1.1.3 Admission decision activation procedure

Depending on the network policy rules and service requirement, either single-phase or two-phase resource commitment schemes are applied. In the single-phase scheme, the gates are opened and the requested resource is allocated immediately when the final admission decisions are installed in the PE-FE.

In the two-phase scheme, the final admission decisions are installed in the PE-FE first; however, the admission decisions are not enforced until an RIR (commitment) is received from the SCF. The admission decision activation procedure for the two-phase scheme is illustrated in Figure 13.

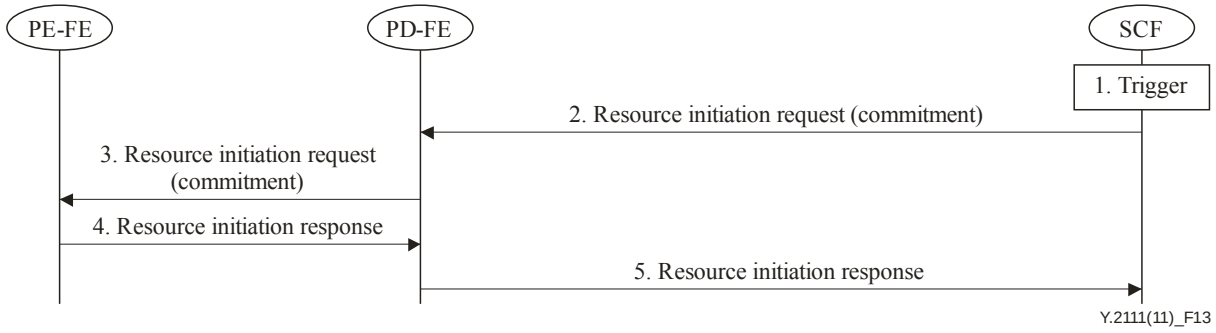


Figure 13 – Admission decision activation procedure

10.1.1.1.4 Admission decision de-activation procedure

The admission decision de-activation procedure illustrated in Figure 14 shows that it is invoked by a resource modification request (i.e., RMR (de-activation)) from the SCF. It causes the PE-FE to stop enforcing admission decisions previously installed for the media flow, but the admission decisions are not deleted or removed from the PE-FE. The de-activation procedure is only needed when the forwarding of media flow needs to be disabled.

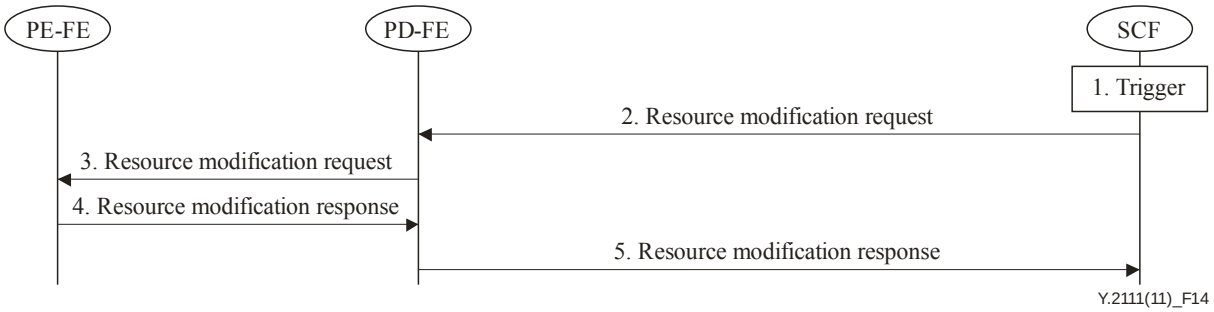


Figure 14 – Admission decision de-activation procedure

10.1.1.1.5 QoS resource modification procedure

The SCF-requested QoS resource modification procedure illustrated in Figure 15 shows that it is invoked by a resource modification request (i.e., RMR (modification)) from the SCF. It makes the PD-FE modify the admission decisions (e.g., QoS attributes). The RMR (modification) is usually triggered by a media renegotiation event or an internal action in the SCF. An example event is that a service signalling message is received at or generated by the SCF. The RMR (modification) may be applied to authorization, reservation or commitment phases.

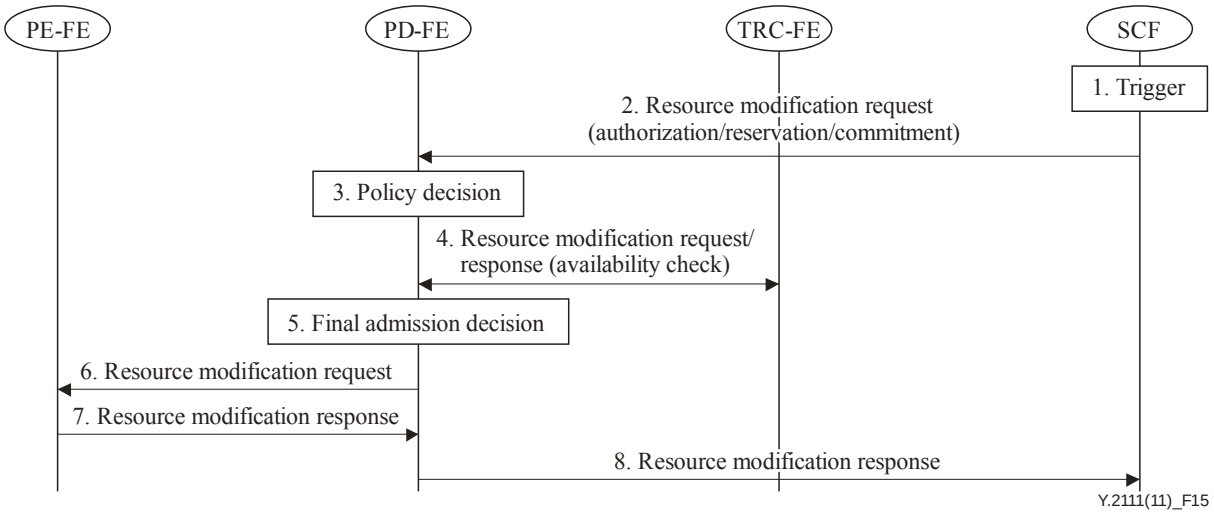


Figure 15 – SCF-requested QoS resource modification procedure

10.1.1.1.6 QoS resource release procedure

The SCF-requested QoS resource release procedure illustrated in Figure 16 shows that it is invoked by a resource release request (i.e., RRR) from the SCF for a given service. The RRR is triggered usually by a service termination event, a media renegotiation event, or an internal action in the SCF. An example event is that a service signalling message is received at or generated by the SCF. When multiple TRC-FE instances are present in the form of distributed hierarchical structure, the PD-FE contacts the top tier TRC-FE instance for resource release operations.

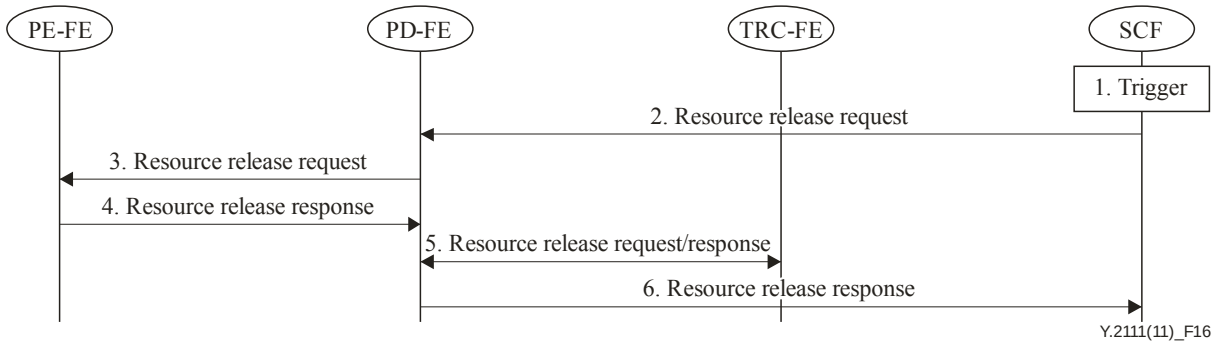


Figure 16 – SCF-requested QoS resource release procedure

10.1.1.2 Failure handling

NOTE – The complexity of providing network failure indications to SCF needs further study.

10.1.1.2.1 PE-FE-indicated event notification procedure

During the running of a media flow, if the PE-FE cannot provide the requested QoS resource any longer for the media flow due to special events, e.g., the reference point path failure, the PE-FE is required to send a resource notification to the PD-FE on its own initiative. The PD-FE is required to forward the resource notification to the relevant SCF for alerting the affected sessions as illustrated in Figure 17.

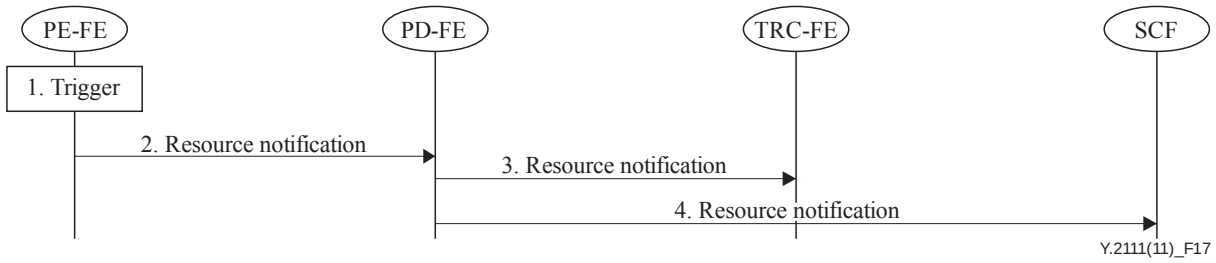


Figure 17 – PE-FE-indicated event notification procedure

10.1.1.2.2 TRC-FE-indicated event notification procedure

During the running of a media flow, if the TRC-FE detects that the network cannot provide the reserved QoS resource any longer for the media flow due to special events, e.g., network failure, the TRC-FE is required to send a resource notification to the PD-FE on its own initiative. The PD-FE is required to forward the resource notification to the relevant SCF for alerting the affected sessions. The PD-FE may send the resource release request (RRR) to the affected PE-FE to release the network resource as illustrated in Figure 18. When multiple TRC-FE instances are present in the form of distributed hierarchical structure, the co-located TRC-FE may report the events to the top tier TRC-FE instance for event notification operations.

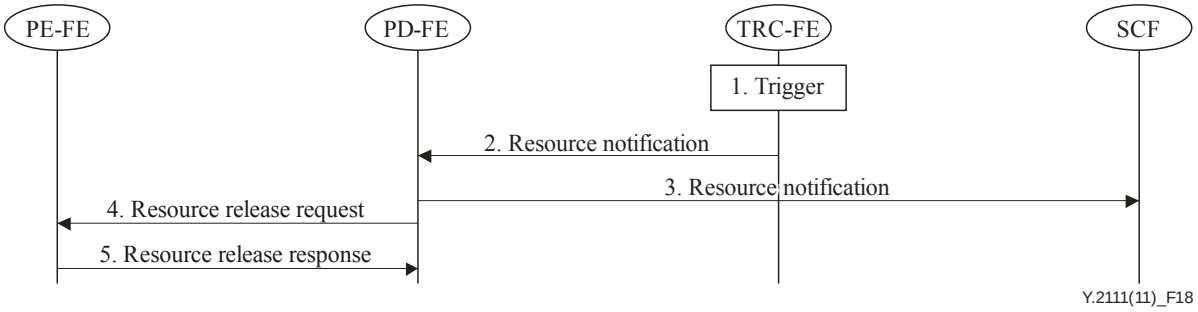


Figure 18 – TRC-FE-indicated event notification procedure

10.1.2 CPE-requested QoS control procedures

Scenario 2 described in clause 7.1 uses the CPE-requested QoS resource reservation mechanism, i.e., the CPE sends a ‘QoS request' over a dedicated path-coupled QoS signalling to invoke the QoS resource reservation for a given flow. Based on the 'QoS request' from the CPE, the network border node is responsible for sending the RACF a resource decision request (i.e., RDR) to pull the admission control decisions from the RACF.

The following procedures are for support of CPE-requested QoS resource reservation mechanism.

10.1.2.1 Basic procedures

10.1.2.1.1 SCF-requested QoS initial authorization procedure

The SCF-requested QoS initial authorization procedure illustrated in Figure 19 shows that it is invoked by a service establishment signalling message from CPE.

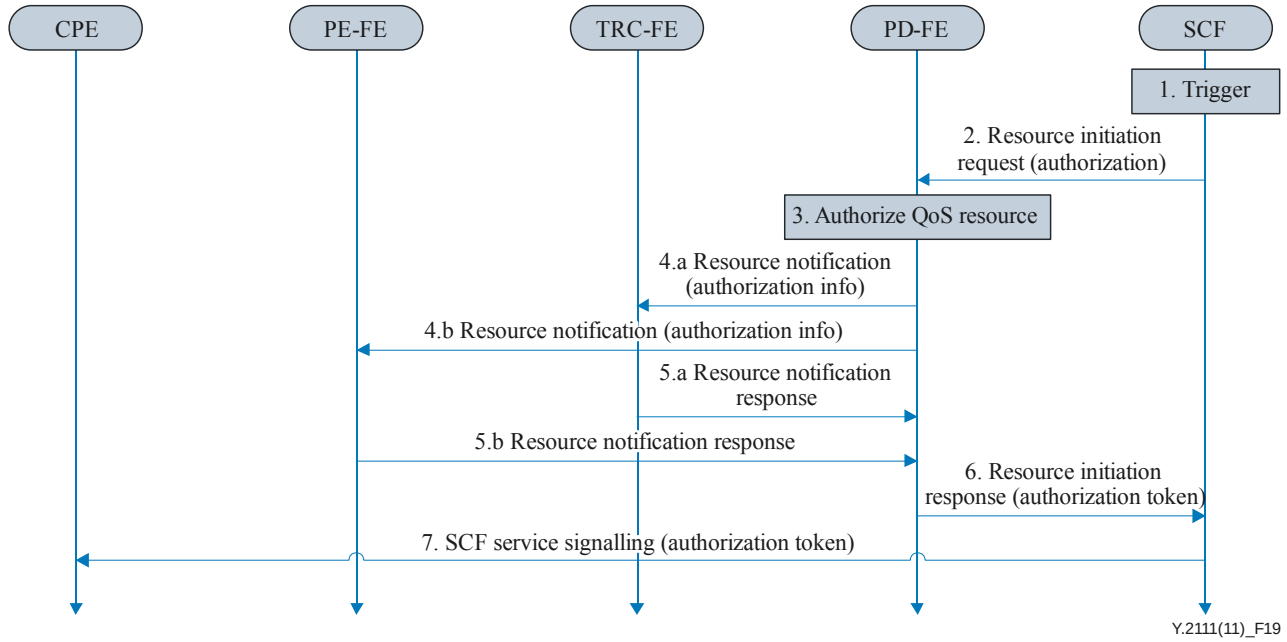


Figure 19 – SCF-requested QoS initial authorization procedure

1) The SCF-requested QoS initial authorization procedure is usually triggered by a service establishment signalling message.

2) The SCF sends an RIR to the PD-FE for requesting authorization.

3) The PD-FE makes a QoS resource authorization decision based on the subscription profile and the operator policies. Optionally, the PD-FE may generate an authorization token for a given service.

4) (Steps (4) and (5) take place to allow the PE-FE and/or the TRC-FE to select the correct PD-FE, when there are multiple PD-FEs)

   a) The PD-FE sends the resource notification messages with the authorization information to the TRC-FE. The TRC-FE may maintain the binding relation of the PD-FE and the authorization information.

   b) The PD-FE sends the resource notification messages with the authorization information to the PE-FE. The PE-FE may maintain the binding relation of the PD-FE and the authorization information.

5)

   a) The TRC-FE sends the resource notification response message to the PD-FE.

b) The PE-FE sends the resource notification response message to the PD-FE.

6) The PD-FE sends an RIR to the SCF. If generating the authorization token in step (3), the PD-FE may take the token with the RIR message.

7) The SCF continues the service signalling negotiation with CPE. If receiving the authorization token from the PD-FE, the SCF may return the token to CPE.

10.1.2.1.2 CPE-requested QoS resource reservation procedure triggered by PE-FE

The CPE-requested QoS resource reservation procedure illustrated in Figure 20 shows that it is invoked by a dedicated path-coupled QoS signalling message from the CPE for a given flow.

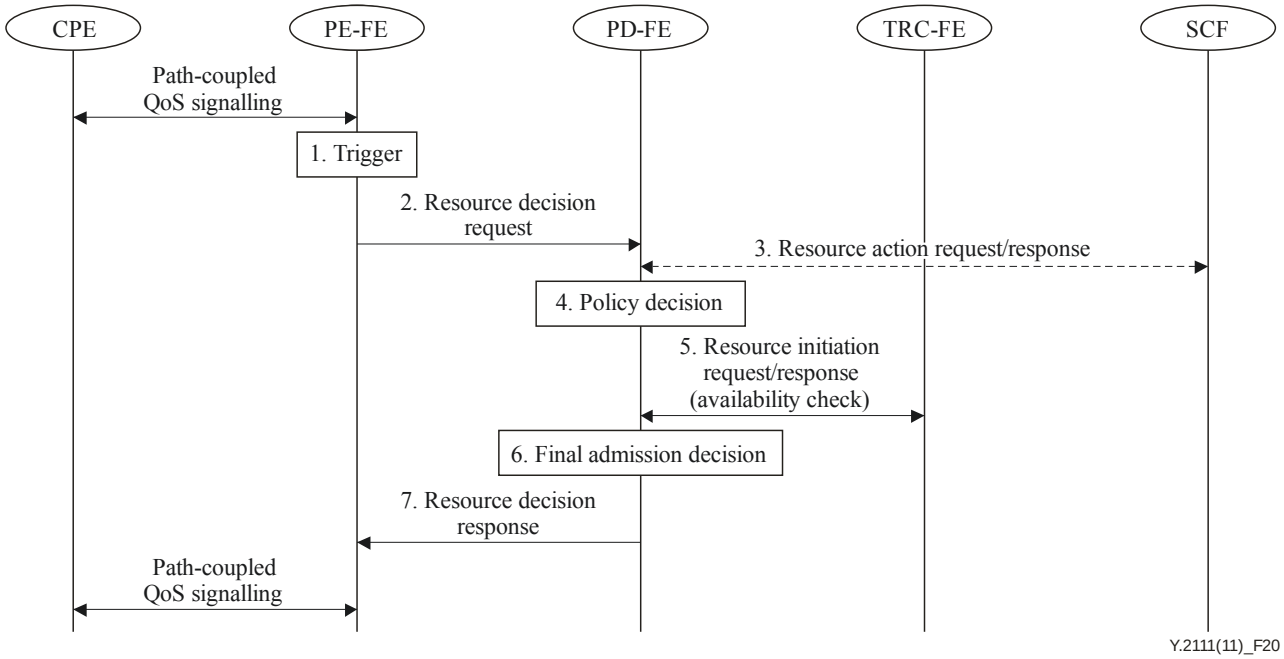


Figure 20 – CPE-requested QoS resource reservation procedure triggered by PE-FE

1) A resource decision request (i.e., RDR) is usually triggered by a request indicated through the QoS signalling from the CPE to reserve the required QoS resource for a given flow. Other nodes in the access or core networks may forward the QoS signalling messages transparently or perform the QoS reservation along the path.

2) Based on the 'QoS request' from the CPE, the PE-FE selects the right PD-FE according to the binding information, and sends an RDR with the flow description and its QoS parameters to the PD-FE across the Rw reference point to pull the admission control decisions from the PD-FE. The PE-FE is required to be able to filter duplicate or malicious QoS request messages, especially if the QoS signalling is refreshed periodically.

3) On receipt of the RDR (if the SCF previously requested the QoS initial authorization related to the flow), the PD-FE is required to send a resource action request (i.e., RAR) to the SCF for retrieving the service information of the flow.

4) The PD-FE checks if the flow description, the required QoS resources and the service information are consistent with network policy rules held in the PD-FE and the transport subscription information held in the NACF.

5) The PD-FE identifies and determines which access networks and core networks are involved for the media flow. If there are TRC-FE instances in an involved network, the PD-FE sends an RIR (availability check) to one of the TRC-FE instances registered in the PD-FE to check if the required QoS resource is available in the involved network. If there are multiple TRC-FE instances in the involved network, they may communicate with each other to determine if the required QoS resource is available in the involved network. Then

the TRC-FE instance that received the RIR (availability check) is required to send an RIP back to the PD-FE. When multiple TRC-FE instances are present in the form of distributed hierarchical structure, the top tier TRC-FE instance forwards the request to other TRC-FE instances in case those instances are in control of resources referenced in the request (i.e., the top tier TRC-FE has delegated resources to other TRC-FE instances). In this case the top tier TRC-FE makes the final resource admission decision based on the results of resource admission from all other instances.

6) The PD-FE makes the final admission decision based on the results of steps (4) and (5).

7) If the RDR from the PE-FE is admitted, the PD-FE is required to send a resource decision response (commitment) (i.e., RDP) to install the final admission decisions in the PE-FE.

In order to ensure that the PE-FE selects the right PD-FE among multiple PD-FEs, there are the following options:

- If step (2) of the resource reservation procedure is performed, the PE-FE can select the right PD-FE according to the stored PD-FE information received in the RIR.
- If step (2) of the resource reservation procedure is not performed, the PE-FE can select the right PD-FE, based on its pre-configuration.
- If the PE-FE cannot identify the right PD-FE through the above options, it sends the message to all of the PD-FEs interacting with it, to find the right PD-FE.

Note that the installed admission decisions may be enforced automatically and immediately or may wait for an RIR (commitment) for gate opening and resources allocation. The PE-FE may process the QoS signalling messages in a termination, snooping or proxy way. Refer to Figure 21 a), b) and c) respectively. If processing in a proxy way, the PE-FE may modify, aggregate and de-aggregate the QoS signalling messages.

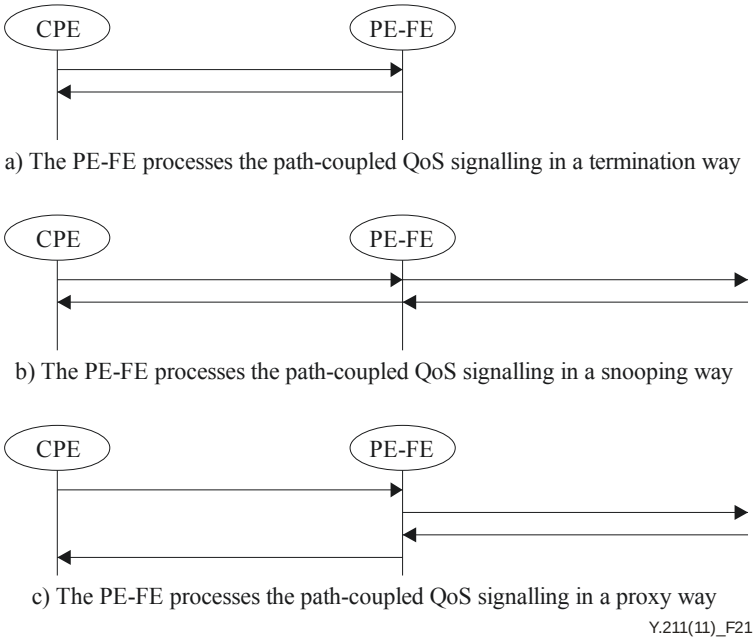


Figure 21 – Three possible QoS signalling processing ways at the PE-FE (not exhaustive)

10.1.2.1.3 SCF-requested QoS initial authorization procedure for nomadicity scenario

The SCF-requested QoS initial authorization procedure for nomadicity scenario is illustrated in Figure 22. It is invoked by a service establishment signalling message from CPE. The home PD-FE (PD-FE(H)) makes QoS resource authorization decision based on the subscription profile and the operator policies. If the required resources belong to the visited network, the PD-FE(H) sends the request to the visited PD-FE (PD-FE(V)) for requesting authorization.

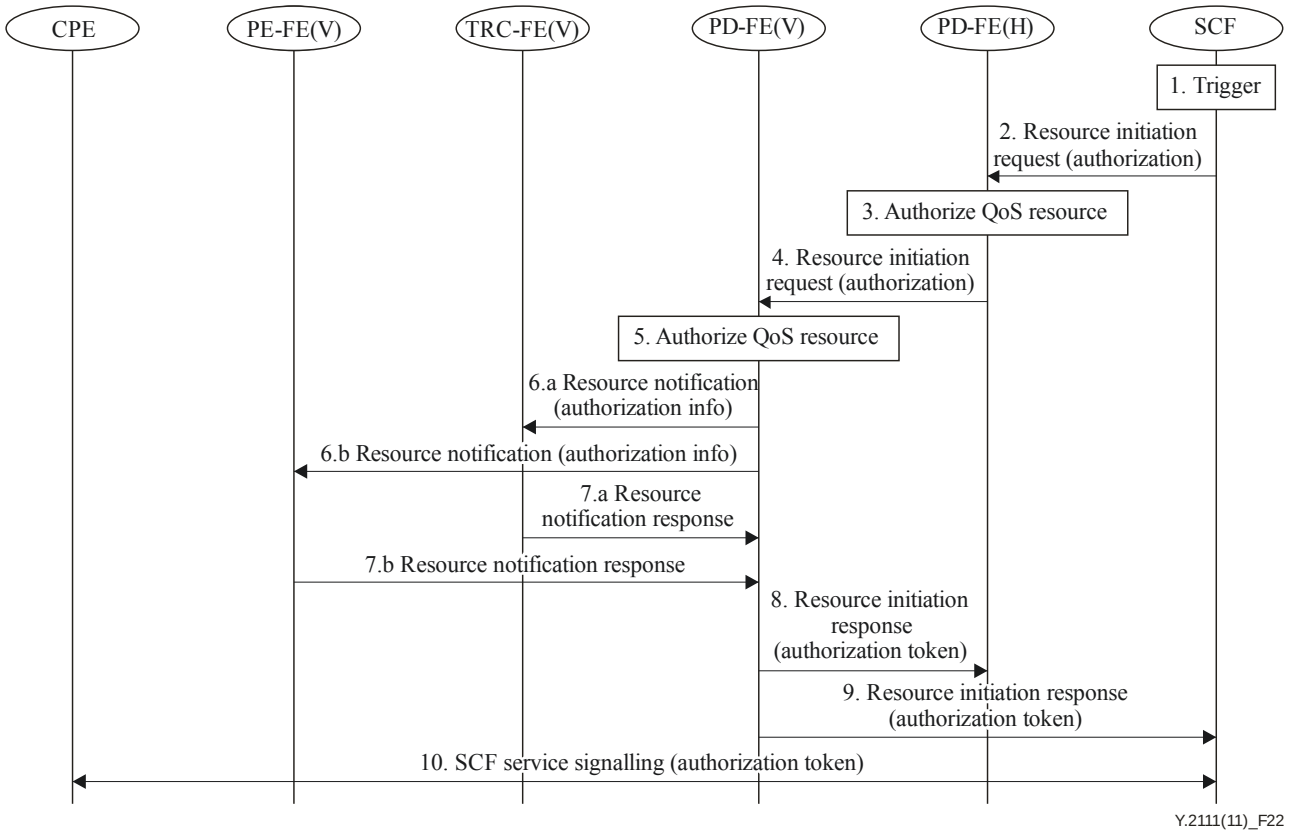


Figure 22 – SCF-requested QoS initial authorization procedure for a nomadicity scenario

1) The SCF-requested QoS initial authorization procedure is usually triggered by a service establishment signalling message.

2) The SCF sends an RIR to the PD-FE(H) for requesting authorization.

3) The PD-FE(H) makes a QoS resource authorization decision based on the subscription profile and the operator policies.

4) As the PD-FE(H) does not own the resources in the transport network, the RIR is sent further to the visited PD-FE (PD-FE(V)).

5) The PD-FE(V) makes a QoS resource authorization decision based on the operator policies. Optionally, the PD-FE(V) generates an authorization token for a given service.

6) (Steps (6) and (7) take place to allow the PE-FE and/or the TRC-FE to select the correct PD-FE, when there are multiple PD-FEs)

   a) The PD-FE(V) sends the resource notification messages with the authorization information to the TRC-FE(V). The TRC-FE(V) maintains the binding relation of the PD-FE(V) and the authorization information.

   b) The PD-FE(V) sends the resource notification messages with the authorization information to the PE-FE(V). The PE-FE(V) maintains the binding relation of the PD-FE(V) and the authorization information.

7)

   a) The TRC-FE(V) sends the resource notification response message to the PD-FE(V).

   b) The PE-FE(V) sends the resource notification response message to the PD-FE(V).

8) The PD-FE(V) sends an RIR to the PD-FE(H). If generating the authorization token in step (5), the PD-FE(V) takes the token with the RIR message.

9) The PD-FE(H) sends an RIR to the SCF. If receiving the authorization token from the PD-FE(V), the PD-FE(H) takes the token with the RIR message.

10) The SCF continues the service signalling negotiation with the CPE. If receiving the authorization token from the PD-FE(H), the SCF returns the token to the CPE.

Another SCF-requested QoS initial authorization procedure for a nomadicity scenario is illustrated in Figure 23. It is invoked by a service establishment signalling message from the CPE. The PD-FE(V) makes a QoS resource authorization decision based on the operator policies. As the PD-FE(V) does not own the subscription profile, the PD-FE(V) sends the request to the PD-FE(H) for requesting authorization.

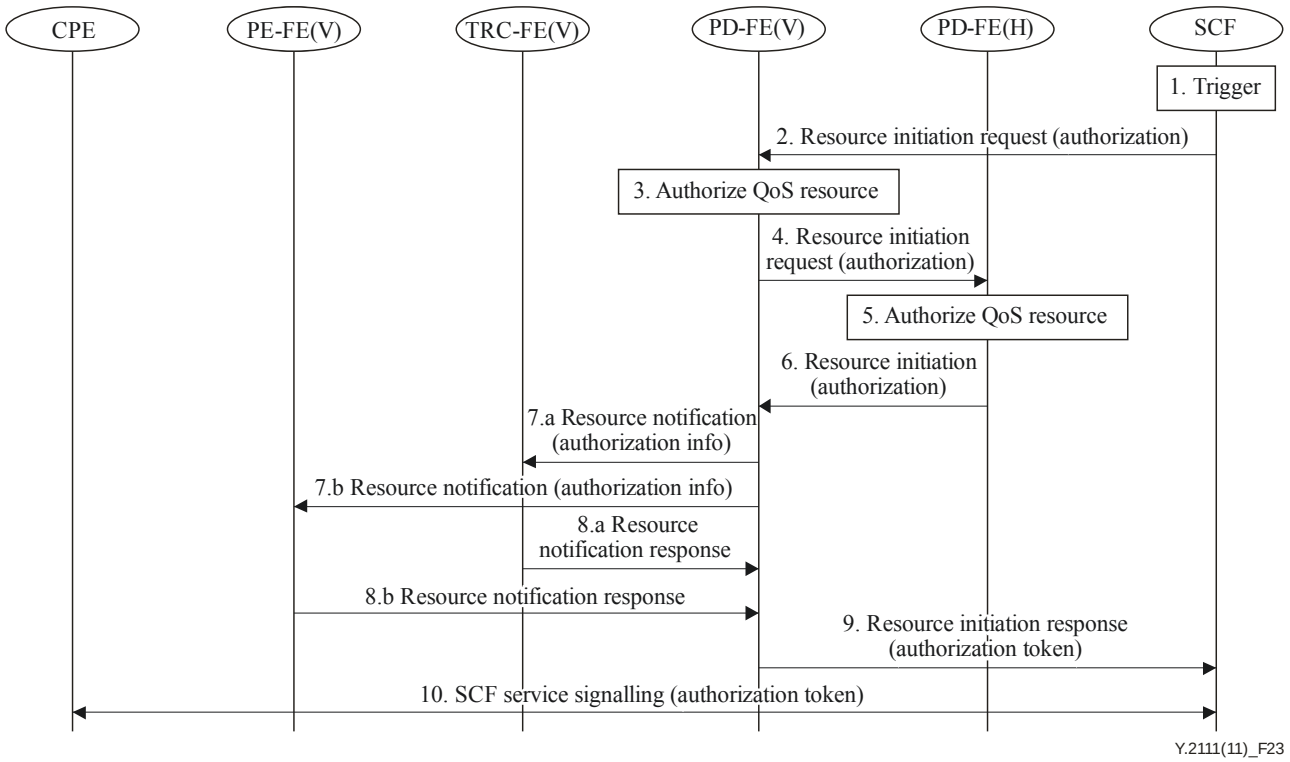


Figure 23 – SCF-requested QoS initial authorization procedure for nomadicity scenario 2

1) The SCF-requested QoS initial authorization procedure is usually triggered by a service establishment signalling message.
2) The SCF sends an RIR to the PD-FE(V) for requesting authorization.
3) The PD-FE(V) makes a QoS resource authorization decision based on the operator policies.
4) As the PD-FE(V) does not own the subscription profile, the RIR is sent on further to the PD-FE (H).
5) The PD-FE(H) makes a QoS resource authorization decision based on the subscription profile and the operator policies.
6) The PD-FE(H) sends an RIP to the PD-FE(V). Optionally, the PD-FE(V) generates an authorization token for a given service.
7)
   a) The PD-FE(V) may send the resource notification messages with the authorization information to the TRC-FE(V). The TRC-FE(V) maintains the binding relation of the PD-FE(V) and the authorization information.
   b) The PD-FE(V) may send the resource notification messages with the authorization information to the PE-FE(V). The PE-FE(V) maintains the binding relation of the PD-FE(V) and the authorization information.

8)

a) The TRC-FE(V) sends the resource notification response message to the PD-FE(V).

b) The PE-FE(V) sends the resource notification response message to the PD-FE(V).

9) The PD-FE(V) sends an RIP to the SCF. If the authorization token is generated in step (6), the PD-FE(V) takes the token with the RIP message.

10) The SCF continues the service signalling negotiation with the CPE. If the authorization token is received from the PD-FE(V), the SCF returns the token to the CPE.

10.1.2.1.4 CPE-requested QoS resource reservation procedure triggered by the PE-FE for a nomadicity scenario

The CPE-requested QoS resource reservation procedure for a nomadicity scenario is illustrated in Figure 24. It shows that it is invoked in the visited network by a dedicated path-coupled transport signalling message from the CPE for a given flow. Based on the 'QoS request' from the CPE, the visited PE-FE sends an RDR with the flow description and its QoS parameters to the visited PD-FE. On receipt of the RDR (if the PD-FE(H) previously requested the QoS initial authorization related to the flow), the PD-FE(V) is required to send a resource action request (i.e., RAR) to the PD-FE(H) for retrieving the service information of the flow.

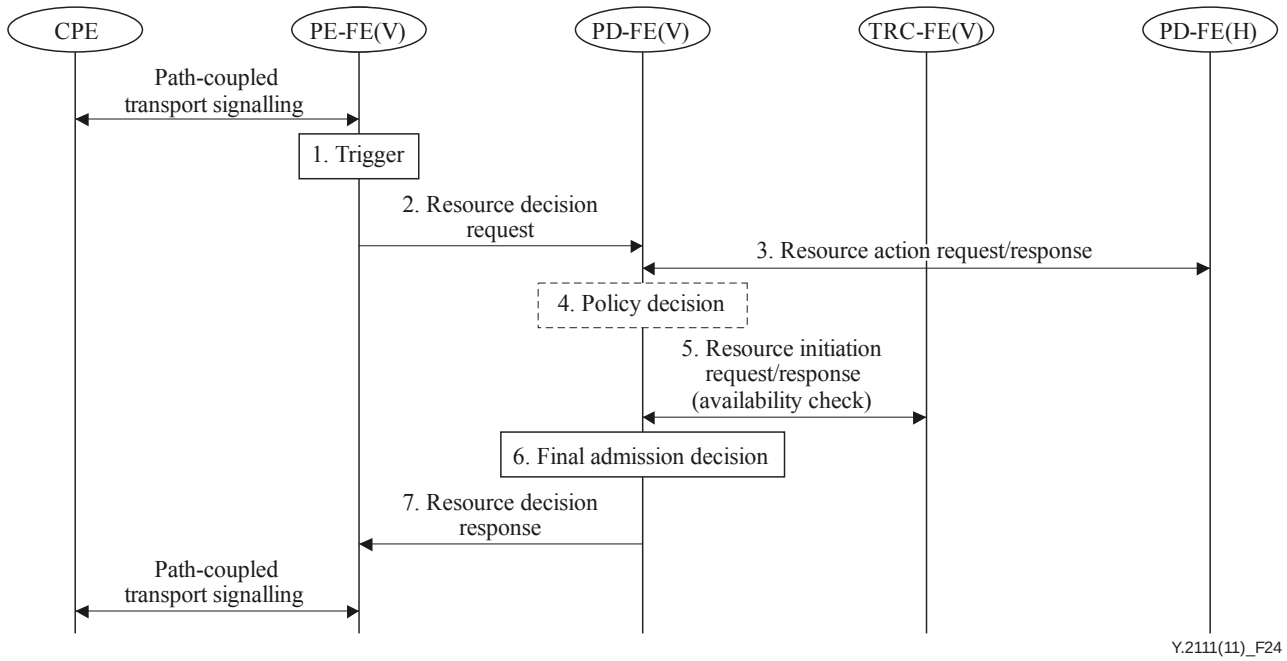


Figure 24 – CPE-requested QoS resource reservation procedure triggered by the PE-FE for a nomadicity scenario

1) A resource decision request (i.e., RDR) is usually triggered by a request indicated through the QoS signalling from the CPE to reserve the required QoS resource for a given flow. Other nodes in the access or core networks may forward the QoS signalling messages transparently or perform the QoS reservation along the path.

2) Based on the QoS request from the CPE, the PE-FE(V) selects the right PD-FE(V) according to the binding information, and sends an RDR with the flow description and its QoS parameters to the PD-FE(V) across the Rw reference point to pull the admission control decisions from the PD-FE(V). It is required that the PE-FE(V) be able to filter duplicate or malicious QoS request messages, especially if the QoS signalling is refreshed periodically.

3) On receipt of the RDR (if the PD-FE(H) previously requested the QoS initial authorization related to the flow), the PD-FE(V) sends a resource action request (i.e., RAR) to the PD-FE(H) for retrieving the service information of the flow.

4) (Optional) If there is no QoS initial authorization procedure, the PD-FE(V) checks if the flow description, the required QoS resources and the service information are consistent with network policy rules held in the PD-FE(V).

5) The PD-FE(V) identifies and determines which access networks and core networks are involved for the media flow. The PD-FE(V) sends an RIR (availability check) to the TRC-FE(V) to check if the required QoS resource is available in the involved network.

6) The PD-FE(V) makes the final admission decision based on the results of steps (4) and (5).

7) If the RDR from the PE-FE(V) is admitted, the PD-FE(V) sends a resource decision response (commitment) (i.e., RDP) to install the final admission decisions in the PE-FE(V).

10.1.2.1.5 CPE-requested QoS resource modification procedure

The CPE-requested QoS resource modification procedure illustrated in Figure 25 is invoked by a resource decision request, i.e., RDR from the PE-FE for a given flow. The RDR is usually triggered by a request indicated through the QoS signalling from the CPE to modify the reserved resource for the flow.

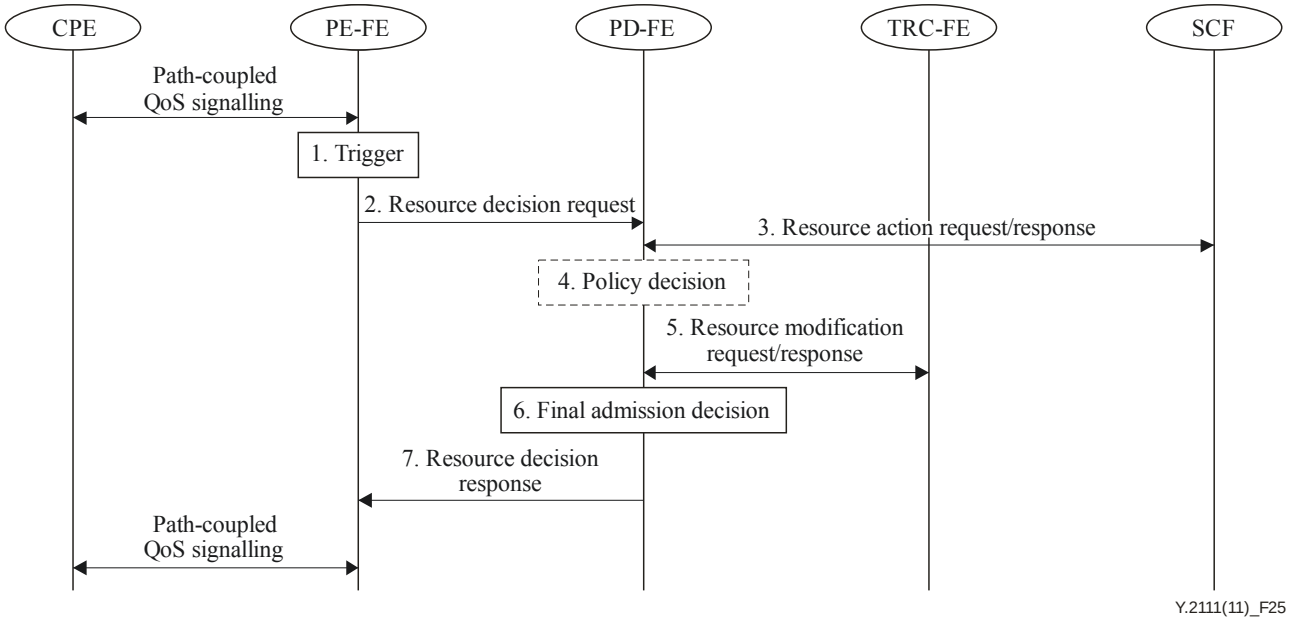


Figure 25 – CPE-requested QoS resource modification procedure

10.1.2.1.6 Admission decision activation procedure

In the two-phase or three-phase control scheme, the PD-FE opens the gates and activates the admission decisions installed in the PE-FE only upon receiving the admission activation request from the SCF. The admission decision activation procedure is only needed when the SCF ordered the PD-FE to wait for an RIR (commitment). The admission decision activation procedure is invoked by the RIR (commitment) from the SCF for a given service as illustrated in Figure 26.

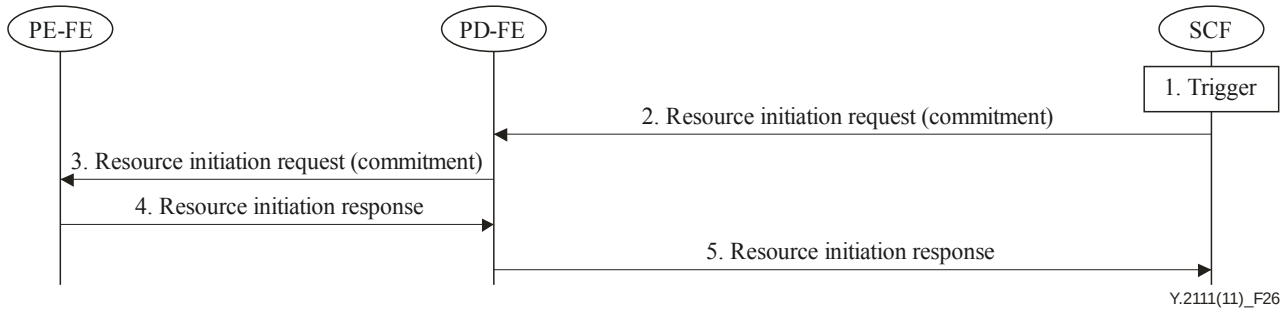


Figure 26 – Admission decision activation procedure

10.1.2.1.7 Admission decision de-activation procedure

The admission decision de-activation procedure illustrated in Figure 27 is invoked by an RMR from the SCF for a given service. It causes the PE-FE to stop enforcing admission decisions previously installed for the media flow of the service, but the admission decisions are not deleted or removed from the PE-FE. The de-activation procedure is only needed when the forwarding of media flow of a given service needs to be disabled.

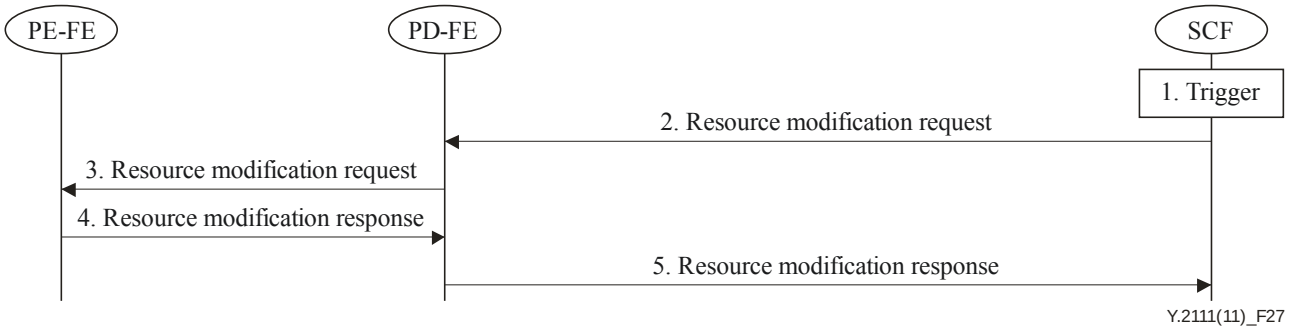


Figure 27 – Admission decision de-activation procedure

10.1.2.1.8 CPE-requested QoS resource release procedure

The CPE-requested QoS resource release procedure illustrated in Figure 28 is invoked by a resource notification from the PE-FE for a given flow. The resource notification is usually triggered by a request indicated through the QoS signalling from the CPE to release the reserved resource for the flow.

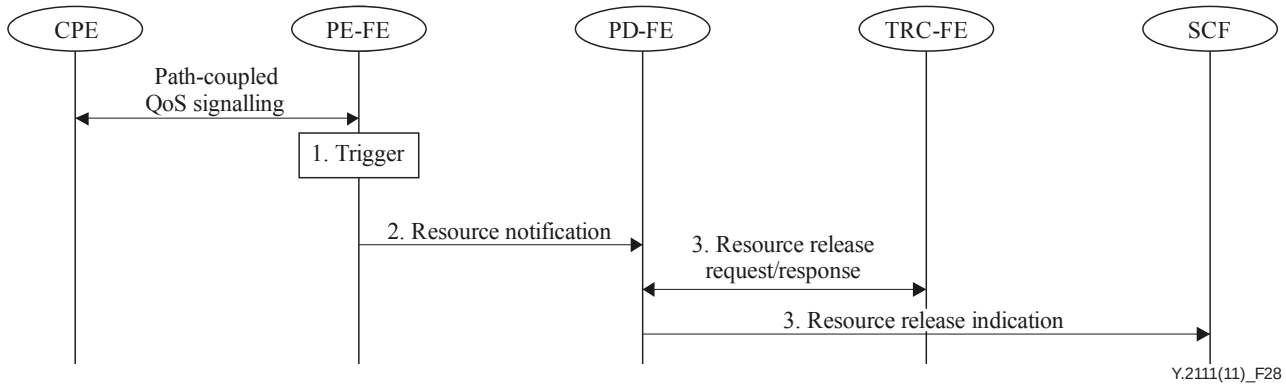


Figure 28 – CPE-requested QoS resource release procedure

10.1.2.1.9 SCF-requested QoS resource release procedure

The SCF-requested QoS resource release procedure illustrated in Figure 29 is invoked by a RRR from the SCF for a given service. The RRR is triggered usually by a service termination event, a

media renegotiation event, or an internal action in the SCF. An example event is that a service signalling message is received at or generated by the SCF.

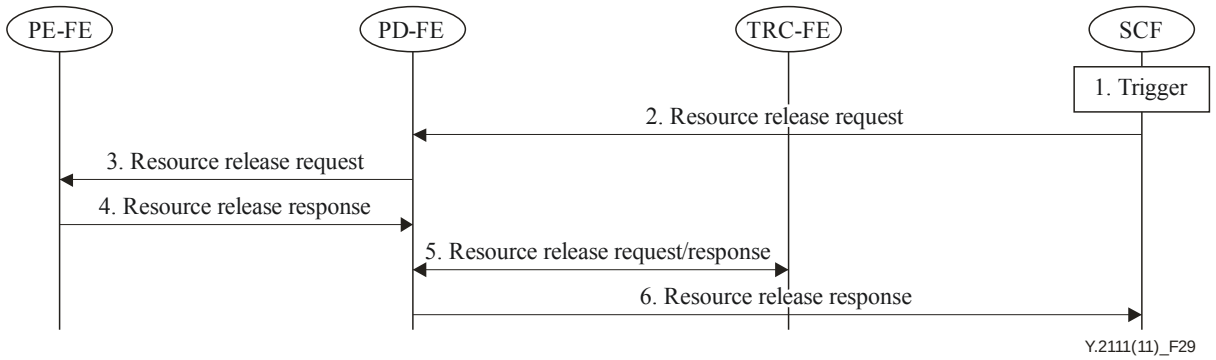


Figure 29 – SCF-requested QoS resource release procedure

For both CPE-requested and SCF-requested QoS resource release procedure, when multiple TRC-FE instances are present in the form of distributed hierarchical structure, the PD-FE contacts the top tier TRC-FE instance for resource release operations.

10.1.2.2 Failure handling

NOTE – The complexity of providing network failure indications to SCF needs further study.

10.1.2.2.1 PE-FE-indicated event notification procedure

During the running of a media flow, if the PE-FE cannot provide the reserved QoS resource any longer for the media flow due to the failure of the reference point path, the PE-FE is required to send a resource notification to the PD-FE on its own initiative. If the reserved QoS resource is relevant with an SCF session, the PD-FE is required to forward the resource notification to the SCF as illustrated in Figure 30.

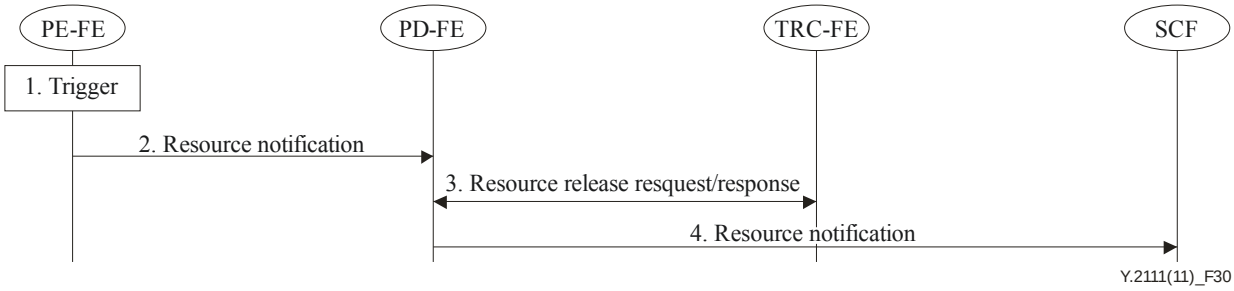


Figure 30 – PE-FE-indicated event notification procedure

10.1.2.2.2 TRC-FE-indicated event notification procedure

During the running of a media flow, if the TRC-FE detects that the network cannot provide the reserved QoS resource any longer for the media flow due to the network failure, the TRC-FE is required to send a resource notification to the PD-FE on its own initiative. If the reserved QoS resource is relevant to an SCF session, the PD-FE is required to forward the resource notification to the SCF as illustrated in Figure 31. When multiple TRC-FE instances are present in the form of distributed hierarchical structure, the co-located TRC-FE may report the events to the top tier TRC-FE instance for event notification operations.

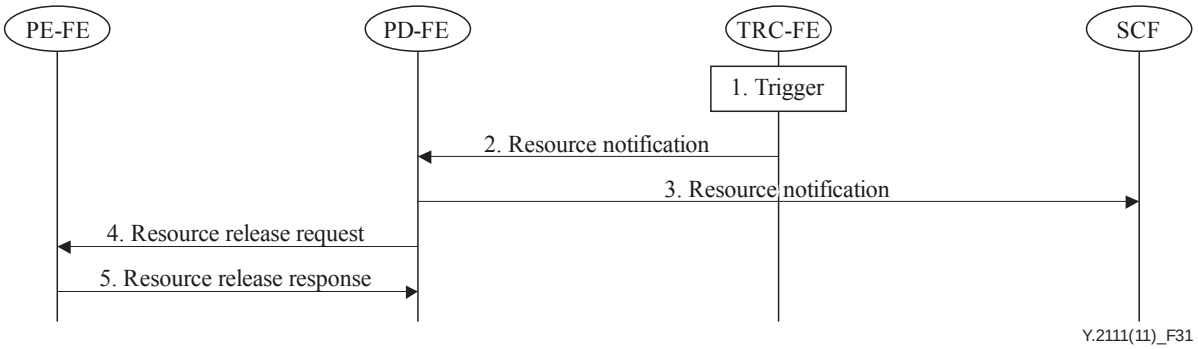


Figure 31 – TRC-FE-indicated event notification procedure

10.1.3 CPE attachment and detachment procedures

The procedure of the CPE's subscription-based policy and resource provisioning is illustrated in Figure 32 when the CPE is attached to an access network.

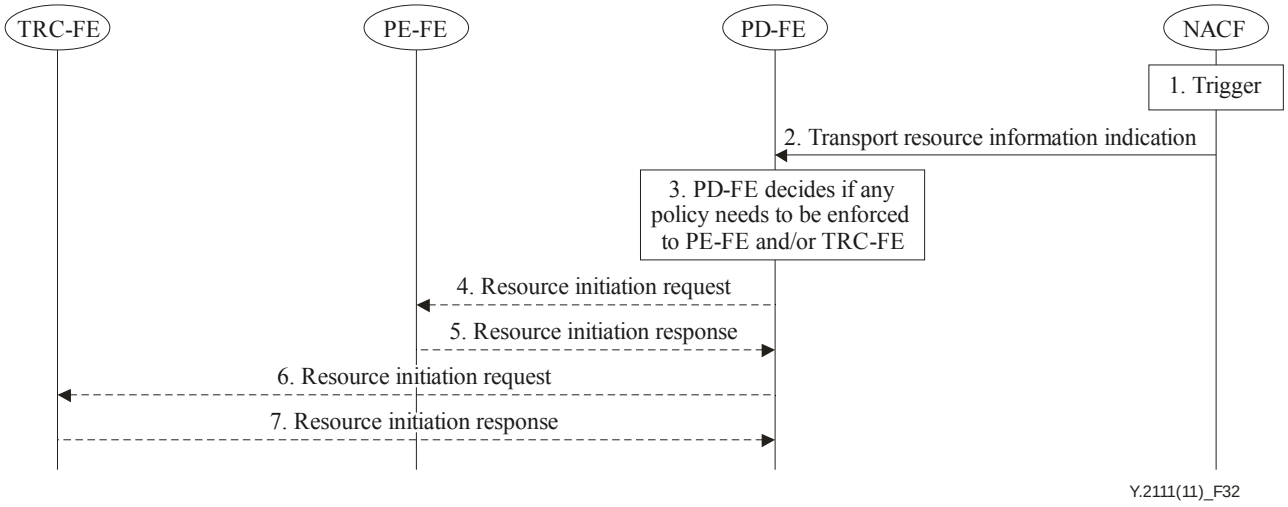


Figure 32 – CPE attachment procedure

1) The NACF finds that a CPE is attached to an access network.
2) The NACF sends the transport resource information indication about the subscriber's transport resource information and default configuration, to the PD-FE.
3) The PD-FE checks if the subscriber's policies need to be installed in the PE-FE.
4) The PD-FE requests the PE-FE to enforce the policies by sending a resource initiation request if it decides that the subscriber's policy needs to be installed in step (3).
5) The PE-FE confirms the enforcement of the policies.
6) The PD-FE requests the TRC-FE to enforce the policies by sending a resource initiation request if it decides that the policies need to be installed into the TRC-FE in step (3).
7) The TRC-FE confirms the enforcement of the policies. The detailed procedure of how the TRC-FE interacts with the TRE-FE is for further study.

The procedure of the CPE's subscription-based policy and resource release is illustrated in Figure 33, when the CPE is detached from an access network.

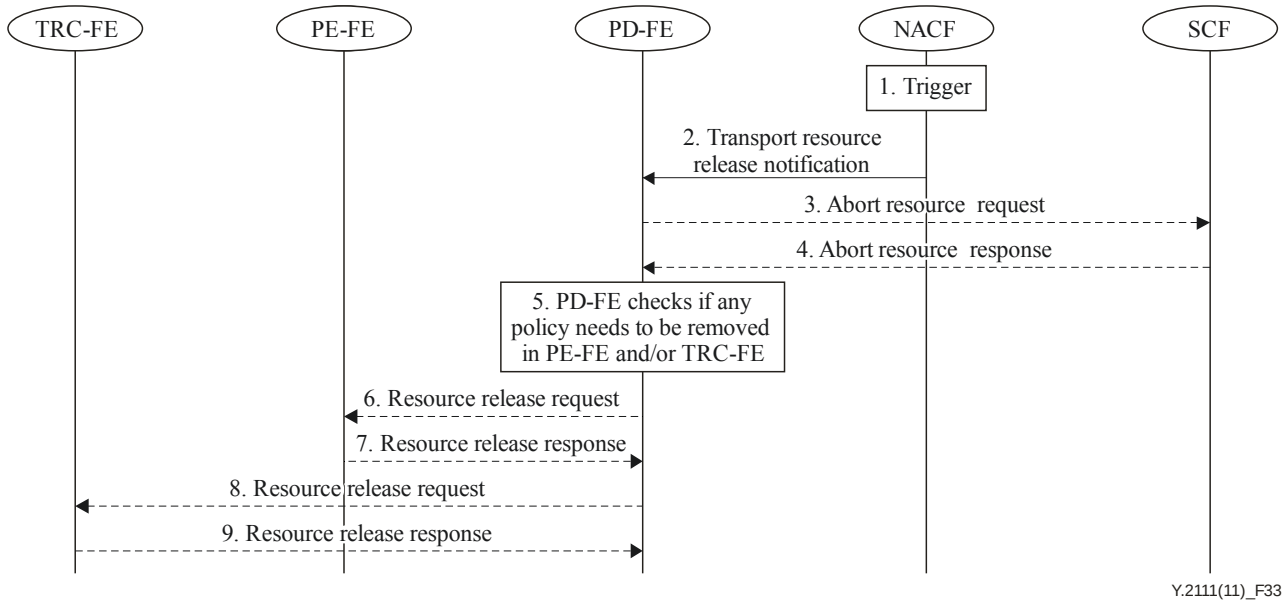


Figure 33 – CPE detachment procedure

1) The NACF finds that a CPE detaches itself from an access network.
2) The NACF notifies the PD-FE that the CPE is being detached by sending a transport resource release notification.
3) The PD-FE may send an abort resource request to the SCF in the case where the CPE detaches itself from the access network without the normal procedure of the session disconnection at the application level.
4) The SCF confirms the removal of the policies by sending an abort release response.
5) The PD-FE checks if any policies need to be removed at the PE-FE and/or the TRC-FE.
6) The PD-FE requests the PE-FE to remove policies by sending a resource release request if it decides that the policies need to be removed from the PE-FE in step (4).
7) The PE-FE confirms the removal of the policies by sending a resource release response.
8) The PD-FE requests the TRC-FE to remove the policies by sending a resource release request if it decides that the policies need to be removed from the TRC-FE in step (4).
9) The TRC-FE confirms the removal of the policies. The detailed procedure of how the TRC-FE interacts with the TRE-FE is for further study.

10.2 Procedures for NAPT control and NAT traversal

10.2.1 NAPT control procedures

This clause describes the procedures of controlling an IP address and/or port translation in the media path at borders between access and core networks and between core networks. The SCF (e.g., SCPF), PD-FE, TRC-FEs and PE-FEs are involved in performing the IP address and/or port translation.

The NAPT control procedure is required to be invoked by the RACF (e.g., PD-FE) based on the network security policy rules (e.g., network address hiding rules). The SCF is required to be able to perform the modification of message body for the NAPT upon the end-to-end call flow status, e.g., when service signalling messages to request and respond the session establishment (e.g., SIP INVITE and 183 Session Progress) are received and the indication of NAPT control is provided by the PD-FE. The PD-FE performs NAPT policy control, obtains the address binding information and performs the gate control to open/close the "gate".

10.2.1.1 Upon receipt of a session initiation request

1) The SCF is required to extract the source and destination network addresses and port numbers from the signalling message body received from the calling party endpoint, is required to send them to the PD-FE, and is required to request the address binding information if a far end NAT traversal is needed.

2) Upon the receipt of source/destination network address and port and related information from the SCF, the PD-FE is required to check NAPT policy rules to decide the NAPT control procedure, e.g., whether network address hiding is required or not (e.g., between access and core networks).

3) If the NAPT is required at the border between an access and core network, the PD-FE is required to locate the PE-FE based on the network address from the SCF and is required to obtain the local network address/port and public network address/port of the selected PE-FE. If the destination endpoint is in another operator's domain, the PD-FE is required to obtain the public network address and port number from the public network address pool of this operator's network.

4) The PD-FE is required to generate the address binding information of the selected PE-FE for the requested media flows, and may store the address binding information if the PD-FE is stateful. The PD-FE is required to return the network address binding information to the SCF.

5) Upon receipt of the RACF response, the SCF is required to modify the addresses and/or ports contained in the application signalling message body based on the public address information and NAPT policy decision provided by RACF, and may store the address binding information if the SCF uses a stateful proxy.

10.2.1.2 Upon receipt of a session initiation response

1) The SCF is required to extract the source and destination network addresses and port numbers from the signalling message body received from the called party, and is required to send them to the PD-FE.

2) Upon the receipt of source/destination network address and port and related information from the SCF, the PD-FE is required to check the NAPT policy rules to decide the NAPT control procedure, e.g., whether network address hiding is required or not (e.g., between core networks).

3) If the NAPT is required at the border between core networks, the PD-FE is required to locate the PE-FE based on the network address information received from the SCF and obtain a local network address/port and a public network address/port of selected PE-FE.

4) The PD-FE is required to generate the network address binding information of the selected PE-FE for the requested media flows, and may store the address binding information if the PD-FE is a stateful functional entity. The PD-FE is required to return the network address binding information to the SCF. In the originating network, the PD-FE is required to return the public network address binding information of selected PE-FE to the SCF. In the terminating network, the PD-FE is required to return the network address binding information of selected PE-FE to the SCF.

5) Upon receipt of NAPT information from the PD-FE, the SCF is required to modify the addresses and/or ports contained in the application signalling message body based on the address information and NAPT policy decision provided by RACF, and may store the address binding information if the SCF uses a stateful proxy.

10.2.1.3 Upon receipt of a media connection change request for an established session

The SCF is required to decide the possible change of media connection based on the recorded network address binding information if SCF uses a stateful proxy, and/or request the PD-FE to make a decision and perform the appropriate NAPT control procedure. The possible scenarios include:

1) New network address(es) and/or port number(s) have been added: additional binding(s) is required to be provided by the SCF/RACF as detailed for the aforementioned procedures;
2) Existing network address(es) and/or port number(s) have been eliminated: the relevant binding(s) is required to be released by the SCF/RACF;
3) Network address(es) and port number(s) have been re-committed to the users: the binding(s) is required to reflect the re-allocation;
4) No change has been made to the network address(es) and port number(s): no operation is required upon the existing binding(s).

10.2.1.4 Upon receipt of a session release request

1) The SCF is required to request the RACF to release the bindings established for the session.

10.2.2 NAT traversal procedure

This clause describes the procedure for controlling the traversal of a far-end NAT for both signalling flows and media flows at the border between the access and core network. The SCF, PD-FE, TRC-FEs and PE-FEs are involved in performing the IP address and/or port translation in accordance with the procedure.

10.2.2.1 NAT traversal procedure for signalling flows

In order to support the NAT traversal procedure for signalling flows, the SCF is required to return the application signalling packets to CPE on the same address and port number from which the signalling packets were sent.

The relevant operations are required to be performed in the following stages as illustrated in Figure 34:

Registration:

1) When the SCF receive a registration request, it is required to store the network address and port number information of the calling CPE in the registration message (e.g., contact header in SIP registration).
2) The SCF may request a registration interval shorter than the keep alive time for the gate in the far-end NAT.

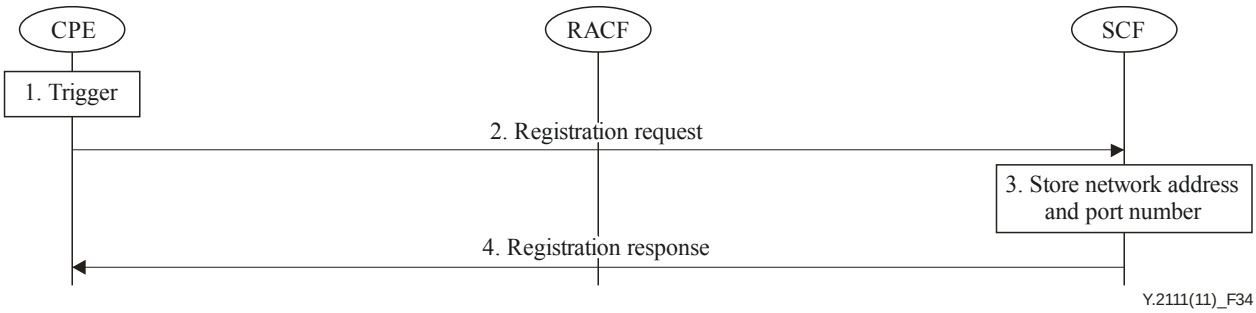


Figure 34 – NAT traversal procedure for signalling registration flows

Session setup process as illustrated in Figure 35:

1) When a session setup request signalling message is received, the pertinent instance of SCF is required to request the RACF to obtain public network address and port number, and is required to replace the network address and port number (e.g., contact header in SDP) of the originating endpoint with the requested network address and port number.

2) When a session setup response is received, the pertinent instance of SCF is required to modify the network address and port number field of the calling CPE in the message body and replace it by CPE's original network address information, and forward the modified message to the CPE.

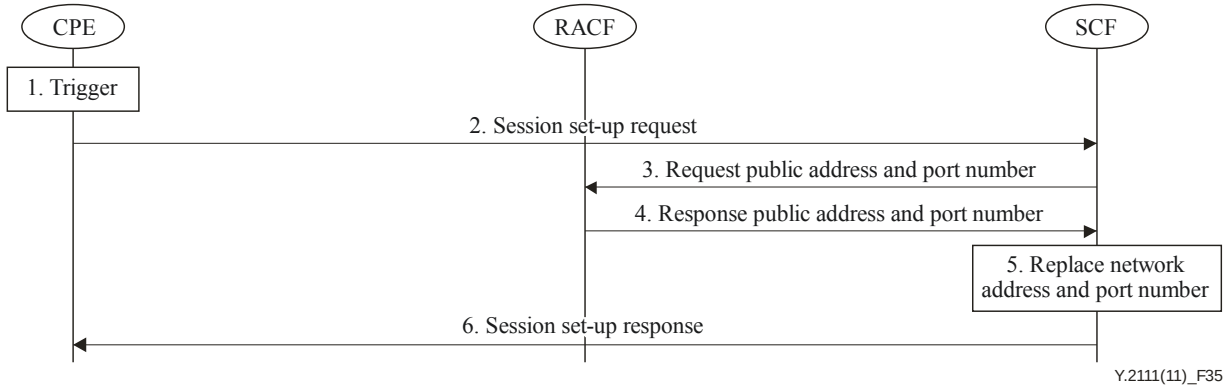


Figure 35 – NAT traversal procedure for signalling session setup flows

10.2.2.2 NAT traversal procedure for media flows

The NAT traversal procedure for media flows is similar to NAPT control procedure between access and core networks as described in clause 10.2.1. However, the NAT traversal procedure is required to be invoked by the SCF based on access network and/or CPN configurations, rather than by the PD-FE based on network security policy rules. The PE-FE is required to serve as an anchor point in support of the media relay function to forward the media flows behind the far-end NAT. For certain applications, both media packets and accompanying media control packets are required to be controlled by the same procedure (e.g., RTP and RTCP for VoIP).

10.2.2.3 Correlation between QoS control and NAT traversal procedures for media flows

When the far-end NAT is deployed in the CPN, the end user IP addresses are not required to be used directly as the source and destination addresses in the QoS control procedure involving RACF-related entities (e.g., SCF, PD-FE, TRC-FE, and PE-FE). Instead, the public source and destination addresses of the involved media flow received by the PE-FEs in the media path are required to be used.

11 Security considerations and requirements

This clause describes security threats and potential attacks and defines security requirements for RACF. The security requirements are based on [b-ITU-T Y.2701]. These considerations are relevant only insofar as the reference points are concerned; the internal security of each RACF is controlled by the security policy rules set forth by the owner of a specific network.

11.1 Overview of threats and potential attacks

The taxonomy of generic threats and their applicability to RACF are as follows:

Destruction of information: This threat refers to the deletion of information pertaining to RACF operations, such as transaction state information, resource usage information, accounting information, topology information, or policy rules. An example of potential consequences is that,

when the information about the existence (or availability) of a particular resource has been destroyed, the resource effectively becomes unavailable. (This is one aspect of the interruption or denial of services described below.)

Corruption or modification of information: This threat has three aspects:

1) Corruption of the recorded resource information (or policy rules) so that such data are rendered meaningless or unusable. This can result in a total loss of resource information or policy rules, which is in itself a threat to the reliability of the RACF.
2) Undetected modification of the recorded resource information or policy rules so that such data appear to be meaningful. This can result in theft of service, degradation of service, loss of service, or fraudulent accounting, or any combination of the above.
3) Corruption or modification of a signalling message, with the same results as the above.

Theft, removal, or loss of information: This threat refers to the theft or loss of recorded resource information. It may result in 1) violation of a subscriber's privacy (in case of theft of subscriber information), 2) theft of service, and 3) degradation, interruption, and, ultimately, unavailability of service (in case of the loss of information).

Theft-of-service attacks can be achieved through repudiation, that is, the denial that a certain transaction has taken place.

Disclosure of information: This can take place because of the interception of the signalling messages or because of granting access to an illegitimate user. The consequence is the same as in the case of theft, removal, or loss of information.

Interruption of services: This threat is typically realized through a denial of service (DoS) attack. Such attacks can make the RACF partially or totally unavailable. Specifically, the resources (including the computing power) can be exhausted by forcing it to process too many requests, or by authorization of illegitimate requests. A few known DoS attacks involve:

1) Replaying the resource request (or response) messages
2) Injection or modification of the resource request (or response) messages; and
3) flooding, where an adversary sends a large number of resource requests. The processing of such requests may exhaust the resources, rendering them unavailable for QoS requests from the legitimate users.

A number of well-known security mechanisms have been either proven or deemed appropriate for mutual authentication and provision of integrity and confidentiality. Transport layer security (TLS) [b-IETF RFC 2246]and IPsec [b-IETF RFC 4301], [b-IETF RFC 2403], [b-IETF RFC 2404], [b-IETF RFC 2405], [b-IETF RFC 4304], [b-IETF RFC 4305], [b-IETF RFC 4307], [b-IETF RFC 4308], [b-IETF RFC 2410], and [b-IETF RFC 2412] protocols already employ such mechanisms for provision of the transport and network layer security, respectively. Various aspects of the use of these protocols are also described in [b-ITU-T Y.2701]. In addition, networks can employ back-end authentication, authorization, and accounting (AAA) servers, which keep the information necessary for these functions.

DoS attacks, however, cannot be prevented. They can only be mitigated.

11.2 Security requirements

The major security requirements for RACF are:

1) Protection of the signalling exchange in support of resource requests.
2) Protection of the information contained in all RACF entities involved in this exchange.
3) Ensuring the availability and overall expected performance of the RACF.

4) Prevention of illegitimate access to the RACF.

- The RACF is required to take the threats identified in clause 11.1 into account, and is required to include measures to counter relevant attacks.
- In particular, mechanisms are required to be explicitly defined for mitigation of the flooding attack. Even in the presence of a DoS attack, the RACF is required to retain its availability.
- Any two entities located in different trust environments (e.g., PD-FE and SCF) are required to authenticate each other before a security association is established. This requires special treatment in support of redundancy (which may, in turn, be needed to ensure reliability or performance or both). If the service of the RACF or any of its components is replicated, an entity that communicates with any such replica is required to use the same authentication information. With that, an eavesdropper is required to be unable to repeat a recorded authentication handshake with another replica.
- During the association, all messages are required to be protected against insertion, deletion, or replay.
- Depending on a specific reference point, the confidentiality protection of the messages may be left optional; however, the integrity of all messages is required to be protected. The decisions are recommended to be made for specific reference points, and they are recommended to leave open a choice of standard cryptographic algorithms to be used in support of confidentiality or integrity.
- Non-repudiation is required to be supported for all requests (unless specifically overridden by a PD-FE policy rule in effect).
- A reference point between un-trusted domains is recommended to make use of commonly used firewall functions.
- Except for the DoS flooding attack, which is systemic, the above requirements are required to be implemented using existing secure-channel mechanisms such as TLS or IPsec (or both) to ensure that well-tested security mechanisms are used.

Annex A

Resource control mechanisms and scenarios for RACF and MPM communication

(This annex forms an integral part of this Recommendation.)

The performance notification between the PD-FE in the RACF and performance measurement reporting functional entity (PMR-FE) in the MPM is illustrated in Figure A.1.

The MPM processes the performance information notification as follows with the RACF:

– CPE-A sends a request to the SCF to establish a session or sessions with CPE-B.

– The RACF receives the service resource request along with other relevant information of the incoming and/or the existing session(s) from the SCF via the Rs reference point in the RACF and passes this information to the MPM over the Rm reference point in the RACF.

– The PMR-FE receives the information of the targeted session(s), and prepares itself for the authenticating requests for the initiation of measurements via the Mu reference point in the MPM. The PMR-FE requests the availability of measurements to the performance measurement execution functional entity (PME-FE) via the performance measurement processing functional entity (PMP-FE) and receives responses from the PME-FE.

– The PMP-FE identifies the targeted session(s) and prepares for the measurement report collection, passive measurement report analysis, measurement data aggregation, and rollup period analysis based on the requests of the RACF.

– The PME-FE recognizes the IP address(es) and sessions information of the incoming and/or the existing session(s) based on the information provided by the PMP-FE. Then, the PME-FE observes the targeted session(s).

– The PMR-FE periodically receives notifications of the performance information measured by the PME-FE and replies with responses to the PME-FE.

– After the analysis of the performance results measured in the PMP-FE, the performance information report is generated in the PMR-FE and periodically sent to the RACF over the Mu reference point in the MPM.

– The report sent to the RACF includes the monitored network resource performance information. Based on the network performance information, the RACF decides whether it needs to adjust the resources allocated to the user. If needed, there are two options as follows:

  Option 1:

  The RACF makes the new policy rules based on the current network performance information, network availability and user subscription information, and then sends them to the PE-FE for enforcement. Also, the RACF informs the SCF that the resources allocated to the user have been modified.

  Option 2:

  The RACF informs the SCF that a user's network resource has been degraded. Then the SCF sends the resource modification request to the RACF with new QoS requirement parameters for resource admission control. The RACF makes the new policy rules based on the new QoS requirement parameters, current network performance information, network availability and user subscription information, and then sends them to the PE-FE for enforcement.

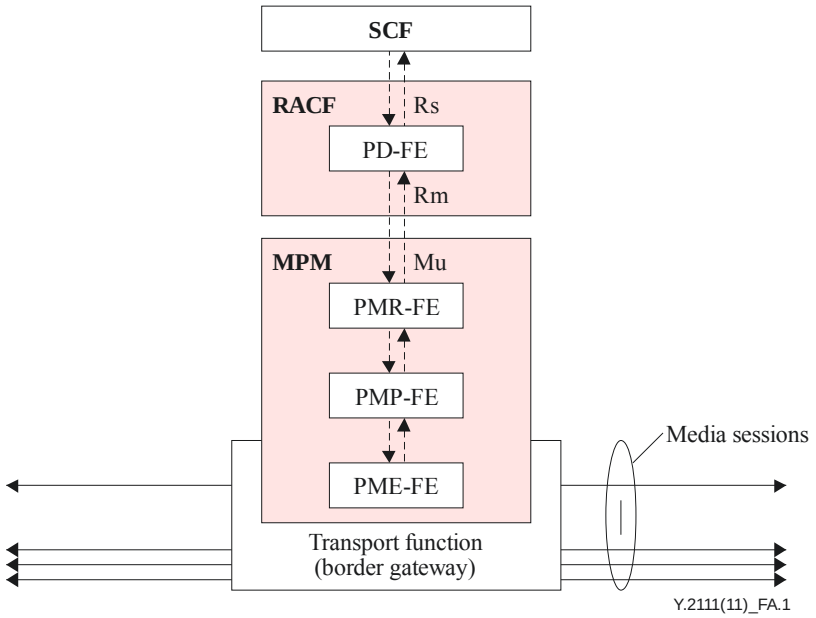


Figure A.1 – Resource control mechanisms and scenarios for RACF and MPM communication

Figure A.2 below depicts the general procedures for the management of inter-domain performance measurement systems. The measurement point (MP) is a functional entity located in the transport, transport control, or service control networks. In the case of active measurement, it is responsible for initiating and receiving probe packets. In the case of passive measurement, it is responsible for capturing target packets. The MPM functions include the interaction with a measurement application (e.g., RACF) and the MPs, the configuration of MPs, and exchanging the required configuration and measured information. The following procedures are described based on such capabilities.

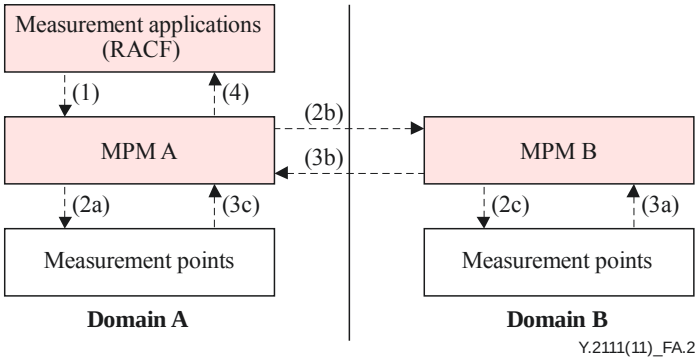


Figure A.2 – Generic inter-domain management process

1) The measurement application (e.g., RACF) of domain A initiates a measurement task by sending a measurement request to the MPM.

2a) Upon receipt of the measurement request, MPM A locates the involved MPs. For the MPs located in domain A, MPM A sends the measurement parameters to the MPs.

2b) Upon receipt of the measurement request, MPM A locates the involved MPs. For the MPs located in domain B, MPM A sends the measurement request to MPM B.

2c) Upon receipt of the measurement request, MPM B locates the involved MPs. For the MPs located in domain B, MPM B sends the measurement parameters to the MPs.

3a) MPM B collects the measured data from the MPs located in domain B.

3b) MPM B sends the measurement information to MPM A.

3c) MPM A collects the measured data from the MPs located in domain A.

4) Based on the received measurement information from domain A and domain B, MPM A sends the response to the measurement applications (e.g., RACF).

Annex B

RACF enhancement for supporting policy-based charging control

(This annex forms an integral part of this Recommendation.)

B.1 Overview of enhancements

Figure B.1 shows the changes made from the functional architecture in [ITU-T Y.2233]. A description of the changes is given below:

1) Extension of the PE-FE to interact with a charging triggering function (CTF) which resides in the transport stratum for transport related charging. This amends clause 8.2.6.1 as described in B.2.2.

2) Extension of the PD-FE to interact with the CTF which resides in the NGN service stratum for contents and service transaction charging. This amends clause 8.2.5.2 as described in B.2.3.

3) Extension of the PD-FE to support both the push-mode and pull-mode of policy-based charging control. This amends clause 8.2.5.2 as described in B.2.3.

4) Creation of a new reference point Ce to support information exchange between the PD-FE and the CTF. This reference point is used to carry a resource control request from the CTF to the PE-FE. This type of control requires real-time execution and direct interaction between the CTF and the PE-FE to avoid unnecessary timing overhead, compared to the case where the decision process has to go through a CTF to the PD-FE and then the PE-FE. This amends clause 9 by adding a new clause for Ce as described in B.3.1.

5) Creation of a new reference point Rr to support information exchange between the PD-FE and the service user profile functional entity (SUP-FE) in the service stratum. This amends clause 9 by adding a new clause Rr as described in B.3.2.

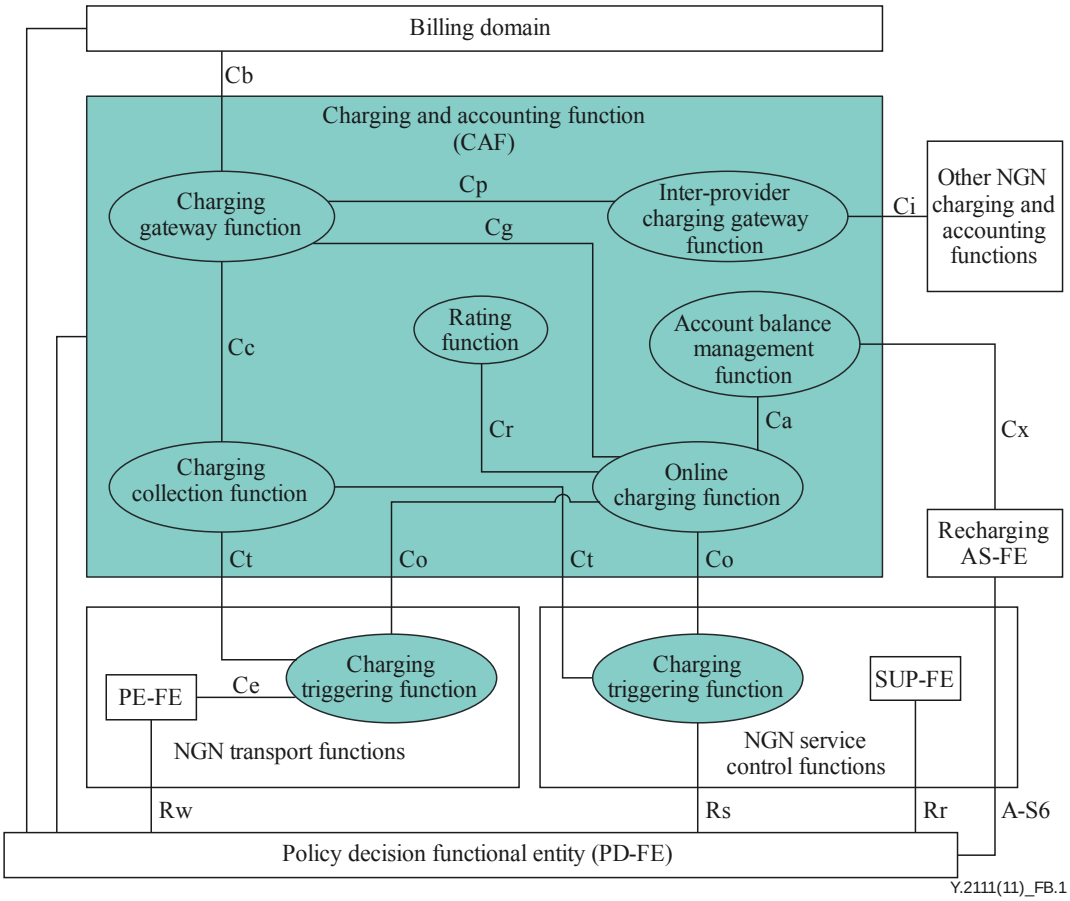


Figure B.1 – Functional architecture supporting policy-based charging and accounting

B.2 Functional architecture

This clause defines the specifics for policy-based charging control.

B.2.1 Charging triggering function (CTF)

Clause 7.1 of [ITU-T Y.2233] specifies the CTF. This annex defines the reference point between the CTF and the PD-FE to allow the former to trigger policy-based charging control.

B.2.2 Policy enforcement functional entity (PE-FE)

The PE-FE supports the following additional functions:

- Traffic policing and shaping based on the resource control request received by the CTF.
- 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 a packet-filtering-based firewall:

  – Static packet filtering: inspecting packet header information and dropping packets based on static security policy rules or the resource control request received by the CTF. 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, dynamic gate status, and/or the resource control request received by the CTF.

  – Delivering charging policies and rules received from the PD-FE to the CTF via the Ce reference point.

B.2.3 Policy decision functional entity (PD-FE)

The PD-FE supports the following additional function:

- Charging policy management: This function interacts with the charging policy repository to retrieve charging policies and rules and transfer them to the PE-FE. How such policies and rules are created and stored are not within the scope of this function. Assumption is given that such policies and rules are managed by billing systems.

B.3 Functional architecture

B.3.1 Reference point Ce

The Ce reference point allows interactions between the CTF and the PE-FE. It shall be able to support the exchange of the following information:

- Charging policies and rules from the PE-FE to the CTF.
- Resource control requests from the CTF to the PE-FE.
- Acknowledgements for these events between the CTF and the PE-FE.

This reference point is required to support the following capabilities:

- Real-time transactions.
- Stateless mode ("event based charging") and stateful mode ("session based charging") of operation.
- Reliable and secure transport based on the protocol requirements in clause 7.3 of [ITU-T Y.2233].

This reference point may support the following capability:

- One-to-many and many-to-one operation modes.

The Ce reference point is an intra-domain reference point.

The detailed information components contained in the relevant events are not within the scope of this annex.

B.3.2 Reference point Rr

The Rr reference point allows interactions between the PD-FE and the SUP-FE.

The Rr reference point is an intra-domain reference point.

The detailed information components contained in the service user profile and policy information exchanged between the SUP-FE and the PD-FE are not within the scope of this annex.

Appendix I

Examples of the implementation of the RACF architecture

(This appendix does not form an integral part of this Recommendation.)

This appendix provides examples of RACF architecture implementation.

From the viewpoint of the end-to-end association between functional entities of RACF, there are different approaches for QoS control. One is the approach in which the RACF performs the QoS control with the intermediation of the SCF (Example 1). Another is the approach in which the RACF performs the QoS coordination at the RACF level without the intermediation of the SCF (Example 2). There is also a specific case where both access and core networks are managed by the same operator (Example 3). The implementation and physical configuration of the PE-FE in transport functions is flexible, and outside the scope of this appendix.

Example 1 (Figure I.1)

Access networks and core networks are in separate administrative domains. The SCF communicates with and controls both PD-FEs in access and core networks via Rs reference points. There is no information exchange between the two PD-FEs in the access and core networks. QoS coordination is performed at the SCF level.

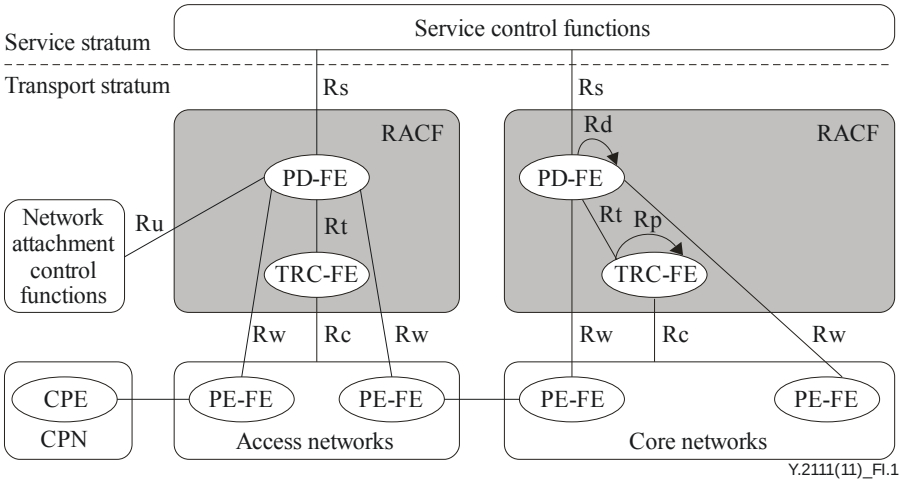


Figure I.1 – Example 1

Example 2 (Figure I.2)

Access networks and core networks are in separate administrative domains. There is no information exchange between the SCF and PD-FEs in the access networks, and SCF communicates with the PD-FE only via the PD-FE in core networks. The PD-FEs in access and core networks communicate via the Ri reference point. QoS coordination is performed at the RACF level.

NOTE – The details of the Ri reference point are for further study.

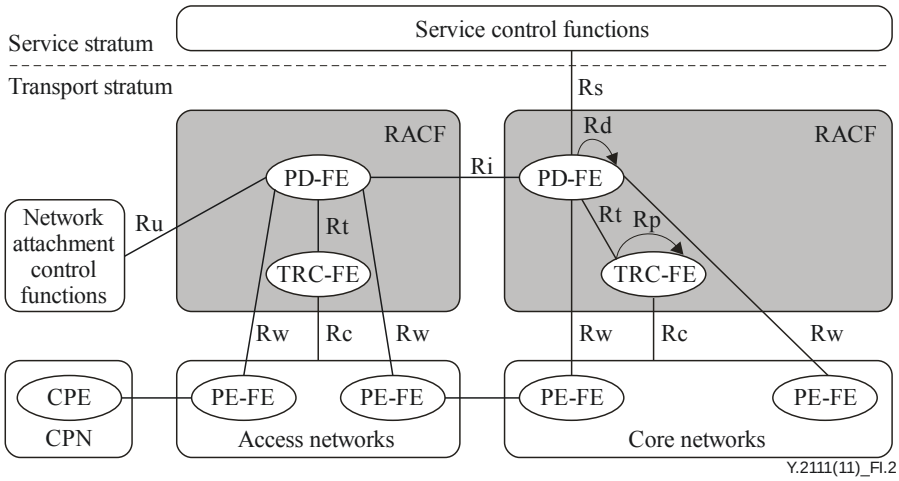


Figure I.2 – Example 2

Example 3 (Figure I.3)

This example describes a specific case where access and core networks are managed by the same operator (access networks and core networks are in a single administrative domain). The PD-FE communicates with and controls both TRC-FEs in access and core networks, and the PD-FE controls both PE-FEs in access and core networks.

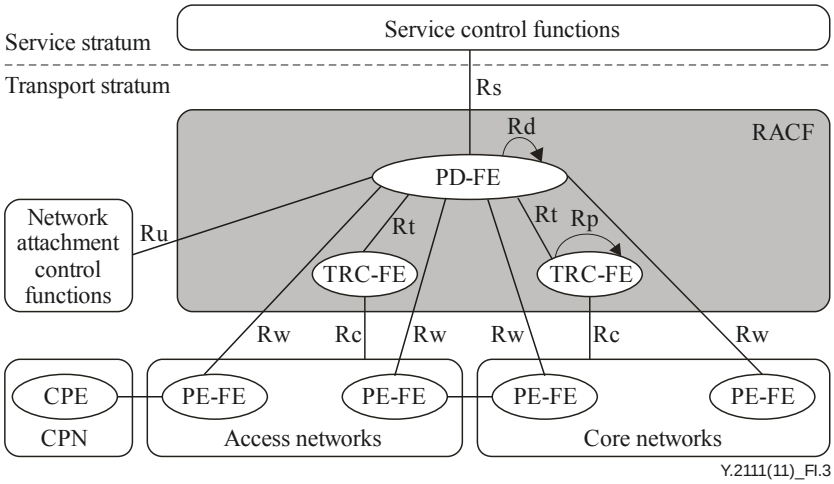


Figure I.3 – Example 3

Appendix II

TRC-FE over different transport technologies

(This appendix does not form an integral part of this Recommendation.)

This appendix describes examples of TRC-FE implementation over different transport technologies, including IP, MPLS, Ethernet and broadband wireless.

II.1 The TRC-FE over an IP network

In an IP network without MPLS support, most nodes can only handle packets in the conventional IP routing way. Routing and forwarding of all traffic is under the control of conventional IP routing protocols and IP Diffserv [b-IETF RFC 2475]. If TRC-FE is implemented, the admission control and resource allocation are dynamically applied with the link-by-link resource reservation.

One or multiple TRC-FE instances are deployed to directly manage all of the physical link resources within an administrative domain. A TRC-FE instance holds and maintains a network topology and resource database (NTRD) of a sub-domain or area within its purview. Based on the information in the NTRD, the TRC-FE instance handles route look-up, link-by-link resource allocation and admission control for each media flow that requires a QoS guarantee. If a media flow is admitted with high priority, it will not interfere with other traffic. If multiple TRC-FE instances are deployed in a domain, they interact with each other through the Rp reference point.

II.2 The TRC-FE over an MPLS network

In a packet network with MPLS support, most nodes can handle packets in the label switching way. LSP technology is used to pre-provision a virtual MPLS transport network (VMTN) for each service type over the underlying packet network infrastructure, either manually or automatically through RSVP-TE or CR-LDP. (Diffserv-aware) MPLS TE [b-IETF RFC 2702], [b-IETF RFC 3272], [b-IETF RFC 3346], [b-IETF RFC 3564] and [b-IETF RFC 4124] can be applied for optimizing network performance. The topology planning and bandwidth reservation of a VMTN depends on the traffic metering and forecasting, network policy rules, and SLAs. For purposes of LSP protection, capacity changes and network performance optimization, VMTN can be adjusted automatically or manually in accordance with traffic engineering constraints. The admission control, route selection, resource allocation and label forwarding for the media flows belonging to a service type are dealt within the same one VMTN.

One or multiple TRC-FE instances are deployed to manage the bandwidth resources of each VMTN or all VMTNs within an administrative domain. A TRC-FE instance records and maintains an NTRD separately for each VMTN within its purview. Based on the NTRDs and policy rules, the TRC-FE instance makes intra-domain route selection, resource allocation and admission control for a media flow within its corresponding VMTN. If multiple TRC-FE instances are deployed for one VMTN in a domain, they interact with each other through the Rp reference point.

The QoS route for a media flow specified by the TRC-FE instance is a label stack that represents a concatenated LSP set. The edge router encapsulates the packets with this label stack, which in turn makes the intermediate transit routers forward the packets of a media flow along the specified route with the specified priority.

II.3 The TRC-FE over an Ethernet network

In an Ethernet network, most nodes handle packets in the Ethernet MAC bridging or virtual bridged way. Generally, only edge nodes are IP-capable. The admission control and resource allocation are dynamically applied with the Ethernet link-by-link resource reservation.

One or multiple TRC-FE instances are deployed to directly manage all of the physical link resources within an Ethernet network. A TRC-FE instance holds and maintains a link layer NTRD for the whole network. Based on the information in the NTRD, the TRC-FE instance makes admission control and resource allocation to ensure that sufficient resources are available within the network for the admitted flows. If multiple TRC-FE instances are deployed in a domain, they interact with each other through a protocol for master/standby communication or load balancing.

II.4 The TRC-FE over a broadband wireless network

In a broadband wireless network, mobile nodes handle packets through the wireless MAC protocol. Broadband wireless MAC protocol provides QoS signalling mechanisms such as the connection set-up bandwidth request uplink information. The QoS classes for QoS signalling define four QoS services: unsolicited grant service (UGS) used for constant bit rate (CBR)-like service flows, real-time polling service used for real-time-variable bit rate (VBR)-like service flows, non-real-time polling service used for non-real-time service flows, and best effort service. Efficient queuing policy rules for such different QoS classes can support priority scheduling and dynamic bandwidth allocation.

Therefore, TRC-FE can be applied for the resource control to provide priority scheduling and dynamic bandwidth allocation. TRC-FE manages the access transport resource based on an NTRD. As a result, the admission control and resource allocation are dynamically applied according to each media flow with different QoS requirements.

One or multiple TRC-FE instances are deployed to directly manage the bandwidth resources within an administrative domain. A TRC-FE instance records and maintains a network topology and NTRD for the whole network. Based on the information in the NTRD, the TRC-FE instance realizes admission control and resource allocation to maintain QoS levels and fairness for media flows of different applications, thus achieving high resource utilization. If multiple TRC-FE instances are deployed in a domain, they interact with each other through Rp reference point for master/standby communication or load balancing.

Appendix III

Example of methods for detecting and determining resource availability in the TRC-FE

(This appendix does not form an integral part of this Recommendation.)

This appendix provides high-level descriptions of the example of methods by which TRC-FE may detect and determine whether requested resources are available.

If the accounting-based method is deployed, the TRC-FE checks whether sufficient resources are available in the transport function by comparing the transport function capacity with the bandwidth (or the number of sessions) already assigned. If the transport function has the required resources, the TRC-FE updates the resource status information to include the new application request and returns a positive response to the PD-FE. If the transport function does not have the required resources, the TRC-FE returns a negative response to the PD-FE.

If the out-of-band measurement-based method is deployed, the TRC-FE admits service requests based on resource status information obtained through periodic polling of routers or switches. To handle high-volume service requests, the TRC-FE can compute admission rules based on the most recent resource measurements, and apply these rules when the PD-FE requests a resource availability check. An example of the TRC-FE admission rules is to block a certain fraction of service requests between a pair of PE-FEs. The TRC-FE admission rules are updated based on transport function resource utilization information obtained through out-of-band measurements. Note that in the out-of-band measurement-based method, there is no need to reserve resources per service request. Furthermore, the TRC-FE admission rules can be uploaded to the PD-FE so that the PD-FE can apply the rules locally without consulting the TRC-FE per service request. The rules cached in the PD-FE are updated by the TRC-FE to reflect the changes in the resource usage in the transport function.

If the in-band measurement-based method is deployed, the TRC-FE admits service requests based on network performance information obtained using active probes or other in-band performance measurement mechanisms. The probing can be done when the PD-FE requests a resource availability check or can be done periodically independent of the PD-FE requests. In the latter case, TRC-FE can compute admission rules similar to those suggested for the out-of-band measurement-based method. These rules can be cached in the PD-FE and updated to reflect rule changes. Note that with the in-band measurement-based method, there is no need to reserve resources per service request. Such caching is a challenge to the PD-FE, because there are many TRC-FE instances in access networks and core networks with different transport technologies.

With the reservation-based method, the TRC-FE explicitly requests bandwidth reservation from the transport functions. To handle high-volume service requests, the TRC-FE can compute admission rules based on per-aggregation resource reservation, and apply these rules when the PD-FE requests a resource availability check. Note that per-session resource reservation is inefficient, so per-aggregation resource reservation is applied in a pre-configuration way and can be adjusted based on the resource usage.

The measurement of performance management (MPM) described in [ITU-T Y.2173] can measure and collect in real-time the performance information such as bandwidth as well as other performance attributes like one-way delay, delay variation, and packet loss ratio. If the MPM-based method is deployed, the TRC-FE admits service requests based on performance information obtained by the MPM. The information can be collected when the PD-FE requests a resource availability check or can be done periodically independent of the PD-FE requests. In the latter case, the TRC-FE can compute admission rules similar to those suggested for the out-of-band measurement-based method. These rules can be cached in the PD-FE and updated to reflect rule changes. Note the requirement for resource reservation per service requests and other details on how to interact with the MPM is for further study.

Appendix IV

Examples of admission control procedures for unicast and multicast

(This appendix does not form an integral part of this Recommendation.)

IV.1 Examples of admission control procedures for unicast and multicast

When the CPE requests multicast service (e.g., broadcast TV) to transport functions via transport-level signalling (e.g., IGMP, MLD) while requesting unicast service (e.g., video on demand or bandwidth on demand) to SCF via service-level signalling, in order to accommodate the performance requirement (e.g., channel zapping), the MTCF, MRF and a local TRC-FE instance co-locate in the same physical node for admission control.

Figure IV.1 illustrates the reference architecture:

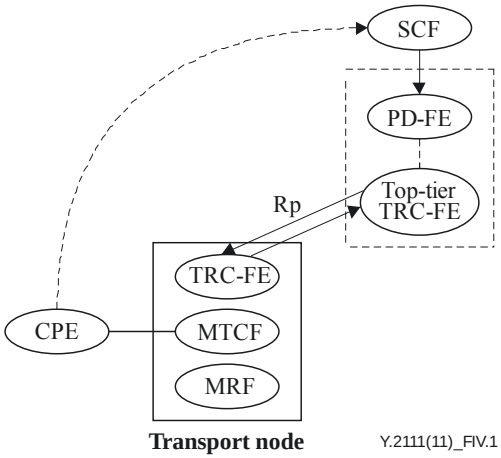


Figure IV.1 – Reference architecture for unicast and multicast admission control

In this scenario, all multicast flows reach the access node. The MTCF is located within the transport node (i.e., access node). The resource admission decision is made based on the resources of the access loop. The MTCF processes a multicast request (e.g., IGMP or MLD), parses the message and sends the trigger for resource admission to the co-located TRC-FE. The co-located TRC-FE is responsible for the resource admission control for a pertinent network segment (e.g., access network) and makes the resource decision based on resource availability. The top-tier TRC-FE is responsible for overall resource admission control across multiple network segments through the interaction with the co-located TRC-FE. The interaction between the top-tier TRC-FE and the co-located TRC-FE through the Rp reference point operates in either the outsourcing or designating mode, dependent on resource admission control approaches deployed in the network.

IV.1.1 Admission control for fully shared resources between unicast and multicast

In this case, the resources are fully shared by unicast and multicast services in a specific network segment, a co-located TRC-FE in the transport node is responsible for resource admission control for both unicast and multicast services over that network segment.

For multicast services, the co-located TRC-FE makes the final decision to authorize the multicast resource request from the MTCF immediately without interaction with the top-tier TRC-FE. For unicast services, the top-tier TRC-FE is required to query the co-located TRC-FE for resource availability and make a final decision based on the result of resource admission control in the co-located TRC-FE, i.e., the outsourcing mode is used for this case.

Scenario 1

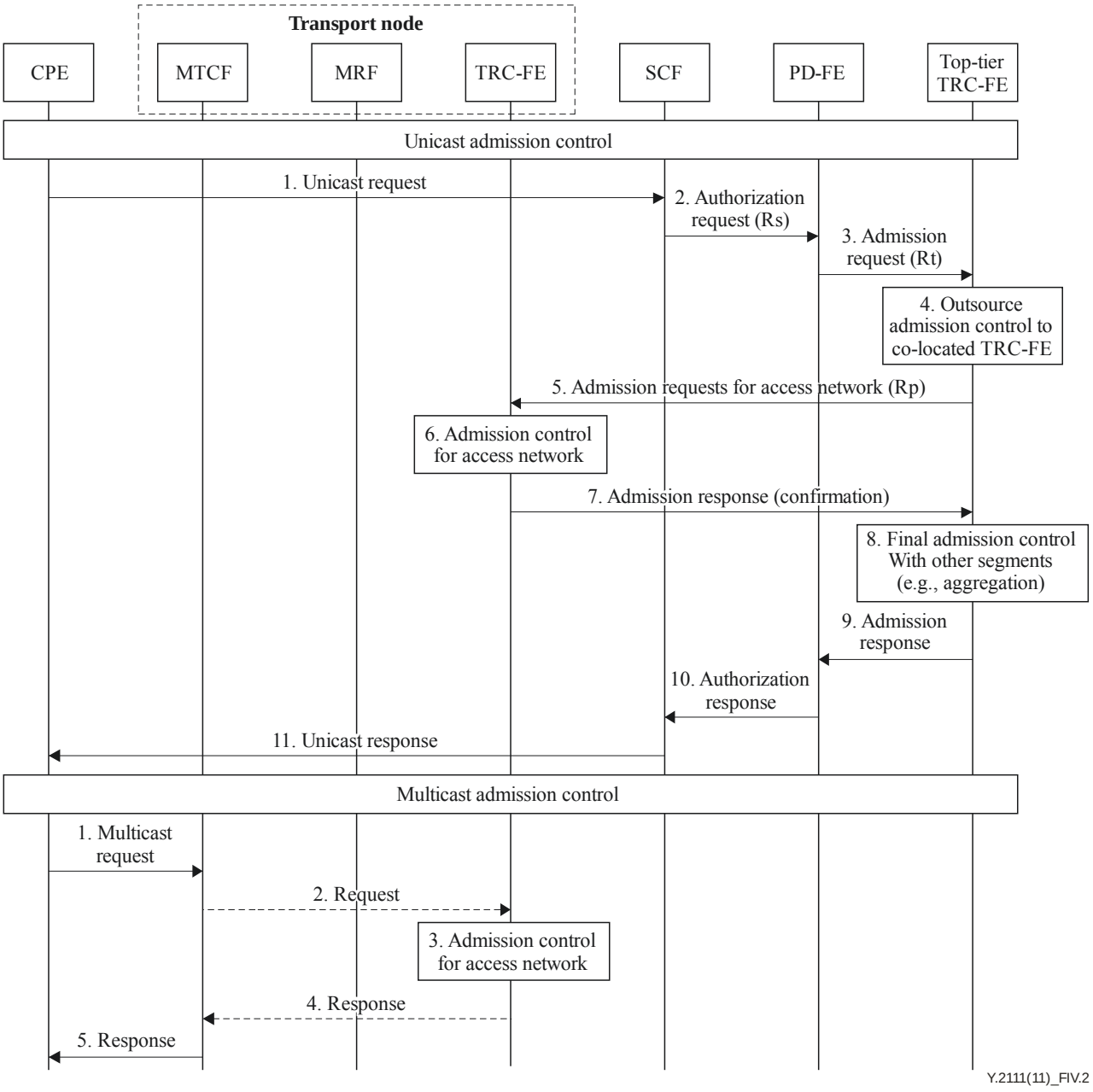


Figure IV.2 – Unicast and multicast admission control for fully shared resources

For unicast services:

1) The CPE sends a request (e.g., SIP Invite) to the SCF.

2) The SCF initiates an authorization request to the PD-FE.

3) The PD-FE performs network policy authorization and sends a resource admission request to the top tier TRC-FE that serves as the single point of contact for resource admission control.

4,5) The top tier TRC-FE identifies specific co-located TRC-FE and forwards the request; meanwhile, top tier TRC-FE performs the resource availability checking in other segments, e.g., aggregate network.

6) The co-located TRC-FE performs resource admission control for the first mile and access node (maybe upstream of the second mile as well).

7) The co-located TRC-FE responds to the top tier TRC-FE with a local admission decision.

8) The top tier TRC-FE makes final resource admission decision based on the result of a local TRC-FE in the access node and a result of resource admission for other segments.

9) The top tier TRC-FE responds to the PD-FE with resource admission decision.

10) The PD-FE may perform other policy control and respond to the SCF.

11) The SCF replies to the CPE or forwards the request to the next hop.

For multicast services:

1) The CPE sends a multicast request (e.g., IGMP join) to an access node.

2) The multicast signalling function in access node processes the multicast message, e.g., IGMP join request, and sends a request to the co-located TRC-FE if the channel is not yet available in the access node associated with the corresponding end-user.

3) The co-located TRC-FE performs resource admission control on multicast resources associated at the first-mile with the corresponding end user and decides if the enforcement operation (e.g., media replication) is required.

4,5) The co-located TRC-FE responds to the MTCF that responds to the CPE or forwards it to the next hop.

Scenario 2

When the share resource approach is deployed, i.e., no dedicated resources are allocated to multicast services and the resources are fully shared by unicast and multicast services in a specific network segment, a co-located TRC-FE in the transport node is responsible for resource admission control for multicast services over that network segment and a top-tier TRC-FE is responsible for resource admission control for unicast services.

For multicast services, the co-located TRC-FE makes resource admission control based on the available resource upon receipt of a multicast request for joining a multicast group (e.g., IGMP). If the available resource is sufficient for the requested resource, the co-located TRC-FE admits the request and reports the resource status information of the specific network segment to the top-tier TRC-FE according to the predefined policies (e.g., after admission or periodically). Upon receipt of the report of resource status, the top-tier TRC-FE makes resource admission decision for unicast services based on the updated resource status information. Note the top-tier TRC-FE maintains the consistency of the resource status information.

For unicast service, the top-tier TRC-FE makes resource admission control based on the available resource. If the available resource is sufficient for the requested resource, the top-tier TRC-FE admits the request and implements the resource policy on the transport node of the specific network segment. The co-located TRC-FE in the transport node updates the resource status information of the specific network segment based on the implemented resource policy.

The granularity of interaction between the top-tier TRC-FE and the co-located TRC-FE can be either at per session level or at aggregate level.

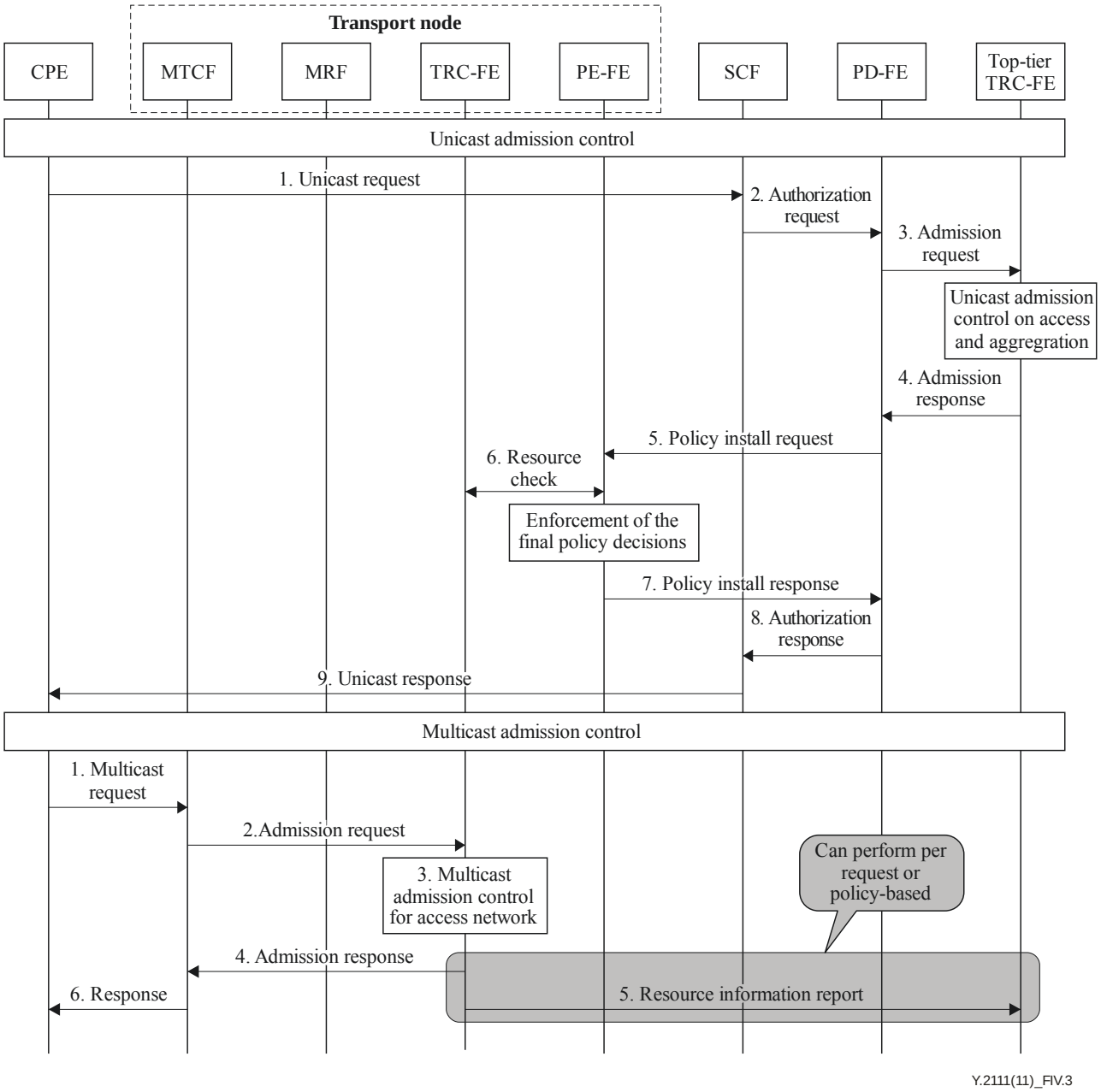


Figure IV.3 – Unicast and multicast admission control for reporting resource

For unicast services:

1) The CPE sends a request (e.g., SIP Invite) to the SCF.

2) The SCF initiates an authorization request to the PD-FE.

3) The PD-FE performs network policy authorization and sends a resource admission request to top-tier TRC-FE that serves as the single point of contact for resource admission control. Top-tier TRC-FE checks the network and subscriber policy against the request and does admission control on both aggregation and access segment.

4) The top-tier TRC-FE sends the response to the PD-FE.

5) The PD-FE sends a policy install request to the PE-FE.

6) The PE-FE informs the resource check of the access line to the co-located TRC-FE to assure if co-located TRC-FE has enough resource for the resource request and accord the resource information with top-tier TRC-FE.

7) The PE-FE enforces the policy decisions and sends the policy install response to the PD-FE.

8) The PD-FE may perform other policy control and respond to the SCF.

9) The SCF sends a unicast response to the CPE.

For multicast services

1) The CPE sends a multicast request (e.g., IGMP join) to an access node.

2) The multicast signalling function in the access node processes the multicast message, e.g., IGMP join request and sends a request to the co-located TRC-FE if the channel is not yet available in the access node associated with the corresponding end-user.

3) The co-located TRC-FE performs resource admission control on multicast resources associated at the first-mile with the corresponding end user and decides if the enforcement operation (e.g., media replication) is required.

4) The co-located TRC-FE sends a resource information report to the top tier TRC-FE to inform the resource usage on access line.

5,6) The co-located TRC-FE responds to the MTCF that responds to the CPE or forwards it to the next hop.

IV.1.2 Admission control for adjustable resources between unicast and multicast

In this case, the dedicated resources are pre-provisioned to unicast and multicast services respectively in a specific network segment, the threshold of aggregate resources are adjustable based on network policy and resource status. A co-located TRC-FE in the transport node is responsible for resource admission control for unicast and multicast services respectively, according to pre-provisioned resource budget and network policy, i.e., designating mode is used.

For multicast services, based on resource availability within pre-provisioned threshold, the co-located TRC-FE makes final decision to authorize the multicast resource request from the MTCF immediately without interaction with top-tier TRC-FE. For unicast services, the top-tier TRC-FE makes a final decision based on resource availability within the pre-provisioned threshold. When the resources reach the threshold, either top-tier TRC-FE can authorize the increase or decrease of the threshold to co-located TRC-FE directly or the co-located TRC-FE can request the increase or decrease of the threshold from top-tier TRC-FE.

For reducing the channel zapping time for broadcast TV service, the co-located TRC-FE, based on the provider policy, admits the request and marks the multicast flow as low priority when the multicast resources reach the threshold. Meanwhile, the co-located TRC-FE requests the top-tier TRC-FE to allocate more resource for multicast service. If the request is admitted by the top-tier TRC-FE, the co-located TRC-FE remarks the admitted multicast flow as the priority corresponding to the requested service; otherwise, the co-located TRC-FE, based on the provider policy, terminates the multicast flow.

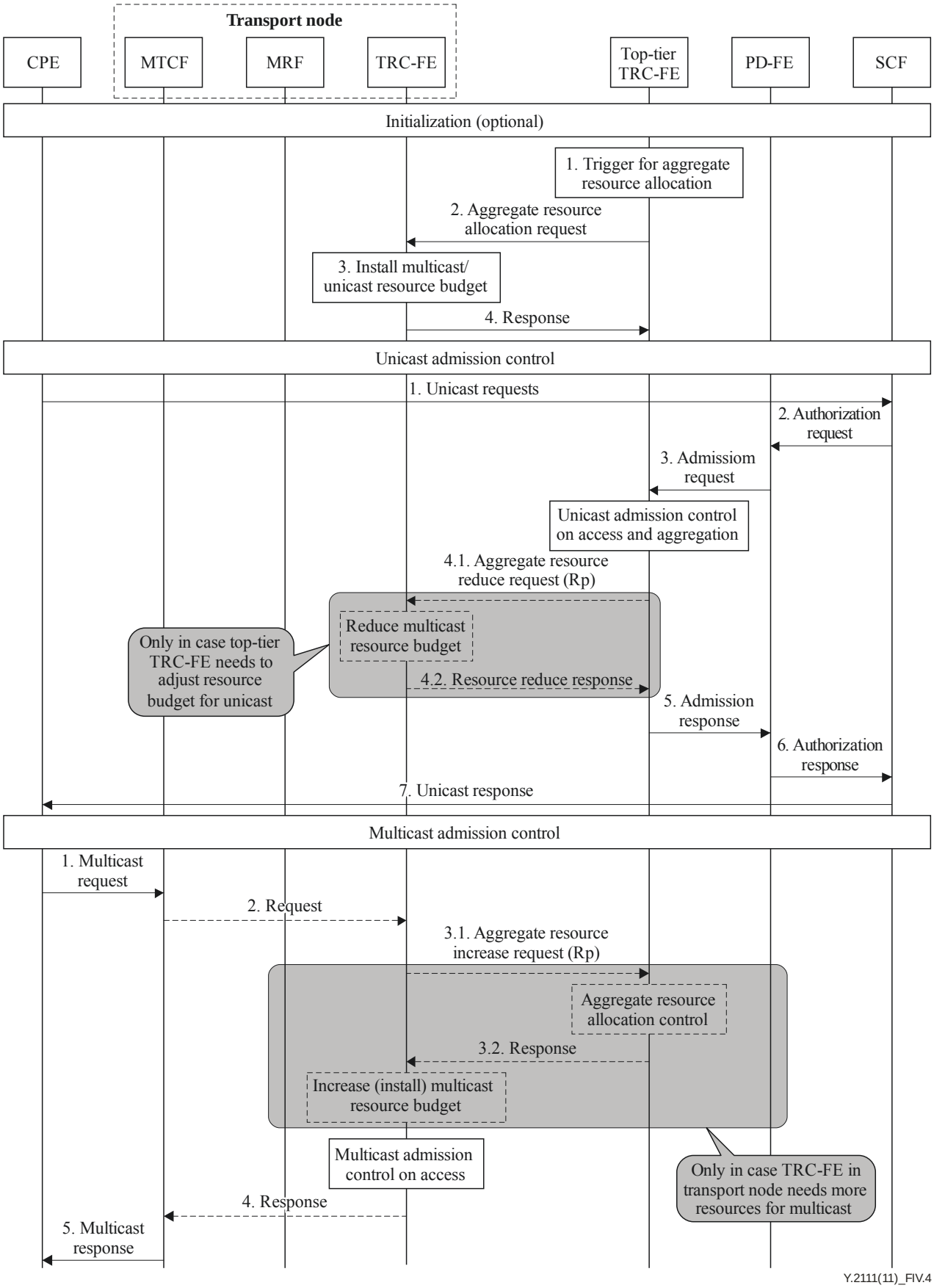


Figure IV.4 – Unicast and multicast admission control for adjustable resources

Initialization (Optional):

1) A trigger occurs towards the top tier TRC-FE for provisioning the aggregate resource budget for multicast and unicast services.

2) The top tier TRC-FE sends the request to the co-located TRC-FE to install the resource budget.

3) The co-located TRC-FE installs the resource budget.

4) The co-located TRC-FE sends a confirmation to the top tier TRC-FE.

For unicast services:

1) The CPE sends a request (e.g., SIP Invite) to the SCF.

2) The SCF initiates an authorization request to the PD-FE.

3) The PD-FE performs network policy authorization and sends a resource admission request to the top tier TRC-FE that serves as the single point of contact for resource admission control. The top tier TRC-FE performs the resource admission control based on pre-provisioned resource budget and resource availability in other segments, e.g., aggregate network;

4.1) In case the top tier TRC-FE needs to adjust the resource budget for unicast services, it sends a resource allocation request to the co-located TRC-FE.

4.2) The co-located TRC-FE performs the resource budget adjustment for the first mile and access node (maybe upstream of the second mile as well) and responds to the top tier TRC-FE.

5) The top tier TRC-FE makes a final resource admission decision based on the result of the co-located TRC-FE in the access node and the result of resource admission for other segments and responds to the PD-FE with a resource admission decision.

6) The PD-FE may perform other policy control and respond to the SCF.

For multicast services:

1) The CPE sends a multicast request (e.g., IGMP join) to an access node.

2) The MTCF in the access node processes the multicast message, e.g., IGMP join request and sends a request to the co-located TRC-FE if the channel is not yet available in the access node associated with the corresponding end-user.

3) The co-located TRC-FE performs resource admission control on multicast resources associated at the first-mile with the corresponding end user and decides if the enforcement operation (e.g., media replication) is required.

3.1) In case the co-located TRC-FE needs to adjust the resource budget for multicast services, it sends a resource allocation request to the top tier TRC-FE.

3.2) The top tier TRC-FE performs the resource budget adjustment and responds to the top tier TRC-FE;

4,5) The co-located TRC-FE responds to the MTCF that responds to the CPE or forwards it to the next hop.

IV.2 Example of multicast resource control scenario

In this scenario, multicast resource control is performed on a bundle of channels basis. Within a bundle, all channels have the same authorization and charging policy. The user sends a service request to IPTV server to access IPTV service. Upon receipt of the request, service provider can request network provider via RACF to activate the policy of the requested bundle of channels on transport node. Then the user can use transport signalling to select channels in the bundle without

triggering the resource authorization and reservation process for each individual TV channel. By this means, it can achieve the goal of fast channel changing.

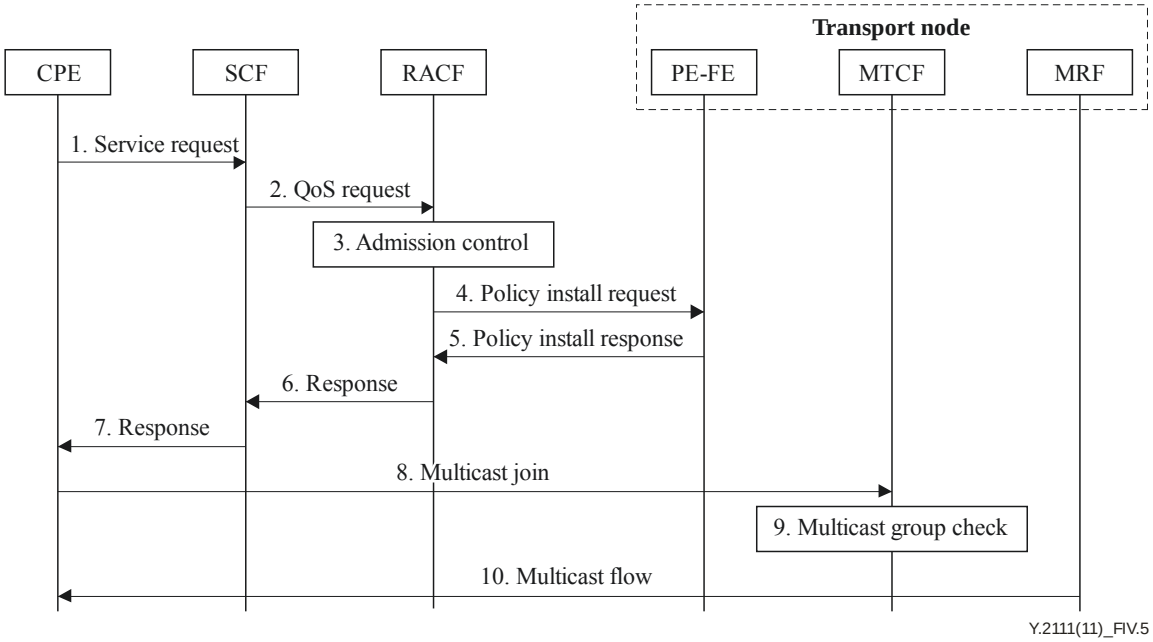


Figure IV.5 – Example of multicast resource control

1) The CPE initiates a service request to the SCF. The request is for a set of channels which have the same QoS requirement, authorization and charging policy. There is an identifier in the request to present the requested bundle.

2) The SCF extracts the QoS requirements for the set of channels from the service request and requests the resource authorization and reservation from the RACF by sending a QoS request to the RACF.

3) The RACF performs authorization and admission control based on policy rules, resource admission decision and transport subscription profile.

4) The RACF sends the policy install request to the PE-FE for the set of channels. The mapping of the bundle and the set of channels may be pre-installed in the PE-FE. In this case, the RACF sends an indicator to activate the bundle instead of installing the policies for each individual channel.

5) The PE-FE sends the policy install response to the RACF.

6) The RACF sends the response to the SCF.

7) The SCF sends the response to the CPE. If it is a positive response, an application session (i.e., application session for IPTV services) is established between the SCF and the CPE.

8) The CPE requests a TV channel by sending transport signalling (e.g., IGMP join) to transport functions (i.e., MTCF).

9) Upon receiving the transport signalling (e.g., IGMP join), the MTCF checks if the requested multicast group belongs to the authorized multicast groups included in the requested service bundle.

10) The MRF replicates the requested multicast flow to the CPE.

Appendix V

The consideration of the CPN gateway control mode

(This appendix does not form an integral part of this Recommendation.)

This appendix provides the structure in which the CPN gateway only has a special policy enforcement functional entity controlled by the RACF at the network side.

V.1 The architecture for CPN gateway control

The structure is illustrated in Figure V.1.

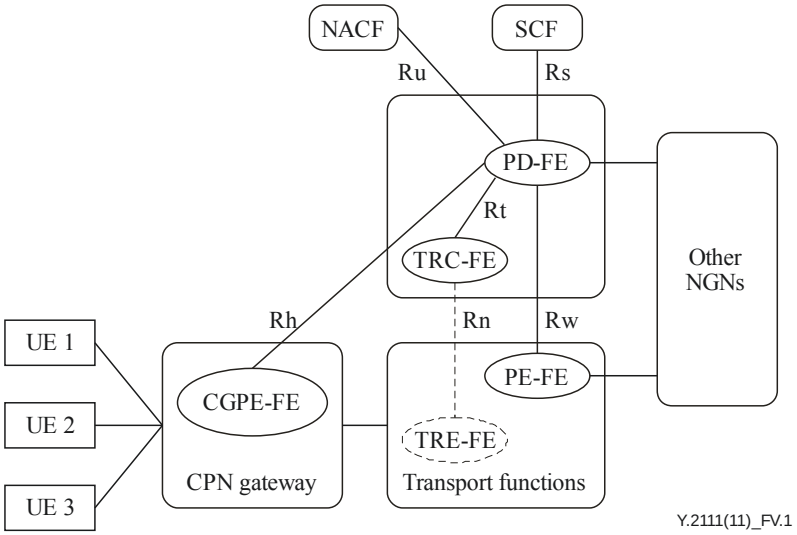


Figure V.1 – Architecture for the CPN gateway

The CGPE-FE is defined in the CPN gateway. The CGPE-FE is a functional entity enforcing the network policy rules instructed by the PD-FE across the Rh reference point.

The Rh reference point allows the PD-FE to push the admission decisions to the CGPE-FE, and also allows the CGPE-FE to request the admission decisions. The PD-FE may specify:

- Resources to be reserved and/or committed for media flows.
- QoS handling such as packet marking and policing to use.
- Gate control (opening/closing) for a media flow.
- Resource usage information request and report for a subscriber.

The CGPE-FE enforces the network policy rules instructed by the PD-FE on a per-subscriber and per-flow basis. It is recommended to 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, ATM VPC/VPI) as needed. The functions of the CGPE-FE include:

- Opening and closing gate: enabling or disabling packet filtering for a 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.
- The 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).

V.2 The procedure of the CPN gateway control mode

In this scenario, the CPN gateway only has a special policy enforcement functional entity (CGPE-FE) controlled by the RACF at the network side. The RACF at the network side is required to support two QoS resource control modes: pull mode and push mode. The pull mode is for further study.

For push mode: the application within CPE/CPN sends a service request to the SCF including resource requirements. The SCF then forwards the request to the RACF. Upon the request of the SCF, the RACF at the network side makes the authorization and resource control decision based on policy rules and autonomously instructs the policy enforcement functional entity in CPN gateway and the PE-FE at the network side to enforce the policy decision.

The QoS resource reservation procedure is illustrated in Figure V.2 that is initiated by a resource initiation request from the SCF.

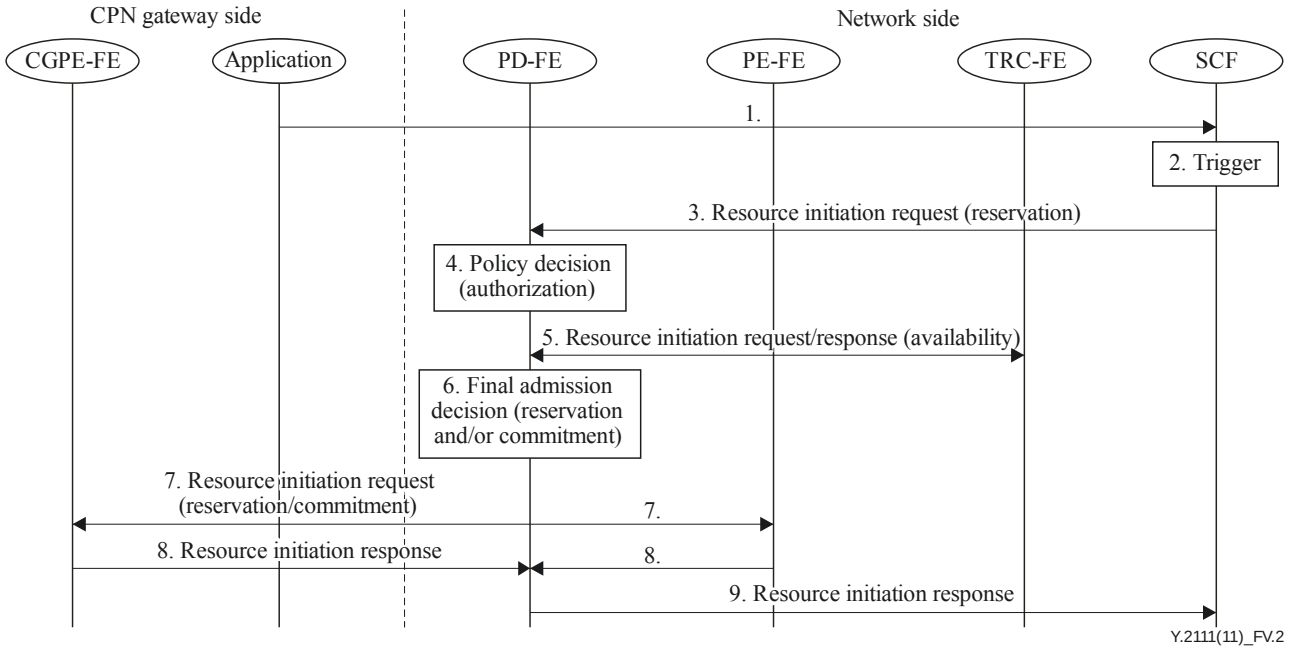


Figure V.2 – QoS reservation procedure in push mode of the CPN gateway

1) The application in the home network requests an application-specific service by sending a service request to the SCF. The service request may or may not contain any explicit (application) service QoS requirements.

2) A resource initiation request (reservation) (i.e., RIR (reservation)) is triggered in the SCF.

3) The SCF determines or derives the QoS requirement parameters (such as bandwidth, class of service) for the media flows of a given service. It then sends an RIR (reservation) with the media flow description and its QoS parameters to the PD-FE at the network side across the Rs reference point for QoS resource authorization and reservation.

4) On receipt of the RIR (reservation), the PD-FE at the network side is required to authorize the required QoS resources for the media flow. The PD-FE checks if the media flow description and the required QoS resources are consistent with network policy rules held in the PD-FE and the transport subscription information held in the NACF.

5) The PD-FE positions and determines which access networks and core networks are involved for the media flow. If there are TRC-FE instances in an involved network, the PD-FE sends an RIR (availability check) to one of the TRC-FE instances registered in the PD-FE to check resource availability in the involved network. If there are multiple TRC-FE instances in the involved network, they communicate with each other to determine if the required QoS resource is available from edge to edge in the involved network. The TRC-FE instance which received the RIR (availability check) is required to send an RIP back to the PD-FE.

6) The PD-FE makes the final admission decisions based on the results of steps (4) and (5). If the media flow is not admitted, the PD-FE sends an RIP with the rejection reason back to the SCF.

7) The PD-FE may send an RIR to install the final admission decisions in the CGPE-FE and the PE-FE.

8) The CGPE-FE and PE-FE install (and enforce) the final admission decisions sent from the PD-FE and send an RIP back to the PD-FE.

9) The PD-FE sends an RIP back to the SCF.

V.3 Example of the implementation of the RACF for CPN gateways

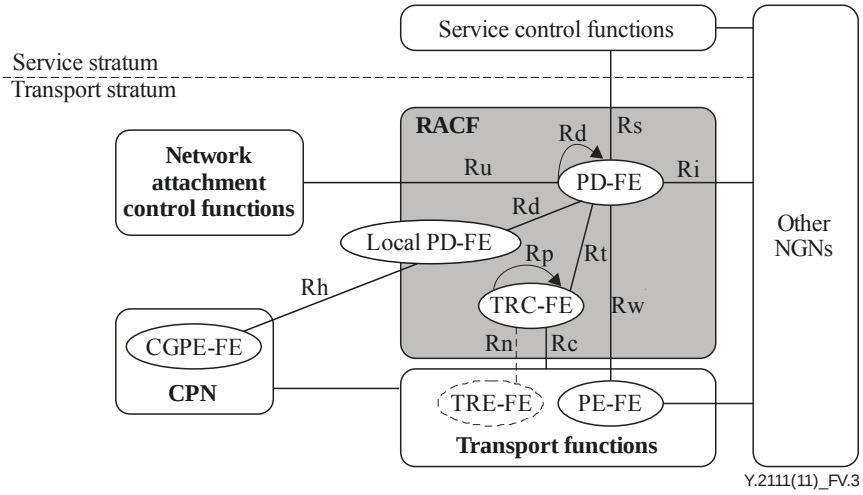


Figure V.3 – Example of the implementation of the RACF for a CPN gateway

Figure V.3 describes an example of implementation of the RACF for a CPN gateway.

The local PD-FE receives the QoS control policy from the PD-FE, and delivers the policy to the involved CPN gateway. Based on the network resource of access link and the policy rules, the local PD-FE makes an admission decision and installs the local policy to the CPN gateway.

The local PD-FE may be implemented in the CPN gateway management server (such as: an extended auto configuration server (ACS) or similar function entity). The ACS is defined in [b-DSL TR 069] and is a component in the broadband network responsible for auto-configuration of the CPN gateway for advanced services.

The local PD-FE performs the following functions:

- Decision point: This function checks the QoS resource request based on service information from the PD-FE, network policy rules and transport subscription information, to detect and determine the requested QoS resource in the CPN and access line.
- Rate limiting control (RLC).
- IP packet marking control (IPMC).
- Gate control (GC).

V.4 CPN gateway control in wholesale mode

In some wholesale scenarios, the user and the CPN gateway belong to the retail service provider (RSP). The CGPE-FE enforces the network policy rules instructed by the PD-FE of the RSP in order to provide services by the RSP.

The Rh reference point allows the PD-FE of the RSP to push the network policy rules to the CGPE-FE, and also allows the CGPE-FE to request admission decisions (Figure V.4).

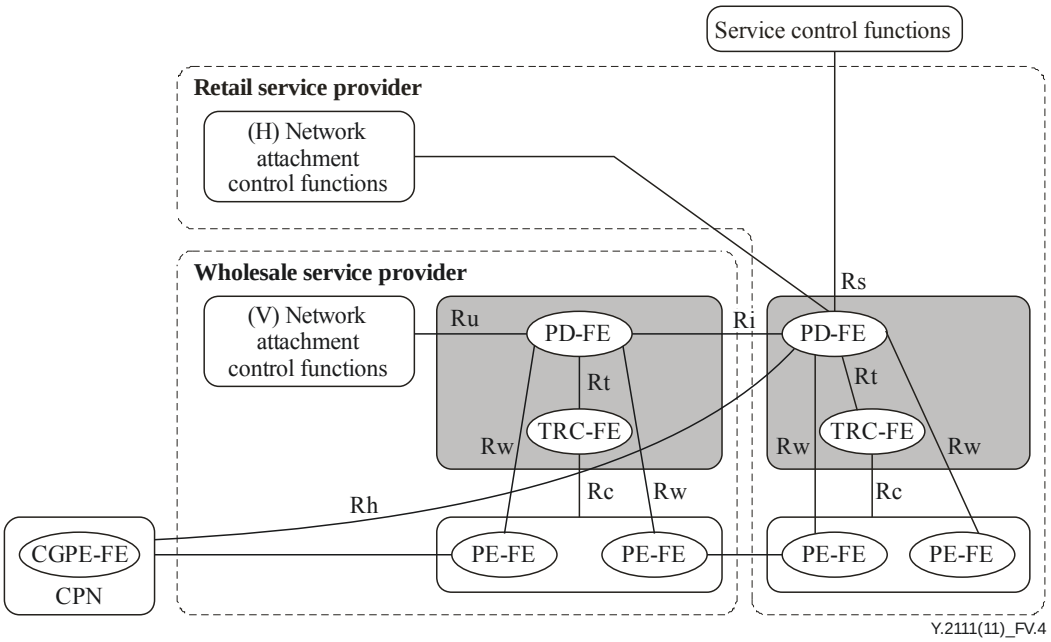


Figure V.4 – Resource and admission control functional architecture for CPN gateway for wholesale

The CGPD-FE has been defined as an admission control functional entity inside the CPN. The PD-FE of the RSP sends the resource initiation request to the CGPD-FE which includes the initial policy decisions. After receiving the request, the CGPD-FE checks the authorization. If successful, the CGPD-FE makes the final admission decisions, and the CGPE-FE enforces the final policy rules.

The Rh' reference point supports the interaction between the CGPD-FE and the PD-FE of the RSP (Figure V.5).

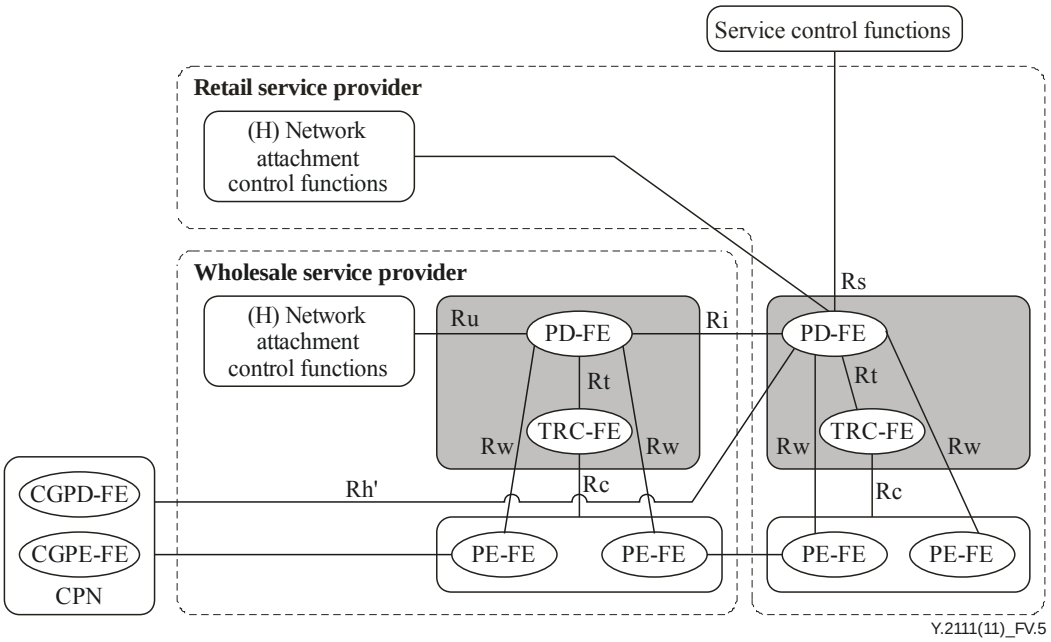


Figure V.5 – Another resource and admission control functional architecture for the CPN gateway for wholesale

Appendix VI

Resource control deployment scenarios for multicast

(This appendix does not form an integral part of this Recommendation.)

Scenario 1: Multicast service control function (MSCF) requested multicast resource control

The multimedia multicast session management service allows for a third party (e.g., application server (AS)) to be provided with multicast presence information via a universal service interface, and to control a multicast session, to manage multicast group membership. The AS plays the role of a service control function (e.g., CSCF). A request for multicast services involves exchange of signalling between the user equipment and the AS. Based on subscriber information and service request information, the AS may initialize resource allocation to the access network to which user equipment is connected. Also, user equipment may exchange with the subscriber access network to facilitate resource allocation. In the access network, access node, edge node, and aggregation nodes in the aggregation network are required to support the transport function. In this deployment scenario, the MSCF is located in the AS while the multicast replication function (MRF) and the multicast transport control function (MTCF) are located in the access node or edge node.

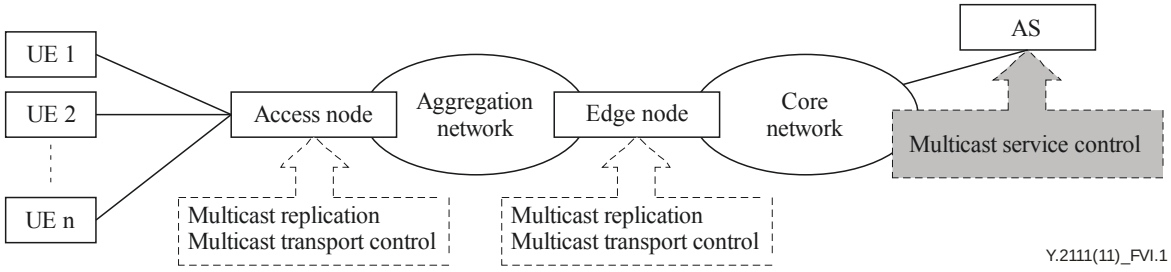


Figure VI.1 – MSCF requested multicast resource control scenario

Scenario 2: Multicast resource control with MTCF requested from the access node

There are scenarios where reception of some video stream programs may be forbidden due to there being no appropriate subscriber privileges. These scenarios may require the network provider to limit the number of streams admitted for a single UE. Admission control is required to be applied on multicast services. Request for multicast services involves exchange of signalling between user equipment and an access node which obtains subscriber privileges from a policy server residing in the edge node. Access node may receive a multicast services request. Based on subscriber privileges, the access node may reject this request or forward it to a multicast router transparently and then allow the media stream to be transferred from the multicast router to the UE. In the access network, access node, edge node, and aggregation nodes in the aggregation network are required to support the transport function. In this deployment scenario, the MRF is located in the access node while the MTCF is also located in the access node.

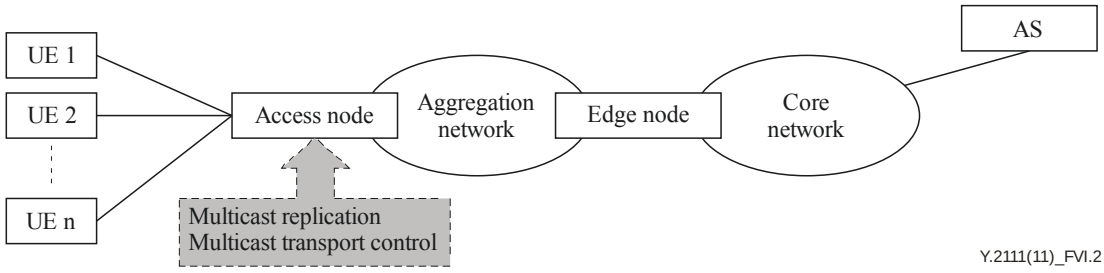


Figure VI.2 – Access node requested multicast resource control scenario

Scenario 3: Multicast resource control with MTCF requested from edge node

The limited bandwidth can only allow a certain number of channels to be carried over the access and aggregation network simultaneously. If the number of multicast channels offered to customers is greater than the number of channels that are carried over the access and aggregation network simultaneously, it usually results in traffic congestion and degradation of QoS. To address this limitation, we can guarantee the resource can be efficiently utilized by the multicast channels with higher channel priority. For this purpose (i.e., channel difference disposal), access nodes may collect user multicast behaviour information including subscriber number, programme item number, start viewing time, stop viewing time, etc., and report them to the edge node. The edge node plays both the role of multicast control function and the role of policy control function and retrieves audience rating statistics information from user multicast behaviour information. Then based on this audience rating statistics information, the edge node can determine channel priority and provision to the access nodes. Thus, the access nodes may apply channel difference disposal based on specific channel priority. In the access network, the access node, edge node, and aggregation nodes in the aggregation network are required to support the transport function. In this deployment scenario, the edge node is required to support the MRF in order to deliver the selected multicast services to the UE, while the MTCF is located in the edge node.

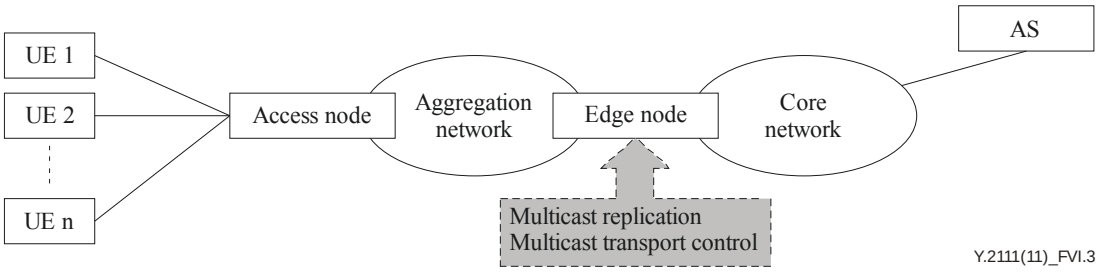


Figure VI.3 – Edge node requested multicast resource control with an MTCF scenario

Appendix VII

Inter-operator RACF communication scenarios for end-to-end QoS control involving nomadicity

(This appendix does not form an integral part of this Recommendation.)

The media flow involving multiple transport networks requires inter-operator RACF communication, if the application layer signalling or the path-coupled QoS signalling cannot be used for end-to-end resource reservation. Typical scenarios requiring inter-operator RACF communication with the Ri reference point are described in this appendix. Mechanisms of the application layer signalling and the path-coupled QoS signalling are not within the scope of this appendix. Note that nomadicity is the only use case for Ri in Recommendation ITU-T Y.2111 (2008).

These scenarios involve the following entities.

- CPE-x_n: Number n CPE provided by operator x
- RACF-x: RACF provided by operator x
- Transport network-x: Transport network provided by operator x

Scenario 1: One CPE is accommodated in a visited operator

Both CPE-A_1 and CPE-A_2 directly communicate with the SCF owned by operator A. Operator B transfers application layer signalling between CPE-A_2 and the SCF. The SCF sends the QoS information to RACF-A. According to the QoS information sent by the SCF, RACF-A reserves QoS resources in transport network-A. RACF-A also communicates with RACF-B using the Ri reference point to reserve QoS resources in transport network-B. Upon receipt of the QoS information, RACF-B reserves QoS resources between CPE-A_2 and transport network-A. Then, end-to-end QoS resources between CPE-A_1 and CPE-A_2 are reserved.

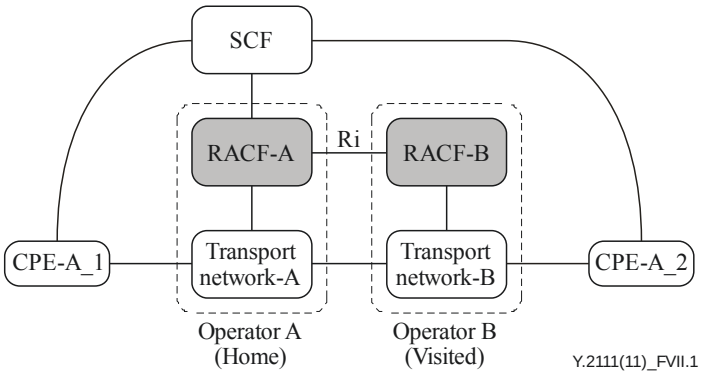


Figure VII.1 – Inter-operator RACF communication where one CPE is accommodated in a visited operator

Scenario 2: Two CPEs are accommodated in the same visited operators

Both CPE-A_1 and CPE-A_2 directly communicate with SCF owned by operator A. Operator B transfers application layer signalling between CPE-A_1 and the SCF. Operator B also transfers application layer signalling between CPE-A_2 and the SCF. SCF sends the QoS information to RACF-A. According to the QoS information sent by the SCF, RACF-A communicates with RACF-B using Ri reference point to reserve QoS resources in transport network-B. Upon receipt of the QoS information, RACF-B reserves QoS resources between CPE-A_1 and CPE-A_2. Then, end-to-end QoS resources between CPE-A_1 and CPE-A_2 are reserved.

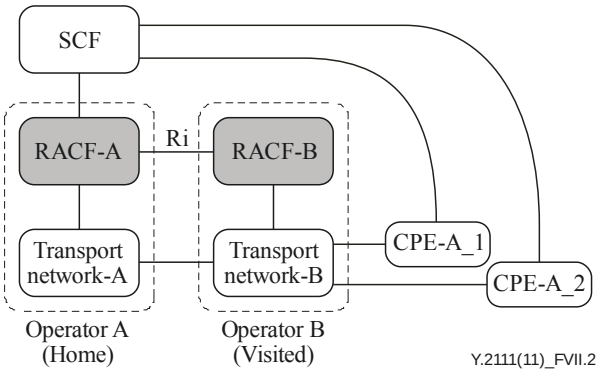


Figure VII.2 – Inter-operator RACF communication where two CPEs are accommodated in the same visited operators

Scenario 3: Two CPEs are accommodated in different visited operators

Both CPE-A_1 and CPE-A_2 directly communicate with the SCF owned by operator A. Operator B transfers application layer signalling between CPE-A_1 and the SCF. Operator C transfers application layer signalling between CPE-A_2 and the SCF. The SCF sends the QoS information to RACF-A. According to the QoS information sent by the SCF, RACF-A reserves QoS resources in transport network-A. RACF-A also communicates with RACF-B and RACF-C using the Ri reference point to reserve QoS resources in transport network-B and transport network-C, respectively. Upon receipt of the QoS information, RACF-B reserves QoS resources between CPE-A_1 and transport network-A, and RACF-C reserves QoS resources between CPE-A_2 and transport network-A. Then, end-to-end QoS resources between CPE-A_1 and CPE-A_2 are reserved.

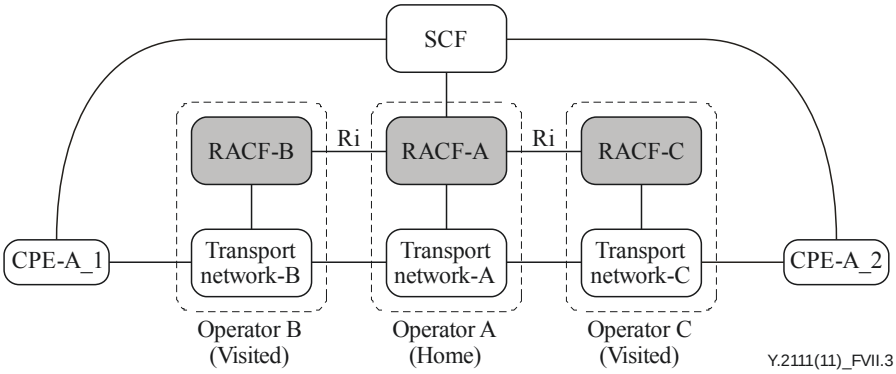


Figure VII.3 – Inter-operator RACF communication where two CPEs are accommodated in different visited operators

Appendix VIII

Comparison between reference point Rw and Rh

(This appendix does not form an integral part of this Recommendation.)

The information components of the Rh reference point are a subset of those of the Rw reference point. The following components of Rw are not included in Rh.

NAT traversal and dynamic firewall working mode:

- NAPT control and NAT traversal indication (Conditional)
  - Address translation command
  - Address binding information request
  - Address binding information response
- Dynamic firewall working mode (Optional)

Related information components used in pull mode:

- Resource reservation mode
- Authorization token (Optional)

The information components specific to the core network:

- Path selection information (Optional)

The information components related to charging:

- Charging correlation information (Optional)

The information flows exchanges of the Rh reference point are a subset of those of the Rw reference point. The following components of information exchange are not included in Rh:

- Resource decision request.
- Resource decision response.

Appendix IX

An example of an approach supporting time-shifted TV

(This appendix does not form an integral part of this Recommendation.)

Admission control for time-shifted TV services

While a CPE provides a live TV service as multicast, it may request a time-shifted TV service. In this case, a service provider places a video recording server which is for recording live TV somewhere in the network and provides a time-shifted TV service as unicast, then the CPE needs to request a new unicast service for time-shifted TV and needs to terminate a multicast service for live TV. One example of these admission control procedures for changing a multicast service to a unicast service is described in Figure IX.1.

On the other hand, if a service provider places a video recording server in the nearby transport node (i.e., access node) and provides a time-shifted TV service as multicast for reducing network resource costs, the CPE needs to change the multicast channel from live TV to time-shifted TV.

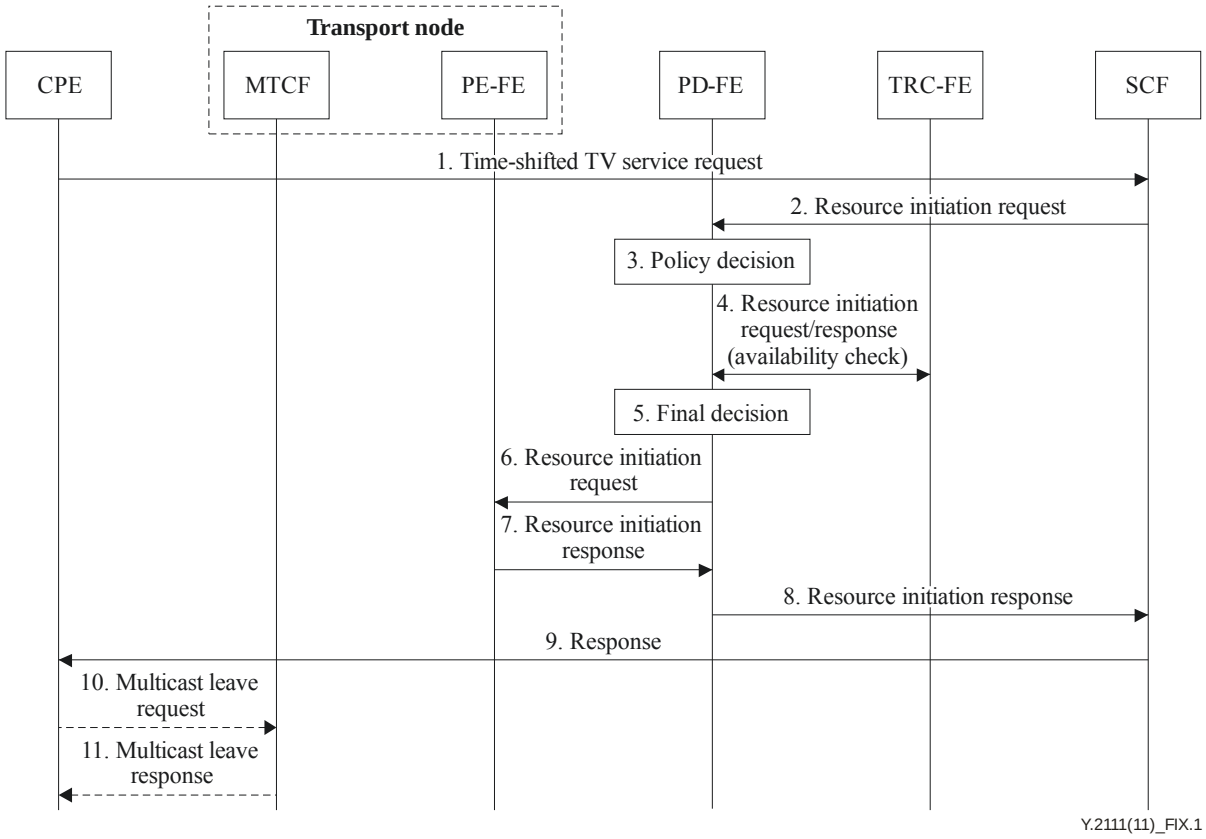


Figure IX.1 – Time-shifted TV service (unicast) request procedure

1) The CPE initiates a time-shifted TV service request to the SCF.

2) A resource initiation request (reservation) (i.e., RIR (reservation)) is usually triggered by the SCF. The SCF determines or derives the QoS requirement parameters (such as bandwidth, class of service) for the media flows of the time-shifted service. It then sends an RIR (reservation) with the media flow description and its QoS parameters to the PD-FE across the Rs reference point for QoS resource authorization and reservation.

3) On receipt of the RIR (reservation), the PD-FE is required to authorize the required QoS resources for the media flow. The PD-FE checks if the media flow description and the required QoS resources are consistent with network policy rules held in the PD-FE and the transport subscription information held in the NACF.

4) The PD-FE positions and determines which access networks and core networks are involved for the media flow. If there are TRC-FE instances in an involved network, the PD-FE sends an RIR (availability check) to one of the TRC-FE instances registered in the PD-FE to check resource availability in the involved network. If there are multiple TRC-FE instances in the involved network, they communicate with each other to determine if the required QoS resource is available from edge to edge in the involved network. The TRC-FE instance which received the RIR (availability check) is required to send an RIP back to the PD-FE. When multiple TRC-FE instances are present in the form of a distributed hierarchical structure, the top tier TRC-FE instance forwards the request to other TRC-FE instances in case those instances are in control of resources referenced in the request (i.e., the top tier TRC-FE has delegated resources to other TRC-FE instances). In this case the top tier TRC-FE makes the final resource admission decision based on the results of resource admission from all other instances.

5) The PD-FE makes the final admission decisions based on the results of steps (3) and (4). If the media flow is not admitted, the PD-FE sends an RIP with the rejection reason back to the SCF.

6) The PD-FE may send an RIR to install the final admission decisions in the PE-FE.

   The RIR from the PD-FE may request the admission decisions to be enforced immediately (i.e., RIR (reservation + commitment)), or may request the installation of admission decisions only (i.e., resource initiation request (reservation only)) and await a separate RIR (commitment) later for gate opening and resource allocation.

7) The PE-FE installs (and enforces) the final admission decisions sent from the PD-FE and sends an RIP back to the PD-FE.

8) The PD-FE sends an RIP back to the SCF.

9) The SCF sends the response to the CPE. If it is a positive response, an application session (application session for time-shifted TV services) is established between the SCF and the CPE. A time-shifted TV service is now provided.

10), (11) The CPE may send a transport signalling message (e.g., IGMP leave) to transport functions (i.e., MTCF) to terminate a multicast service for live TV.

Appendix X

Performance notification between the RACF and the MPM

(This appendix does not form an integral part of this Recommendation.)

X.1 Communication of multiple MPM functions

Figure X.1 illustrates the configuration of the communication between the RACF and multiple MPM functions. The PMR-FE in MPM1 communicates with the PMR-FE in MPM2 via the Mi reference point. Please note that the MPM1 also communicates with MPM3 via MPM2 or directly with MPM3 without going through MPM2.

The MPM functions process the performance information notification with the RACF as follows:

– CPE-A sends a request to the SCF to establish a session or sessions with CPE-B.

– The RACF receives the service resource request along with other relevant information of the incoming and/or the existing session(s) from the SCF via the Rs reference point in the RACF and passes this information to MPM1 over the Rm reference point in the RACF.

– The PMR-FE in MPM1 receives this information of the targeted session(s) and prepares for the authenticating requests for the initiation of measurements via the Mu reference point in MPM1. Furthermore, the PMR-FE in MPM1 communicates with the PMR-FE of MPM2 and other MPM functions via the Mi reference point in the MPMs, if the notifications of other MPM functions are required. Please note that each MPM has the communication paths among MPM functions prospectively established and the targeted session(s) are also identified by the indications of MPM1 which communicates with the RACF.

– Each PMR-FE requests the availability of measurements to each PME-FE via the PMP-FE and receives responses from the PME-FE.

– PMP-FEs in MPM1, MPM2 and MPM3 identify the targeted session(s) and prepare for the measurement report collection, passive measurement report analysis, measurement data aggregation, and rollup period analysis based on the requests of the RACF.

– PME-FE in MPM1 recognizes the IP address(es) and sessions information of the incoming and/or existing session(s).

– PME-FEs in MPM2 and MPM3 recognize the IP address(es) and sessions information of the incoming and/or existing session(s) based on the information provided by MPM1 via the Mi reference point in MPM.

– Then, PME-FEs in MPM1, MPM2 and MPM3 observe the targeted session(s).

– Each PMR-FE periodically receives notifications of the performance information measured by each PME-FE and replies with responses to the PME-FE.

– PMR-FEs in MPM1, MPM2 and MPM3 receive performance information measured by each PME-FE.

– After the analysis of the performance results measured at PMP-FEs in MPM1, MPM2 and MPM3, the performance information report is generated in PMR-FE in MPM1 and sent periodically to the RACF over the Mu reference point in MPM1.

– The report sent to the RACF includes the monitored network resource performance information.

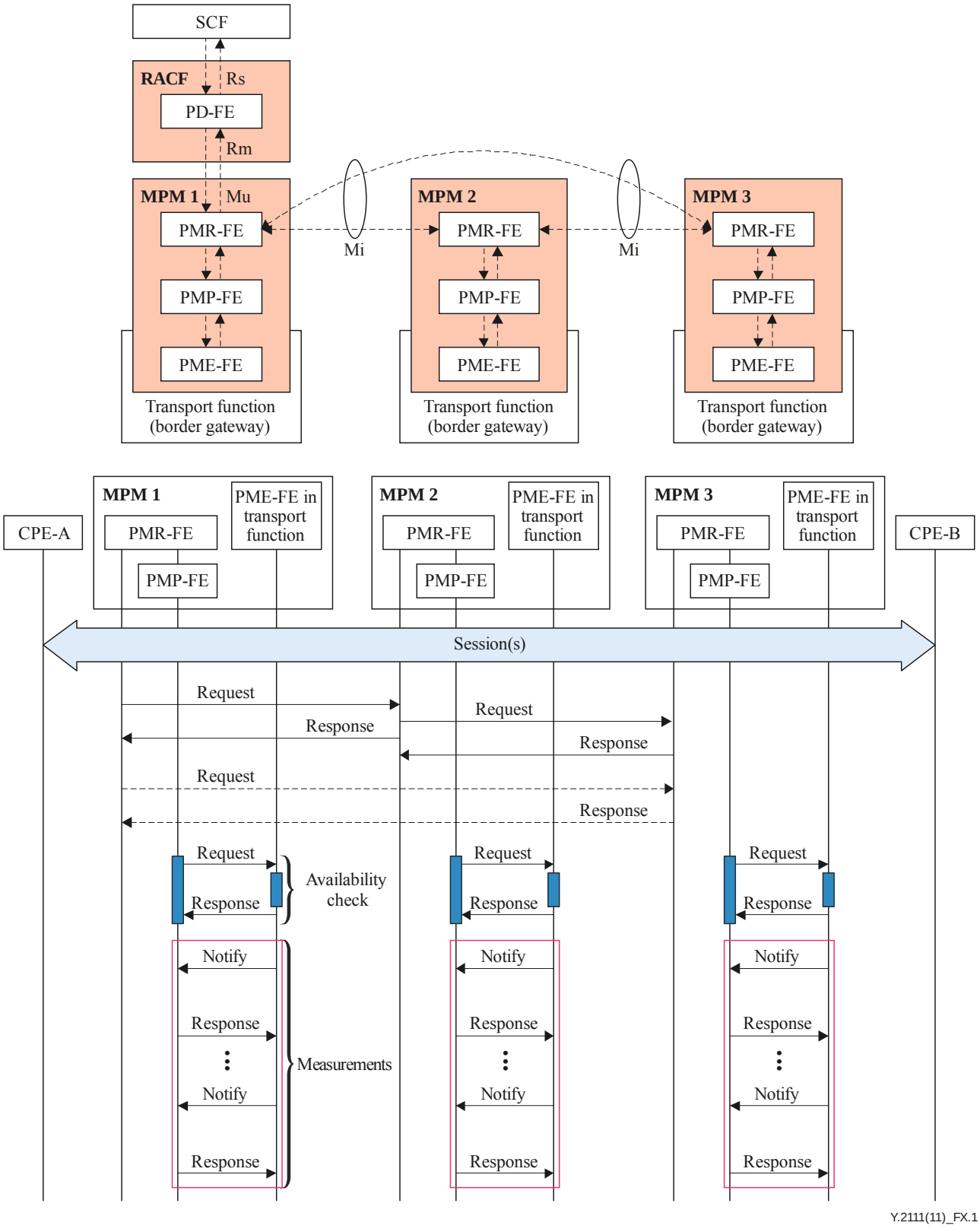


Figure X.1 – Performance notification between the PD-FE and the PMR-FE based on the communication of multiple MPM functions

X.2 The comparison of the specifications of the reference points between the Rc and the Rm in the RACF

Table X.1 – Comparison of the reference points between Rc and Rm in the RACF

	Rc	Rm
FEs using this reference point	TRC-FE and transport functions	PMR-FE of the MPM
1) Functional requirements	Collect the network topology information Collect the resource status information	Provide a description of sessions to measure Provide measurement and reporting intervals Collect a network-wide performance report
2) Information exchanged	Network topology information Resource status information	Session description Descriptions of the measurement and reporting intervals Network performance report
3) Information exchange requirements	Request/response transaction Notification Reliable delivery Capabilities Security	Request/response transaction Notification Reliable delivery Security Multiple connection between MPM applications and the PMR-FE
4) Protocols defined	SNMP	Not defined
5) Exchanged information details	Topology information Node IP address Interface IP address Link ID Resource status information Bandwidth usage per link and session Pre-provisioned bandwidth per link and session Reserved bandwidth per link and session	Session information The number of sessions 5 or 6-tuple session information Initiation/termination time to measure Frequency of measurement QoS class to measure RTP/RTCP information Performance report One-way delay per session One-way delay variation per session Loss ratio per session Bandwidth usage per link and session Reporting information specified by the RTCP Bandwidth of the session (s) such as the RTP and RTCP flow(s)

X.3 Use cases based on RACF-MPM communication

When the RACF performs an admission decision, the resource status information can be used:

1) It can be used to support an admission decision when a new session is requested.

2) It can be used to support an adjustment of an admission decision which has already been made for an admitted existing session(s).

In case 1, the current RACF uses resource status information mainly based on the bandwidth usage per link and session. With MPM, more detailed resource status information such as one-way delay, delay variation, and packet loss can be provided to the RACF for greater precision admission decisions. Since a new session is not yet established, resource status information is history information supporting that particular session. For example a session request between a pair of two hosts arrives; the RACF will request history resource status information collected for that particular pair of hosts. This information includes performance data (e.g., one-way delay, delay variation, loss rate or throughput) of sessions established between the pair hosts. With available bandwidth and other performance information, the RACF can make more accurate admission decisions (for example, a request with specific QoS requirements).

Furthermore, it is possible that the terminal could control the outgoing/incoming traffic of IP packets based on the QoS/QoE information measured by the MPM function located inside the terminal (terminal-side MPM function). The terminal could precisely perform autonomous traffic control if it can collect the QoS information of the core network as well as of the access network via functionaries of the MPM (network-side MPM). Then, the bandwidth of session(s) between the terminal-side MPM and the network-side MPM could be dynamically changed by the notifications of MPMs. Figure X.2 illustrates the rough concept of autonomous control of the traffic of the session(s) between the terminal-side MPM and the network-side MPM. It also shows that the RACF controls admissions of the incoming services, based on the QoS/QoE notifications of the terminal-side MPM via the network-side MPM. In other words, the MPMs between the terminal and the network node control the traffic between them and, at the same time, MPMs notify the updated terminal side QoS/QoE information to the RACF.

Please note that the notification intervals between the terminal-side MPM and the network-side MPM are relatively short. But the notification intervals between the network-side MPM and the RACF should be aligned considering the QoS requirements of the sessions of services controlled by the RACF. In general, the roles of the MPM functions for performance measurement is different from the terminal side and the network side, considering the scalability in the number of the sessions handled at an event.

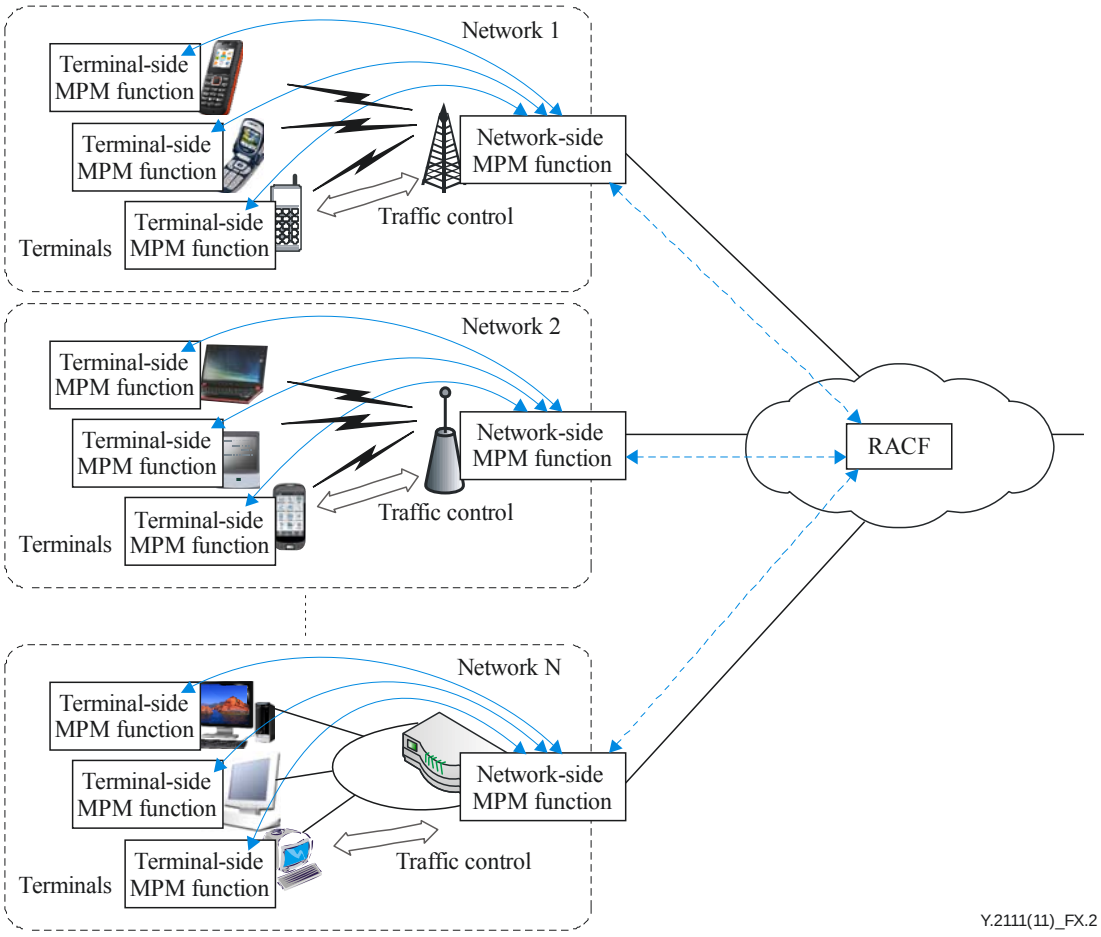


Figure X.2 – Autonomous traffic control based on the MPM function

In case 2, the current RACF does not support this scenario yet. Once a session is admitted, it stays for the duration of its lifetime, no matter how the quality of that particular session is degraded. This is mainly because there is no real-time performance monitoring support for an admitted session quality check. However, if we have such a capability support, the live session's admission decision can be adjusted, based on the real-time performance status. For example, a VoIP session once admitted starts to show severe performance degradation during the call. If this happens for a very short period of time so that the users can ignore or endure it, the case is relatively simple. But if this quality degradation lasts longer than the user's endurance level and the impacted call has a very high priority status, it would be better to deal with the situation. There are various ways to handle it. The simplest way is to find any available resource to be allocated for this call so that the problem can be fixed. Another solution is to pre-empt any less important resource if no resource is available without affecting others. Such a complex admission control adjustment can be possible if we have real-time performance information of the live sessions.

Appendix XI

Interaction examples between the RACF and the PCC

(This appendix does not form an integral part of this Recommendation.)

The network operator may run both the fixed and mobile networks. Usually, for the fixed network the RACF is deployed for resource admission control while for the mobile network, the PCC is deployed. For the user of, e.g., a dual-mode mobile UE, access to different networks may be chosen according to the user's requirement. For example, the mobile UE may connect to the network from a mobile access network, while visiting the service in the fixed network. Or the mobile UE may connect to the network from a fixed access network, while visiting the service in the mobile network. All these situations need the interaction between the RACF and the PCC in order to provide a QoS-guaranteed service. As the RACF and the PCC are different in functional architecture, functional entities and reference points, the interacting information flows between them cannot be directly recognized by each other. In order to ensure the effective cooperation, on the part of the RACF, it needs to enhance the function for mapping the policy rules from the PCC in order to fit the fixed transport functions.

NOTE – The interaction procedure in this Recommendation is defined from the RACF point of view only. The agreed interaction between the RACF and the PCC is for further study.

The following three scenarios show the details.

Scenario 1

Figure XI.1 depicts one situation where communication between the RACF and the PCC is needed. The mobile UE is connected to the mobile network, and its subscription information is located in the mobile network. The UE wants to visit the QoS-guaranteed service of the fixed network. In order to support this kind of service, the interaction between the RACF and the PCC is needed. Figure XI.3 shows a detailed procedure for the RACF interacting with the PCC.

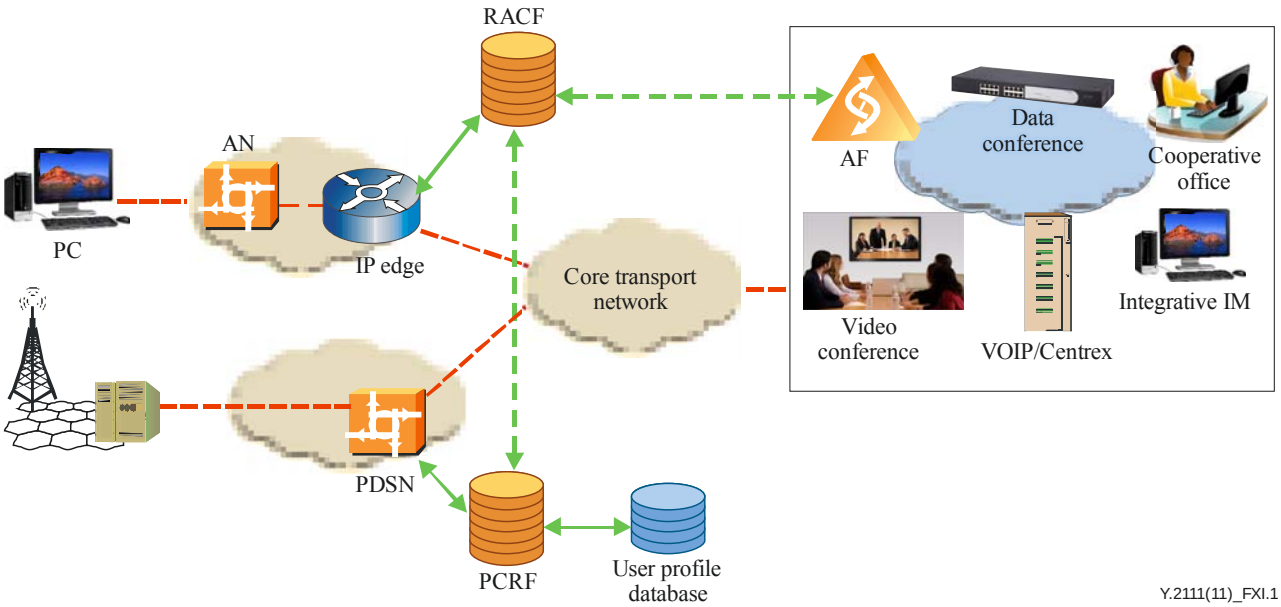


Figure XI.1 – Scenario 1: The RACF interacting with the PCC

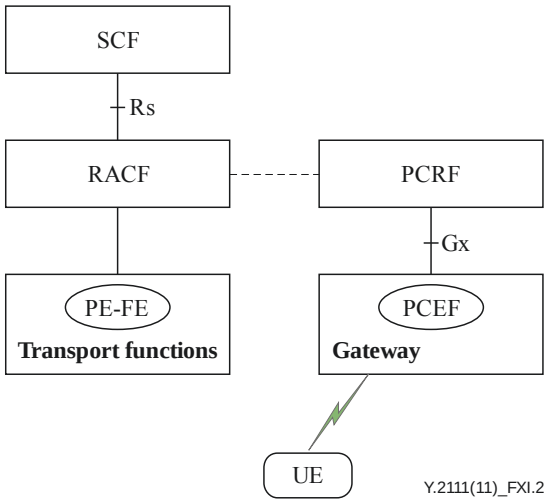


Figure XI.2 – The RACF interacting with the PCC of scenario 1

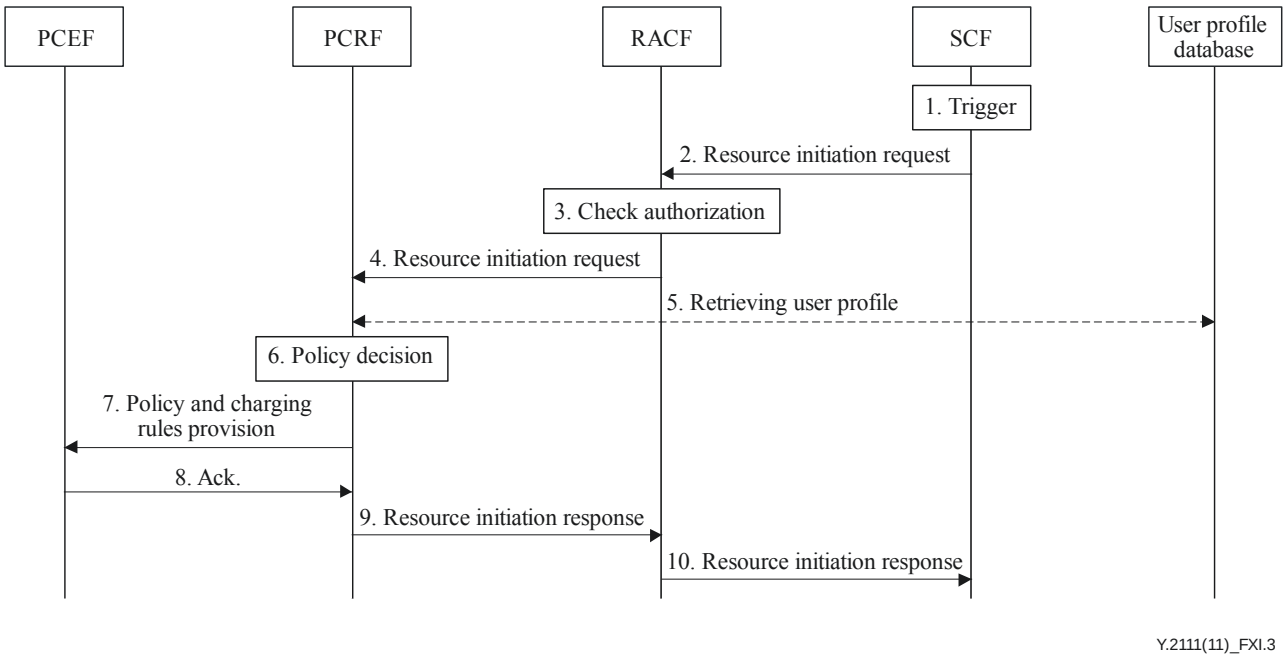


Figure XI.3 – The procedure for the RACF interacting with the PCC of scenario 1

1) A resource initiation request is usually triggered by a service establishment event or an internal action in the SCF. An example event is that a service signalling message is received at or generated by the SCF.

2) The SCF determines or derives the QoS requirement parameters (such as bandwidth, class of service) for the media flows of a given service. It then sends an RIR with the media flow description and its QoS parameters to the RACF across the Rs reference point for QoS resource authorization and reservation.

3) On receipt of the RIR, the RACF is required to authorize the required QoS resources for the media flow. The RACF checks if the media flow description and the required QoS resources are consistent with network policy rules held in the RACF.

4) As the RACF does not own the resources in the transport network, the RIR is sent on further to the PCRF.

5) If the PCRF does not have the subscriber's subscription-related information, it sends a request to the user profile database in order to receive the information related to the IP-connectivity access network (IP-CAN) session. The PCRF stores the subscription-related information containing the information about the allowed service(s) and the PCC rules information.

6) The PCRF makes the authorization and the policy decision.

7) The PCRF sends the policy and charging rules provision (PCC rules, event trigger, event report) to the PCEF.

8) The PCEF enforces the decision and sends the acknowledgement to the PCRF.

9) The PCRF sends an RIP back to the RACF.

10) The RACF sends an RIP back to the SCF.

Scenario 2

Figure XI.4 depicts another situation where communication between the RACF and the PCC is needed. The mobile UE is connected to the fixed network, while its subscription information belongs to the mobile network. The UE wants to visit the QoS-guaranteed service of the fixed network. In order to support this kind of service, the interaction between the RACF and the PCC is needed. Figure XI.5 shows a detailed procedure for the RACF interacting with the PCC.

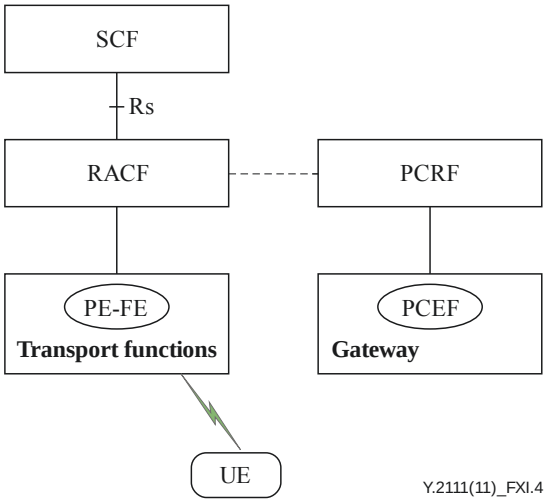


Figure XI.4 – The RACF interacting with the PCC of scenario 2

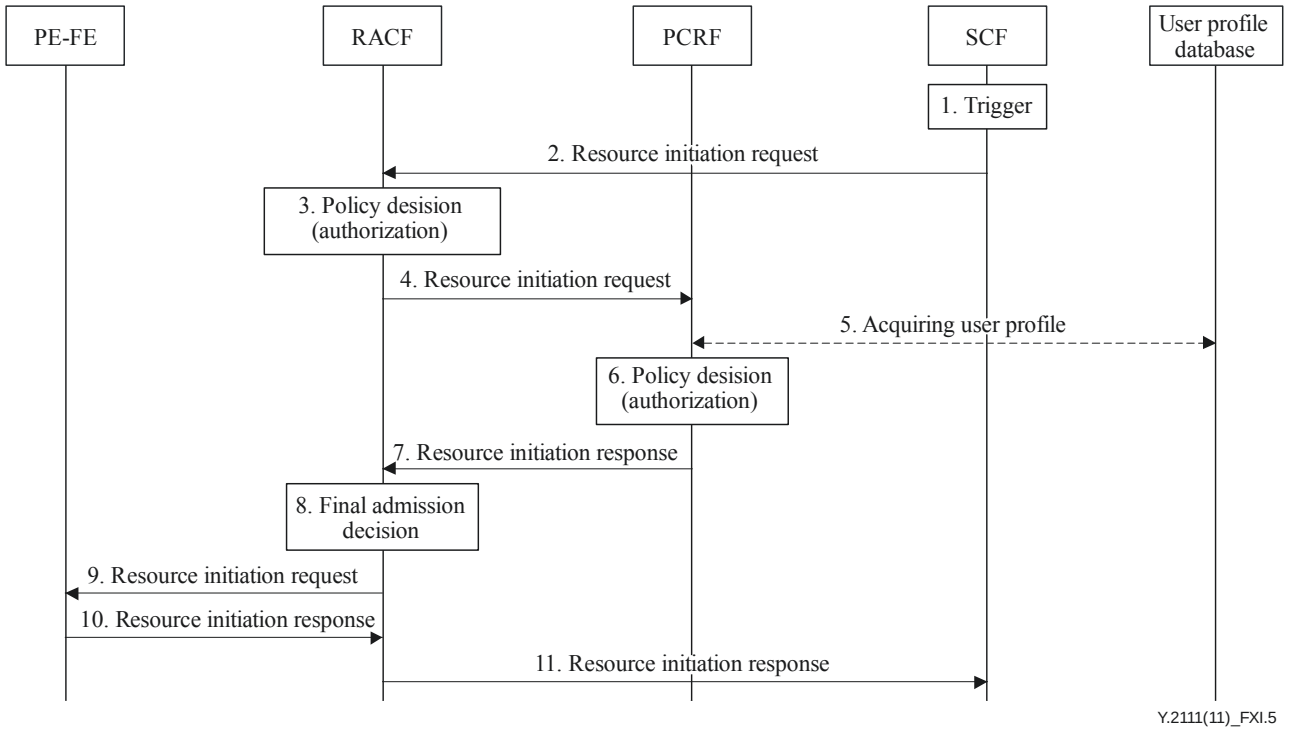


Figure XI.5 – The procedure for RACF interacting with PCC of scenario 2

1) A resource initiation request is usually triggered by a service establishment event or an internal action in the SCF. An example event is that a service signalling message is received at or generated by the SCF.

2) The SCF determines or derives the QoS requirement parameters (such as bandwidth, class of service) for the media flows of a given service. It then sends an RIR with the media flow description and its QoS parameters to the RACF across the Rs reference point for QoS resource authorization and reservation.

3) On receipt of the RIR, the RACF is required to authorize the required QoS resources for the media flow. The RACF checks if the media flow description and the required QoS resources are consistent with network policy rules held in the RACF and also the RACF checks resource availability in the involved network.

4) As the RACF does not own the access user profile, the RIR is sent on further to the PCRF.

5) If the PCRF does not have the subscriber's subscription-related information, it sends a request to the user profile database in order to receive the information. The PCRF stores the subscription-related information.

6) The PCRF makes the authorization and policy decision based on the subscription-related information, local network policy rules and service information.

7) After authorization, an RIP is sent to the RACF including the initial policy decisions from the PCRF.

8) The RACF makes the final admission decisions based on the results of steps (3) and (7).

9) The RACF may send an RIR to install the final admission decisions in the PE-FE.

10) The PE-FE installs (and enforces) the final admission decisions sent from the RACF and sends an RIP back to the RACF.

11) The RACF sends an RIP back to the SCF.

Scenario 3

Figure XI.6 depicts another situation where communication between the RACF and the PCC is needed. The mobile UE is connected to the fixed network, and its subscription information is located in the mobile network. The UE wants to visit the QoS-guaranteed service of the mobile network. In order to support this kind of service, the interaction between the RACF and the PCC is needed. Figure XI.8 shows a detailed procedure for the RACF interacting with the PCC.

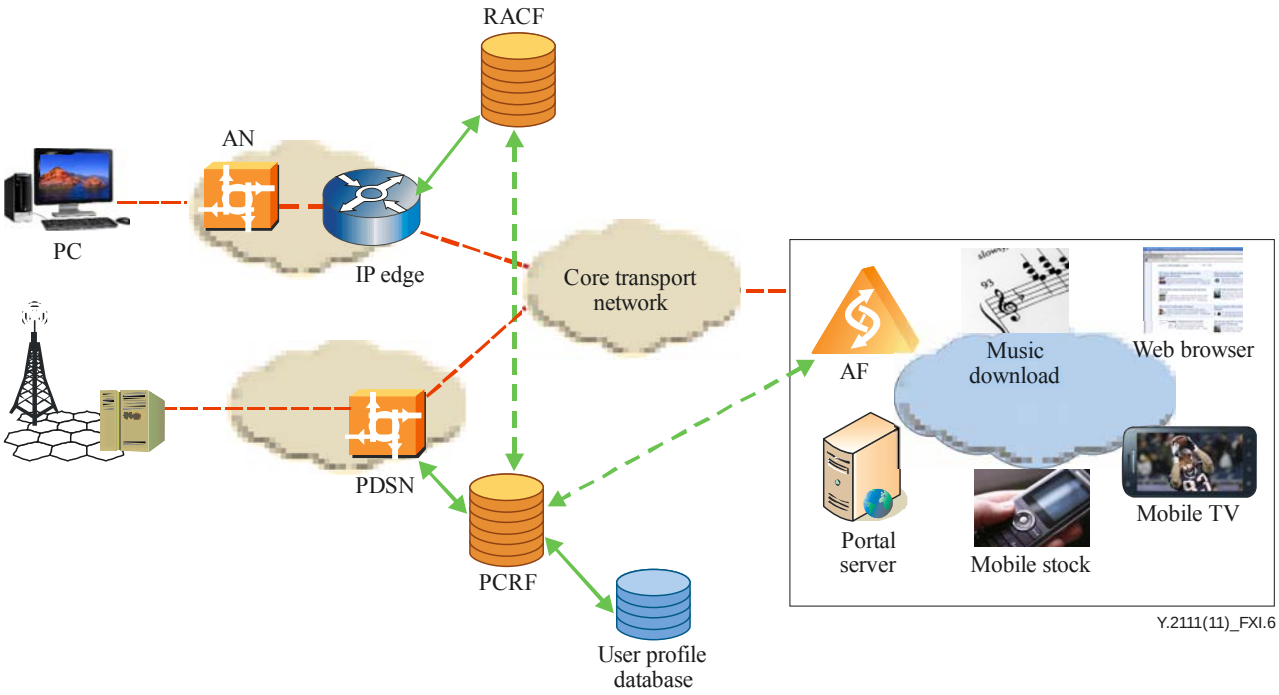


Figure XI.6 – Scenario 3 – The RACF interacting with the PCC

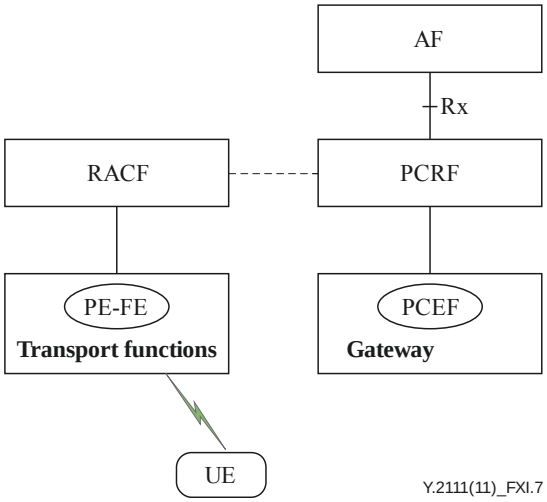


Figure XI.7 – The RACF interacting with the PCC of scenario 3

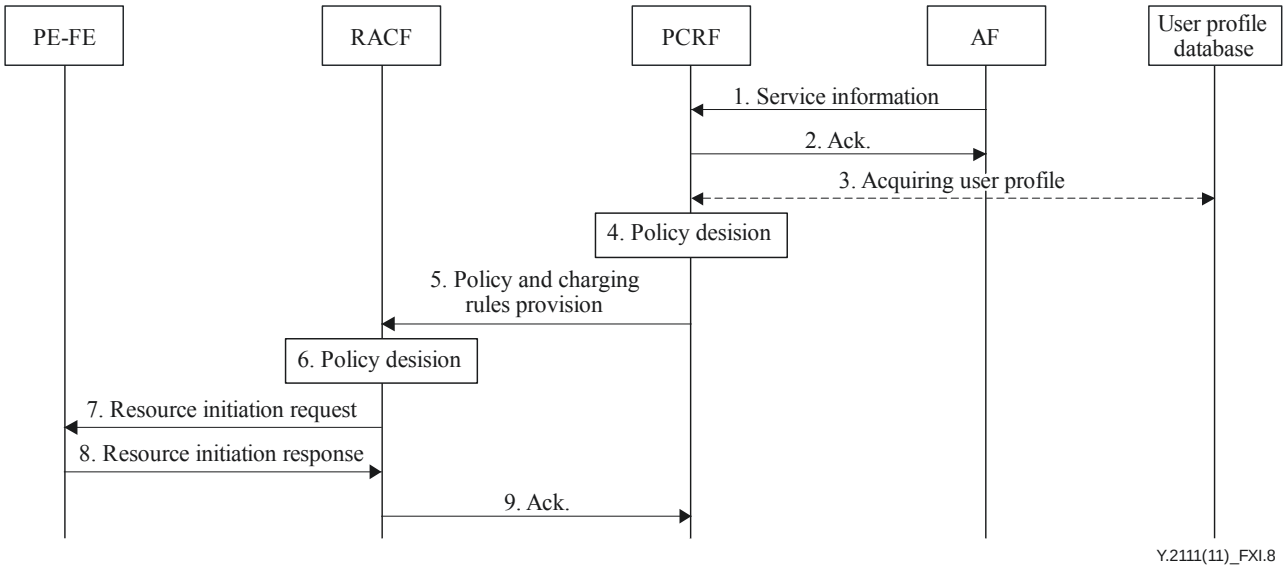


Figure XI.8 – The procedure for the RACF interacting with the PCC of scenario 3

1) Optionally, the AF provides service information to the PCRF due to AF session signalling.
2) The PCRF stores the service information if available. The PCRF determines if the request QoS resources are in the fixed network. If yes, the acknowledgement to the AF will be sent after step (9). If not, the acknowledgement will be sent just after step (1).
3) If the PCRF does not have the subscriber's subscription-related information, it sends a request to the user profile database in order to receive the information. The PCRF stores the subscription-related information.
4) The PCRF makes the authorization and policy decision.
5) The PCRF sends the policy and charging rules provision (PCC rules, event trigger, event report) to the RACF.
6) On receipt of the request, the RACF is required to authorize the required QoS resources for the media flow. The RACF checks if the media flow description and the required QoS resources are consistent with network policy rules held in the RACF and also the RACF checks resource availability in the involved network. If successful, the RACF would translate or transform the policy rules from the PCRF to the appropriate format which can be handled by the PE-FE.
7) The RACF may send an RIR to install the final admission decisions in the PE-FE.
8) The PE-FE installs (and enforces) the final admission decisions sent from the RACF and sends an RIP back to the RACF.
9) The RACF responds with the acknowledgement to the PCRF.

Appendix XII

Example admission control for IPTV service by invitation

(This appendix does not form an integral part of this Recommendation.)

An IPTV service user invites one of his friends to watch a program. The charge of the program will be paid by the inviter. In this case, he/she may initiate an IPTV service by invitation. If the invitee accepts the invitation, the SCF will send the service request to the invitee's RACF containing an invitation indication. After receiving the service request with the invitation indication, the RACF authorizes the required resources based on the network policy rules, including availability of the required resources. Since the required service is provided by the invitation to the invitee, the RACF does not check the invitee's transport subscription information during authorization.

The SCF-requested QoS resource reservation procedure for an IPTV service by invitation is illustrated in Figure XII.1.

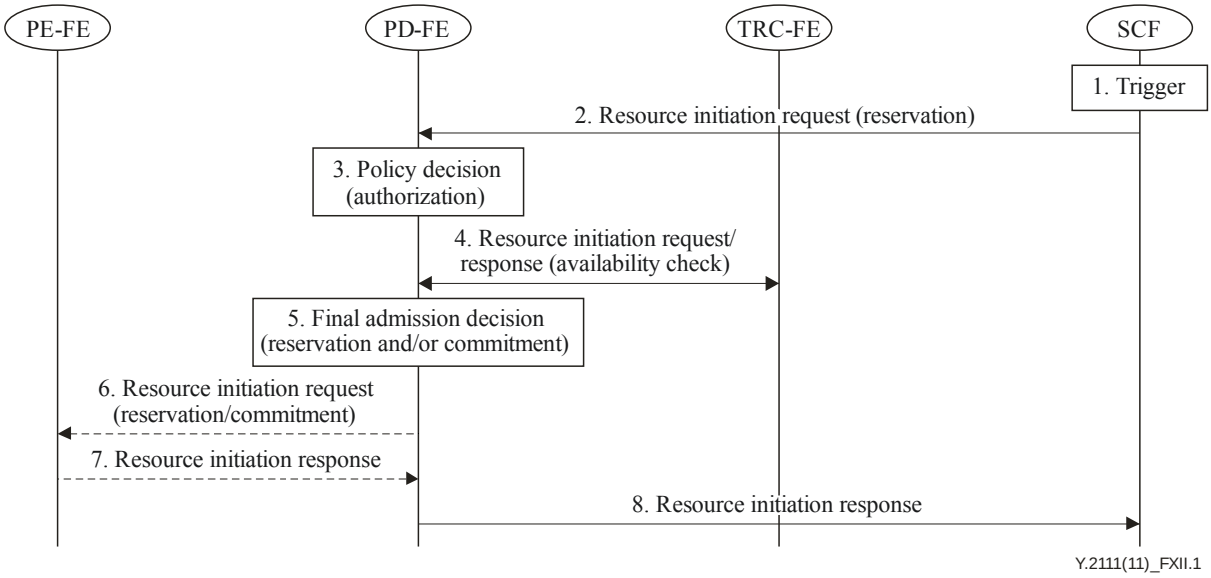


Figure XII.1 – SCF-requested QoS resource reservation procedure for an IPTV service by invitation

1) A resource initiation request (reservation) (i.e., RIR (reservation)) is usually triggered by a service establishment event or an internal action in the SCF. An example event can be when a service signalling message is received at or generated by the SCF.

2) The SCF determines or derives the QoS requirement parameters (such as bandwidth, class of service) for the media flows of a given IPTV service by invitation. It then sends an RIR (reservation) with the media flow description, invitation indication and its QoS parameters to the PD-FE across the Rs reference point for QoS resource authorization and reservation.

3) On receipt of the RIR (reservation), the PD-FE is required to authorize the required QoS resources for the media flow. The PD-FE checks if the media flow description and the required QoS resources are consistent with network policy rules which are made by the PD-FE. It includes checking on physical network resource availability. If the network physically cannot support the required resources, the RIR from the SCF will be rejected by the PD-FE.

4) The PD-FE determines which access networks and core networks are involved for the media flow. If there are TRC-FE instances in an involved network, the PD-FE sends an RIR (availability check) to one of the registered TRC-FEs to check resource availability in the involved network.

5) The PD-FE makes the final admission decision based on the results of steps (3) and (4). If the media flow is not admitted, the PD-FE sends an RIP with a rejection reason back to the SCF.

6) The PD-FE determines whether this service request requires sending a request to the PE-FE. If needed, the PD-FE sends an RIR to install the final admission decisions in the PE-FE.

7) The RIR from the PD-FE may request the admission decision to be enforced immediately (i.e., RIR (reservation + commitment)), or may request the installation of admission decision only (i.e., RIR (reservation only)) and await a separate RIR (commitment) later for gate opening and resource allocation. The detailed procedure for the separate RIR (commitment) is described in clause 10.1.1.1.3.

8) The PE-FE installs (and enforces) the final admission decision sent from the PD-FE and sends an RIP back to the PD-FE.

9) The PD-FE sends an RIP back to the SCF.

Bibliography

[b-ITU-T H.323] Recommendation ITU-T H.323 (2009), *Packet-based multimedia communications systems.*

[b-ITU-T Q.825] Recommendation ITU-T Q.825 (1998), *Specification of TMN applications at the Q3 interface: call detail recording.*

[b-ITU-T Q.Sup.51] ITU-T Q-Series Recommendations – Supplement 51 (2004), *Signalling requirements for IP-QoS.*

[b-ITU-T Y.101] Recommendation ITU-T Y.101 (2000), *Global Information Infrastructure terminology: Terms and definitions.*

[b-ITU-T Y.1221] Recommendation ITU-T Y.1221 (2010), *Traffic control and congestion control in IP-based networks.*

[b-ITU-T Y.1541] Recommendation ITU-T Y.1541 (2006), *Network performance objectives for IP-based services.*

[b-ITU-T Y.2171] Recommendation ITU-T Y.2171 (2006), *Admission control priority levels in Next Generation Networks.*

[b-ITU-T Y.2174] Recommendation ITU-T Y.2174 (2008) *Distributed RACF architecture for MPLS networks.*

[b-ITU-T Y.2701] Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN Release 1.*

[b-DSL TR 069] DSL Forum TR-069 (2004), *CPE WAN management protocol.*

[b-ETSI TS 123 207] ETSI TS 123 207 Ver. 10.0.0 (2011), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); End-to-end Quality of Service (QoS) concept and architecture.*

[b-ETSI TS 123 228] ETSI TS 123 228 Ver.10.5.0 (2011), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; IP Multimedia Subsystem (IMS); Stage 2.*

[b-IETF RFC 2205] IETF RFC 2205 (1997), *Resource ReSerVation Protocol (RSVP) Version 1 Functional Specification.*

[b-IETF RFC 2246] IETF RFC 2246 (1999), *The TLS Protocol Version 1.0.*

[b-IETF RFC 2403] IETF RFC 2403 (1998), *The Use of HMAC-MD5-96 within ESP and AH.*

[b-IETF RFC 2404] IETF RFC 2404 (1998), *The Use of HMAC-SHA-1-96 within ESP and AH.*

[b-IETF RFC 2405] IETF RFC 2405 (1998), *The ESP DES-CBC Cipher Algorithm With Explicit. IV.*

[b-IETF RFC 2410] IETF RFC 2410 (1998), *The NULL Encryption Algorithm and Its Use With IPsec.*

[b-IETF RFC 2412] IETF RFC 2412 (1998), *The OAKLEY Key Determination Protocol.*

[b-IETF RFC 2475] IETF RFC 2475 (1998), *An Architecture for Differentiated Services.*

[b-IETF RFC 2702] IETF RFC 2702 (1999), *Requirements for Traffic Engineering Over MPLS.*

[b-IETF RFC 3261] IETF RFC 3261 (2002), *SIP: Session Initiation Protocol.*

[b-IETF RFC 3272] IETF RFC 3272 (2002), *Overview and Principles of Internet Traffic Engineering.*

[b-IETF RFC 3312] IETF RFC 3312 (2002), *Integration of Resource Management and Session Initiation Protocol (SIP).*

[b-IETF RFC 3346] IETF RFC 3346 (2002), *Applicability Statement for Traffic Engineering with MPLS.*

[b-IETF RFC 3520] IETF RFC 3520 (2003), *Session Authorization Policy Element.*

[b-IETF RFC 3564] IETF RFC 3564 (2003), *Requirements for Support of Differentiated Services-aware MPLS Traffic Engineering.*

[b-IETF RFC 4124] IETF RFC 4124 (2005), *Protocol Extensions for Support of Diffserv-aware MPLS Traffic Engineering.*

[b-IETF RFC 4301] IETF RFC 4301 (2005), *Security Architecture for the Internet Protocol.*

[b-IETF RFC 4304] IETF RFC 4304 (2005), *Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP).*

[b-IETF RFC 4305] IETF RFC 4305 (2005), *Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH).*

[b-IETF RFC 4306] IETF RFC 4306 (2005), *Internet Key Exchange (IKEv2) Protocol.*

[b-IETF RFC 4307] IETF RFC 4307 (2005), *Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2).*

[b-IETF RFC 4308] IETF RFC 4308 (2005), *Cryptographic Suites for IPsec.*

[b-IETF RFC 4566] IETF RFC 4566 (2006), *SDP: Session Description Protocol.*

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects and next-generation networks**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2012