International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.2111

(09/2006)

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

ITU-T Recommendation Y.2111

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
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
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899

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

ITU-T Recommendation Y.2111

Resource and admission control functions in Next Generation Networks

Summary

This Recommendation specifies the functional architecture and requirements for the resource and admission control functions in Next Generation Networks, 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.

Source

ITU-T Recommendation Y.2111 was approved on 13 September 2006 by ITU-T Study Group 13 (2005-2008) under the ITU-T Recommendation A.8 procedure.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. 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/.

CONTENTS

Page

ITU-T Recommendation 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 (fixed, mobile, etc.). Services can make use of RACF whether the IP multimedia subsystem 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.

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 and NAT traversal.

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.

[Y.1291] ITU-T Recommendation Y.1291 (2004), *An architectural framework for support of Quality of Service in packet networks*.

[Y.2001] ITU-T Recommendation Y.2001 (2004), *General overview of NGN*.

[Y.2011] ITU-T Recommendation Y.2011 (2004), *General principles and general reference model for Next Generation Networks*.

[Y.2012] ITU-T Recommendation Y.2012 (2006), *Functional requirements and architecture of the NGN*.

3 Definitions

This Recommendation defines the following terms:

3.1 absolute QoS: Traffic delivery with numerical bounds on some or all QoS 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 relative QoS: Traffic delivery where bounds on QoS parameters such as delay, etc., 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.

3.3 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 conformance to the same set of policy decisions.

3.4 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.

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

3.6 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.

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

3.8 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 (mapped) from one address domain to another address domain.

3.9 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.

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

3.11 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.

3.12 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.

3.13 hard state: The state that is persistent until explicitly removed.

3.14 soft state: The state that has a lifetime and requires renewal to keep alive.

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

3.16 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.

4 Abbreviations

This Recommendation uses the following abbreviations:

AAA Authentication, Authorization and Accounting

ATM Asynchronous Transfer Mode

CDMA Code Division Multiple Access

CMTS Cable Modem Termination System

CNPS Core Network Path Selection

CPE	Customer Premises Equipment
CPN	Customer Premises Network
DiffServ	Differentiated Services
DoS	Denial of Service
DSCP	Differentiated Services CodePoint
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
ERC	Element Resource Control
ETS	Emergency Telecommunications Service
FDP	Final Decision Point
FWMS	Firewall Working Mode Selection
GC	Gate Control
GGSN	Gateway GPRS Support Node
GTP	GPRS Tunnelling Protocol
HTTP	Hypertext Transfer Protocol
ID	Identifier
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPMC	IP Packet Marking Control
LAN	Local Area Network
LSP	Label Switched Path
LTN	Logical Transport Network
MPLS	Multi-Protocol Label Switching
NACF	Network Attachment Control Functions
NAPT	Network Address Port Translation
NAPTC	NAPT Control
NAT	Network Address Translator
NGN	Next Generation Network
NRM	Network Resource Maintenance
NS	Network Selection
NTM	Network Topology Maintenance
NTRD	Network Topology and Resource Database
P-CSCF	Proxy-Call Session Control Function
PD-FE	Policy Decision Functional Entity
PE-FE	Policy Enforcement Functional Entity
PNNI	Private Network-to-Network Interface
PPP	Point-to-Point Protocol

QMTD QoS Mapping – Technology Dependent

QMTI QoS Mapping – Technology Independent

QoS Quality of Service

RACF Resource and Admission Control Function

RDR Resource Decision Request

RIP Resource Initiation Response

RIR Resource Initiation Request

RLC Rate Limiting Control

RMR Resource Modification Request

RRR Resource Release Request

RSVP Resource ReSerVation Protocol

RTCP RTP Control Protocol

RTP Real-Time Transport

SCF Service Control Function

SLA Service Level Agreement

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

UMTS Universal Mobile Telecommunications System

VCI Virtual Channel Identifier

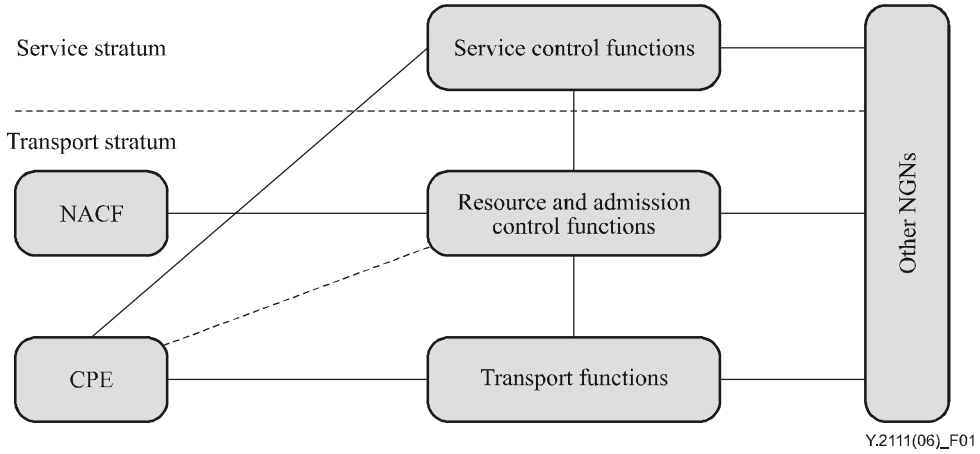
VPI Virtual Path Identifier

VPN Virtual Private Network

5 Overview and requirements

5.1 Overview

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



NOTE – The reference point between CPE and RACF is for further study.

Figure 1/Y.2111 – RACF within the NGN architecture

The RACF provides an abstract view of transport network infrastructure to the SCF and makes service providers agnostic to the details of transport facilities such as network topology, connectivity, resource utilization and QoS mechanisms/technology, etc. The RACF interacts with the SCF and transport functions for a variety of applications (e.g., SIP-based call [RFC 3261], video streaming, etc.) 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, 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), 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.

5.2 High-level requirements

The resource and admission control functional architecture shall meet the following mandatory high-level 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 CPE's differing intelligence and capability. For example, some CPE may support transport QoS signalling (e.g., GPRS session management signalling [TS 123 207], RSVP [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 [Q.Sup51]. 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 should meet the following optional high-level requirements:

a) Export information to support charging based on resource usage and/or QoS treatments.

b) Support methods for resource-based admission control.

c) Have access to and make use of information provided by network management on performance monitoring to assist in making resource-based admission decisions.

d) 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.

e) 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.

f) Support path selection between ingress and egress points within a single domain to satisfy QoS resource requirements.

6 RACF mechanisms and scenarios

6.1 QoS resource control mechanisms and scenarios

6.1.1 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 [RFC 4566]/SIP QoS extensions [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 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 shall 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 shall 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 resources 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 shall 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.

Information for resource control

The RACF shall 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 shall 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 does not vary from the individual resource request. 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.

6.1.2 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 shall 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 IMS [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 a dedicated application layer QoS signalling used for those application signalling protocols without QoS extensions or 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 with path-coupled QoS signalling in the transport stratum, i.e., CPE type 3 can be supported 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 must be pushed to the transport functions in advance. The path-coupled QoS signalling can be used to invoke resource commitment at the transport functions that, in turn, interact with the RACF or can be used in the reverse direction to 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 9.1.1.

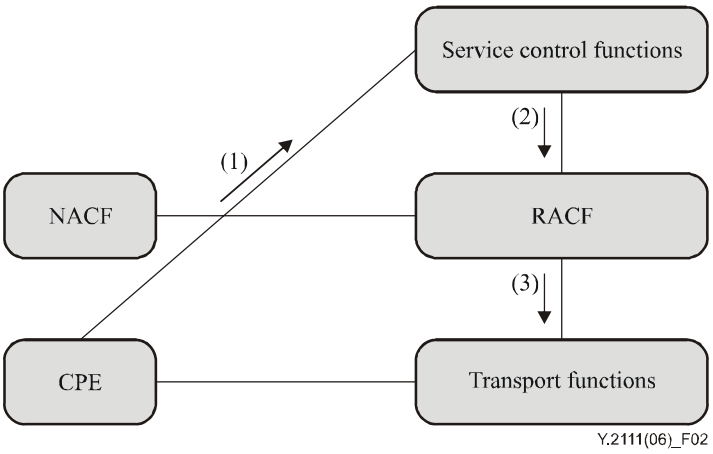


Figure 2/Y.2111 – The flow diagram for scenario 1

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 QoS signalling, such as CPE type 3.

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. But the QoS resource reservation needs pre-authorization via the SCF.

In this scenario the two-phase or three-phase resource control scheme can be used for coordination between the service signalling and the dedicated path-coupled transport QoS signalling.

Figure 3 depicts the high-level QoS resource control steps for scenario 2. The detailed information flows can be found in 9.1.2.

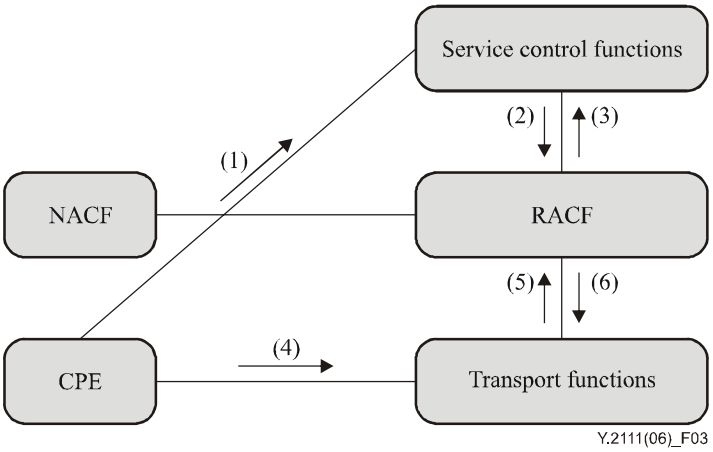


Figure 3/Y.2111 – The flow diagram for scenario 2

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 [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 initiates an explicit QoS request 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.

5) On receipt of the QoS request, the transport functions at the network edge send a request to RACF for resource reservation and admission control that may contain the authorization token as an option.

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.

6.2 NAPT control and NAT traversal mechanisms and scenarios

6.2.1 NAPT control and NAT traversal scenarios

The RACF shall 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.

6.2.2 NAPT control and NAT traversal mechanisms

The RACF shall 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.

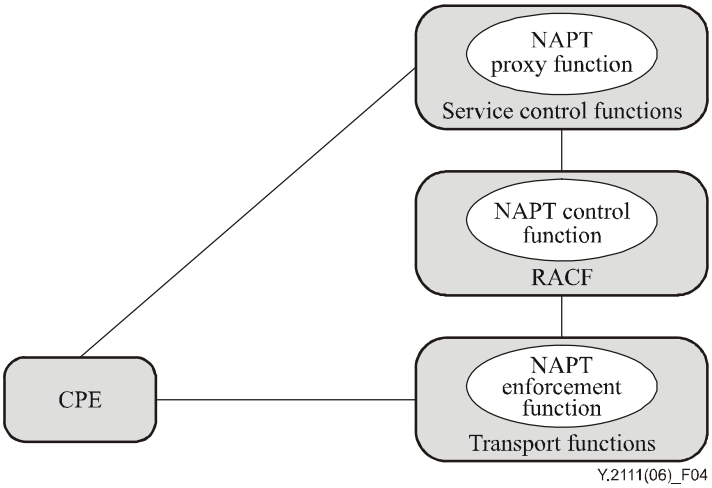


Figure 4/Y.2111 – NAPT and NAT traversal control mechanisms

The NAPT control function in RACF shall 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 network address/port translation information.

7 Functional architecture

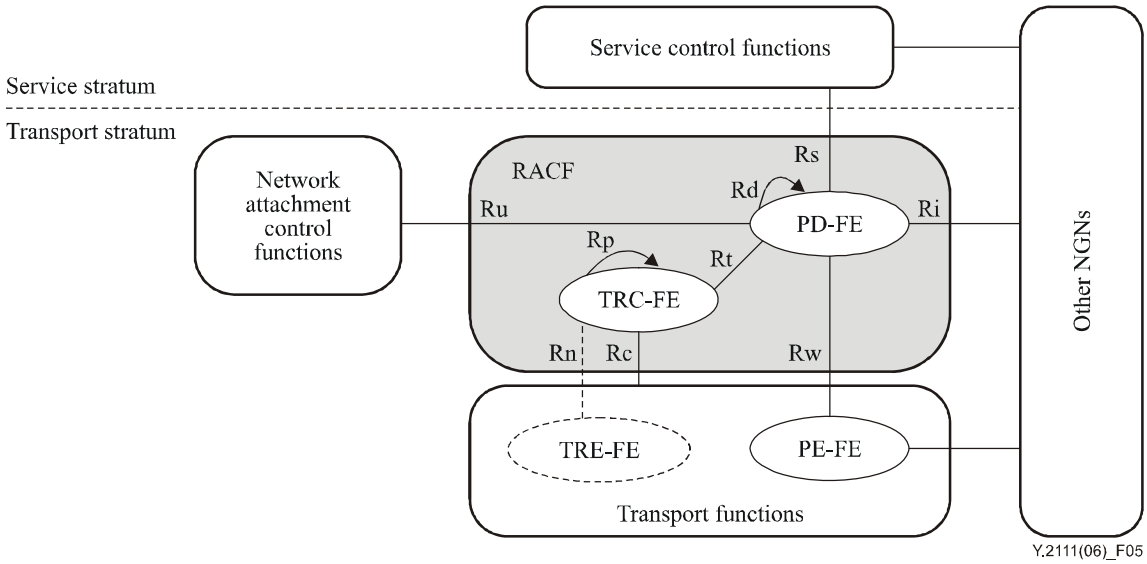


Figure 5/Y.2111 – Generic resource and admission control functional architecture in NGN

Figure 5 describes the functional architecture with functional entities and 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);
- NACF (Network attachment control functions).

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. Other NGNs may include access networks only or core networks only or both of them. The transport functions could also apply to access networks and core networks. NGN should allow both IPv4 and IPv6, so the impacts of NATs on the architecture and reference points (e.g., Rs and Rw) shall be considered as a whole. The NACF shall be connected to PD-FE in access network domains. 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 PE-FE, TRE-FE and other transport processing functional entities in the transport stratum defined in [Y.2012], to obtain the pertinent information.

Administrative domains are not represented in Figure 5. At least one PD-FE shall 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 access network domain or core network domain, or 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.

7.1 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 PD-FE and 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 to 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 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 subset 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 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 [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.

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 CPE and access network. It is the key injection node to enforce dynamic QoS and resource control, NAPT control and NAT traversal.

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 scope and functions of the TRE-FE and the Rn reference point are for further study.

7.2 Functional entity descriptions

7.2.1 Service control functions

The SCF in different domains can interact with 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 shall 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 shall 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 shall 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 shall indicate to the PD-FE whether it should be 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 shall be included in a signalling message to CPE.

7.2.2 Network attachment control functions

Network attachment control functions (NACF) provide 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.

7.2.3 Resource and admission control functions

7.2.3.1 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/Y.2111 – 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 on request from the SCF.
QMTI	QoS Mapping – Technology Independent	Maps the service QoS requirements and priority received from the SCF to network QoS parameters (e.g., Y.1541 class [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.

Table 1/Y.2111 – PD-FE elementary functions

Acronym	Function	Description
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/Y.2111 – 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.
NTM	Network Topology Maintenance	Collects and maintains the transport network topology information.
NRM	Network Resource Maintenance	Collects and maintains the transport resource status information.
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.		

7.2.3.2 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 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 PD-FE to relinquish all resources associated with the 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., Y.1541 class) and priority based on the network policy rules.
- Gate control (GC): This function controls 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 PE-FE and 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 7.2.4.1).
- 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 shall 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 shall 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, traffic descriptor, etc.

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 shall 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 PD-FE, such as the session duration, the resource control session information (e.g., the association between SCF and PD-FE, PD-FE and TRC-FE, PD-FE and 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.

7.2.3.3 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 PD-FE, the TRC-FE shall perform resource-based admission control based on the QoS and priority requirements received from the PD-FE (e.g., bandwidth and Y.1541 class), in conjunction with the resource utilization information and transport dependent policy rules, and shall update the resource status and return the result to 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 shall 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 a 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 PD-FE via the Rt reference point. This function detects and determines the availability of requested QoS resources based on the network topology and resource status information, as well as 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 PD-FE with a positive answer (e.g., resource available); otherwise, it responds PD-FE with a negative answer (e.g., resource unavailable).
- Network topology maintenance (NTM): This function collects and maintains the transport network topology information via the Rc reference point. Note that the Rc reference point can be connected to any transport functions including PE-FE, TRE-FE and other entities defined in [Y.2012] to obtain the relevant resource information.
- Network resource maintenance (NRM): This function collects and maintains the transport resource status information via the Rc reference point.
- 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. 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.

7.2.4 Transport functions

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

7.2.4.1 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 should 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 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.

7.2.4.2 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 should 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 scope and functions of the TRE-FE are for further study.

7.3 Mechanisms

7.3.1 Selection mechanisms

In order to transfer the resource control request between relevant functional entities (such as between SCF and PD-FE, PD-FE and TRC-FE, PD-FE and PE-FE, TRC-FE and TRC-FE, or PD-FE and PD-FE), a functional entity first needs to select the communicating party based on the information provided by a static or dynamic mechanism:

- Static mechanism: A functional entity may identify the target communicating party (e.g., SCF to PD-FE, PD-FE to TRC-FE) through statically configured location information, which includes either the IP address or the fully qualified domain name (FQDN). This information would be processed through, for example, the DNS.
- Dynamic mechanism: A functional entity may identify the target communicating party and determine its network address automatically through information such as the type of service and a set of service attributes, or the query of, for example, the DNS using the end user's identifier for the target communicating party in a particular address realm.

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

7.3.2 Binding mechanisms

The RACF shall 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 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 shall be used for the binding. The fully qualified domain name of the PD-FE and the 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.

8 Reference points

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

8.1 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 shall be able to support resource control for both fixed and mobile networks, and should 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.

8.1.1 Functional requirements

8.1.1.1 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 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.

8.1.1.2 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 shall provide the capability to support overload control for preventing the overflow of information messages exchanged between SCF and PD-FE.

Synchronization and audit: The Rs reference point shall 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 shall 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.

8.1.2 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 must 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 shall support the notification of asynchronous events (from the PD-FE to the SCF).

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

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

Security: All messages between the SCF and the PD-FE shall be authenticated 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.

One-to-many/many-to-one: Two modes shall be supported:

1) One-to-many mode: a SCF shall be able to communicate with multiple PD-FEs;
2) Many-to-one mode: multiple SCF instances shall 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.

8.1.3 Information components

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

8.1.3.1 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/Y.2111 – 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 requestor.
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 Requestor Identifier	An identifier for the requestor (i.e., the owner of SCF (e.g., a Service Provider)) of resource control service. It is unique over the requestors 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 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 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 is expired.

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 SCF and 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 globally unique IP address or transport subscriber identifier should 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 messages in 8.1.4. NOTE 3 – How the SCF obtains the information of transport subscriber ID is an issue for service stratum functionality.	

8.1.3.2 QoS resource information components

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

Table 4/Y.2111 – 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 PD-FE, and is to be converted by PD-FE to Network Class of Service (e.g., Y.1541 class for performance requirement) based on 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 5.

Table 5/Y.2111 – 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).
– 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 BW should be provided separately.

8.1.3.3 Authorization token information components

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

Table 6/Y.2111 – 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.

8.1.3.4 Charging correlation information component

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

Table 7/Y.2111 – 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.

8.1.3.5 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/Y.2111 – 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.
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 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 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 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 shall obtain the NAPT information, generate the address binding information and send it to relevant SCF instance. The SCF shall modify the message body of application signalling accordingly.

8.1.4 Information flows exchanged over Rs

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

8.1.4.1 Resource initiation request

The resource initiation request information flow is sent by the SCF to 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:

- 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 Requestor 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 (Conditional)
  - Address Binding Information Request

NOTE – One of these should be present.

8.1.4.2 Resource initiation response

The resource initiation response information flow is sent by 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)
  - 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

8.1.4.3 Resource modification request

The resource modification request information flow is sent by the SCF to 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 Requestor 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 (Conditional)
  - Address Binding Information Request

8.1.4.4 Resource modification response

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

8.1.4.5 Resource action request

The resource action request information flow is sent by 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)

  - 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

8.1.4.6 Resource action response

The resource action response information flow is sent by the SCF to 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 Requestor 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 (Conditional)
    - Address Binding Information Request

8.1.4.7 Resource notification

The resource notification information flow is sent by 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)
    - 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.

8.1.4.8 Resource release request

The resource release request information flow is sent by the SCF to 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 Requestor 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

8.1.4.9 Resource release response

The resource release response information flow is sent by PD-FE to the SCF to confirm the resource release request has been received and 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

8.1.4.10 Abort resource request

The abort resource request information flow is sent by 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 Requestor Identifier
- Resource Control Session Information (Optional)

- Timestamp
- Reason

8.1.4.11 Abort resource response

The abort resource response is sent by the SCF to 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)

8.2 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 shall be able to support resource control for both fixed and mobile access networks and should support NAPT/firewall control and NAT traversal at the PE-FE as needed.

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

8.2.1 Functional requirements

8.2.1.1 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 should allow for this flexibility.

8.2.1.2 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 shall 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 shall 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 shall 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.

8.2.2 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 must 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 must allow the notification of asynchronous events (from the PE-FE to the PD-FE).

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

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

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

One-to-many/many-to-one: Two modes shall be supported:

1) One-to-many mode: a PD-FE shall be able to communicate with multiple PE-FEs;

2) Many-to-one mode: multiple PD-FEs shall be able to make requests to a given PE-FE.

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

8.2.3 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.

8.2.3.1 Resource control processing information components

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

Table 9/Y.2111 – 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 Requestor Identifier (Optional, Note 2)	An identifier for the requestor (i.e., the owner of SCF (e.g., a Service Provider)) of resource control service. It is unique over the requestors 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 PE-FE based on the priority level.

Table 9/Y.2111 – Resource control processing information components (Rw)

Information component	Description
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 is 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 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 messages in 8.2.4. NOTE 2 – The resource requestor identifier may be used to assist PD-FE in identifying the unique relationship between the resource control session and requestor of the SCF. NOTE 3 – Reservation holding time may be used by PE-FE to assist 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., PE-FE or TRC-FE).	

8.2.3.2 QoS resource information components

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

Table 10/Y.2111 – 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., 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).
– 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.

Table 10/Y.2111 – QoS resource information sub-components (Rw)

Information component	Description
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 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 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 sub-components of the media flow description are described in Table 11.

Table 11/Y.2111 – 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.
– 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 BW should be provided separately.
– IP QoS handling class (Optional)	A QoS parameter for IP packet marking and handling in 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 [Y.1221]).

8.2.3.3 Authorization token information component

Table 12/Y.2111 – 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.	

8.2.3.4 Charging correlation information component

Table 13/Y.2111 – 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.

8.2.3.5 Resource control action information components

Table 14/Y.2111 – 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.

Table 14/Y.2111 – Resource control action information components (Rw)

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

8.2.4 Messages exchanged over Rw

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

8.2.4.1 Resource initiation request

The resource initiation request information flow is sent by PD-FE to 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 PD-FE if a stateless PE-FE is used. It contains the following information components:

- PD-FE Identifier
- Resource Control Session Identifier
- Resource Requestor 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

8.2.4.2 Resource initiation response

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

- PD-FE Identifier
- Resource Control Session Identifier
- Resource Requestor 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

8.2.4.3 Resource modification request

The resource modification request information flow is sent by PD-FE to 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 Requestor 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

8.2.4.4 Resource modification response

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

8.2.4.5 Resource action request

The resource action request information flow is sent by PE-FE to 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 Requestor 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

8.2.4.6 Resource action response

The resource action response information flow is sent by PD-FE to 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 Requestor 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

8.2.4.7 Resource notification

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

- PD-FE Identifier
- Resource Control Session Identifier
- Resource Requestor 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

8.2.4.8 Resource decision request

The resource decision request information flow is sent by PE-FE to 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 Requestor 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

8.2.4.9 Resource decision response

The resource decision response information flow is sent by PD-FE to authorize the request and provide the information to 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 Requestor 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

8.2.4.10 Resource release request

The resource release request information flow is sent by PD-FE to 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 Requestor 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

8.2.4.11 Resource release response

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

- PD-FE Identifier
- Resource Control Session Identifier
- Resource Requestor Identifier (Optional)
- Resource Control Session Information (Optional)
- Resource Request Result

8.2.4.12 Abort resource request

The abort resource request information flow is sent by PE-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 Requestor Identifier (Optional)
- Resource Control Session Information (Optional)
- Authorization Token (Optional)
- Timestamp
- Reason

8.2.4.13 Abort resource response

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

- PD-FE Identifier
- Resource Control Session Identifier
- Resource Requestor Identifier (Optional)
- Resource Control Session Information (Optional)

8.3 Reference point Rc

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

The Rc reference point allows 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 PE-FE, TRE-FE and other functional entities in the transport stratum defined in [Y.2012], to obtain the relevant information.

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

8.3.1 Functional requirements

The Rc reference point provides the ability for 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.

8.3.2 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 must 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 must allow the notification of asynchronous events (from a transport element to the TRC-FE).

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

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

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

8.3.3 Information exchanged

The resource status information should 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 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.

8.4 Reference point Ru

The Ru reference point allows 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.

8.4.1 Functional requirements

8.4.1.1 Resource control functional requirements

The Ru reference point provides the ability for 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.

8.4.1.2 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 shall provide the capability to support overload control for preventing the overflow of information messages exchanged between the PD-FE and NACF.

Synchronization and audit: The Ru reference point shall 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 shall 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.

8.4.2 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 must 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 shall support the notification of asynchronous events (from the NACF to the PD-FE).

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

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

Security: All messages between the PD-FE and NACF shall be authenticated such that requests to the NACF from unauthenticated sources will not be performed and such that the PD-FE can verify the source of notifications sent from the NACF.

Many-to-one: Many-to-one mode, multiple PD-FE instances shall 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.

8.4.3 Information components

The information components consist of those in Tables 15 to 17.

Table 15/Y.2111 – 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 PE-FE device, and MAC address or Link ID and physical port).
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 16/Y.2111 – 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 17/Y.2111 – 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., 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.

8.4.4 Information exchanged over Ru

The Ru reference point should allow information exchange as follows:

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

The PD-FE and NACF should use one of two selection mechanisms, either local static configuration or dynamic discovery, based on 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 should be exchanged through the Ru reference point:

8.4.4.1 Transport resource information request

The transport resource information request information flow is sent by PD-FE to NACF to request the access transport network profile information. Globally unique IP address information and/or transport subscriber identifier should 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)

NOTE – One of them shall be present.

8.4.4.2 Transport resource information response

The transport resource information response information flow is sent by the NACF to 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

NOTE – One of them shall be present.

8.4.4.3 Transport resource information indication

The transport resource information indication information flow is sent by the NACF to 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
- Default Configuration (Optional)
  - Default Access Control List
  - Default Upstream Bandwidth
  - Default Downstream Bandwidth

NOTE – One of them shall be present.

8.4.4.4 Transport resource release notification

The transport resource release notification information flow is sent by 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 shall be present.

8.5 Reference point Rt

The Rt reference point allows PD-FE to interact with 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 NACF to TRC-FE through PD-FE.

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

8.5.1 Functional requirements

8.5.1.1 Resource control functional requirements

The Rt reference point provides the ability for 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. PD-FE may also request TRC-FE to provide the path selection information for a given flow in the core network.

8.5.1.2 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 shall 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 shall 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 shall 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.

8.5.2 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 must 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 must allow the notification of asynchronous events (from the TRC-FE to the PD-FE).

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

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

Security: All messages between PD-FE and TRC-FE should be authenticated such that requests to the TRC-FE from unauthenticated sources will not be performed and such that notifications sent from the TRC-FE to PD-FE can be ensured to come from an authenticated PE-FE source.

One-to-many/many-to-one: Two modes shall be supported:

1) One-to-many mode: a PD-FE shall be able to communicate with multiple TRC-FEs;

2) Many-to-one mode: multiple PD-FEs shall be able to make requests to a given TRC-FE.

8.5.3 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.

8.5.3.1 Resource control processing information components

The resource control processing information components at Rt are as described in Table 18.

Table 18/Y.2111 – 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, Note 2)	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 Requestor Identifier (Optional, Note 3)	An identifier for the requestor (i.e., the owner of SCF (e.g., a Service Provider)) of resource control service. It is unique over the requestors 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 TRC-FE based on the priority level.
Reservation Holding Time (Optional, Note 4)	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 is expired.

Table 18/Y.2111 – Resource control processing information components (Rt)

Information component	Description
Resource Control Session Information (Optional, Note 5)	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 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 messages in 8.5.4. NOTE 2 – One of them should be present. NOTE 3 – The resource requestor identifier may be used to assist PD-FE in identifying the unique relationship between the resource control session and requestor of the SCF. NOTE 4 – Reservation holding time may be used by PE-FE to assist PD-FE in monitoring the resource control session timeout and/or state. NOTE 5 – 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., PE-FE or TRC-FE).	

8.5.3.2 QoS resource information components

The QoS resource information sub-components for media session and media flows are described in Table 19.

Table 19/Y.2111 – 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).
– 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., 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., Y.1541 class).

Table 19/Y.2111 – QoS resource information sub-components (Rt)

Information component	Description
– 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, may be also 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 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 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., 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.
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 20.

Table 20/Y.2111 – 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 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 BW should be provided separately.
– IP QoS handling class (Optional)	A QoS parameter for IP packet marking and handling in 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 [Y.1221]).

8.5.3.3 Authorization token information component

N/A.

8.5.3.4 Charging correlation information component

N/A.

8.5.3.5 Resource control action information components

Table 21/Y.2111 – 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).

Table 21/Y.2111 – Resource control action information components (Rt)

Information component	Description
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 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.

8.5.4 Information exchanged over Rt

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

8.5.4.1 Resource initiation request

The resource initiation request information flow is sent by PD-FE to 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 Requestor 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 should be present.

8.5.4.2 Resource initiation response

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

- PD-FE Identifier
- Resource Control Session Identifier
- Resource Requestor 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)

8.5.4.3 Resource modification request

The resource modification request information flow is sent by PD-FE to 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 Requestor 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

8.5.4.4 Resource modification response

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

8.5.4.5 Resource action request

The resource action request information flow is sent by TRC-FE to 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 Requestor 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

8.5.4.6 Resource action response

The resource action response information flow is sent by PD-FE to 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 Requestor 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

8.5.4.7 Resource notification

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

- PD-FE Identifier
- Resource Control Session Identifier
- Resource Requestor 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

8.5.4.8 Resource release request

The resource release request information flow is sent by PD-FE to 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 Requestor 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

8.5.4.9 Resource release response

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

- PD-FE Identifier
- Resource Control Session Identifier
- Resource Requestor Identifier (Optional)
- Resource Control Session Information (Optional)
- Resource Request Result

8.5.4.10 Abort resource request

The abort resource request information flow is sent by TRC-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 Requestor Identifier (Optional)
- Resource Control Session Information (Optional)
- Timestamp
- Reason

8.5.4.11 Abort resource response

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

- PD-FE Identifier
- Resource Control Session Identifier
- Resource Requestor Identifier (Optional)
- Resource Control Session Information (Optional)

8.6 Reference point Rp

An operator's core network may have multiple sub-domains. It may deploy multiple TRC-FE instances to control different sub-domains.

Some sub-domains only provide transport functions without service support nodes. In NGN, the signalling path between the SCF for a session is not always coupled with the data path. For an individual session, commonly only the SCF in the source and destination domains are involved in the session control signalling, whereas other domains along the data path are not. It could be

difficult for the SCF in the source and destination domains to identify and contact all TRC-FE instances along the media flow path within the whole operator's network to detect and determine the requested resource, since SCF and PD-FE have no knowledge of the details of the media flow path and the transport-dependent network resource status information within the operator's network. The communication between TRC-FE instances enables the SCF to only contact a single TRC-FE instance through the PD-FE.

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

8.6.1 Functional requirements

8.6.1.1 Resource control functional requirements

The Rp reference point allows the TRC-FE instances to communicate with each other for detection and determination of the availability of the requested QoS resource for a media flow from edge to edge within an operator's core network, and for path selection. Rp is applicable to TRC-FE instances under the control of the same PD-FE.

8.6.1.2 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 shall 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 shall 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 shall 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.

8.6.2 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 must 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 must allow the notification of asynchronous events (from a TRC-FE to another TRC-FE).

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

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

Security: All messages between TRC-FE instances should be authenticated such that requests to a TRC-FE from unauthenticated sources will not be performed and such that notifications sent from a TRC-FE to another TRC-FE can be ensured to come from an authenticated source.

8.6.3 Information components

8.6.3.1 Resource control processing information components

The information components for request processing, described in Table 22 below, provide the information used for discovery, binding, flow control (overload control), state maintenance, etc.:

Table 22/Y.2111 – Resource control processing information components (Rp)

Information component	Description
TRC-FE Identifier	A unique identifier for different instances of 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 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 is 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.

8.6.3.2 QoS resource information components

The QoS resource information sub-components for media session and media flows are described in Table 23.

Table 23/Y.2111 – QoS resource information sub-components (Rp)

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).
– 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., 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.

Table 23/Y.2111 – QoS resource information sub-components (Rp)

Information component	Description
– 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, may be also 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.

The information sub-components of the media flow description are described in Table 24.

Table 24/Y.2111 – 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 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 BW should be provided separately.
– IP QoS handling class (Optional)	A QoS parameter for IP packet marking and handling in 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 [Y.1221]).

8.6.3.3 Authorization token information components

N/A.

8.6.3.4 Charging correlation information components

N/A.

8.6.3.5 Resource control action information components

Table 25/Y.2111 – 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.

8.6.4 Information exchanged over Rp

This clause describes the information exchanged over Rp.

8.6.4.1 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. The request, i.e., information flow, communicates the following information:

- TRC-FE Identifier
- Resource Control Session Identifier
- Resource Requestor Identifier (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)
- Event Notification Indication (Optional)
  - Resource Information Indicator
  - Transport Loss Indicator
  - Transport Recovery Indicator
  - Transport Release Indicator

8.6.4.2 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 Requestor 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)
  - 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)

8.6.4.3 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. The request, i.e., information flow, communicates the following information:

- TRC-FE Identifier
- Resource Control Session Identifier
- Resource Requestor Identifier (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)
- Event Notification Indication (Optional)
  - Resource Information Indicator
  - Transport Loss Indicator
  - Transport Recovery Indicator
  - Transport Release Indicator

8.6.4.4 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.

8.6.4.5 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 Requestor Identifier (Optional)
- Resource Control Session Information (Optional)
- Reason

8.6.4.6 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 Requestor Identifier (Optional)
- Resource Control Session Information (Optional)
- Reason

8.6.4.7 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 Requestor Identifier (Optional)
- Resource Control Session Information (Optional)
- Reason

8.6.4.8 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 Requestor Identifier (Optional)
- Resource Control Session Information (Optional)
- Reason

8.7 Reference Point Ri

The Ri reference point is an inter-domain reference point.

The Ri reference point may convey network QoS information between domains. The format and content of this information is for further study.

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.

For example:

- When the SCF interacts with the PD-FE only at the originating and terminating network domains, the Ri reference point can be used to request resource and admission control over intermediate third-party transit domain(s).
- 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 that the details of Ri reference point are for further study.

8.7.1 Functional requirements

The functional requirements on Ri are similar to the requirements on Rs. In peering relations between operators, the PD-FE instance of each operator may interact with PD-FE instances of other operators.

8.8 Reference point Rd

Note that the details of Rd reference point are for further study.

The PD-FE shall 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.

8.8.1 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 PD-FE.

8.9 Summary

Table 26/Y.2111 – Reference points and domain attributes

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

9 Procedures

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

9.1 Procedures for QoS control

9.1.1 SCF-requested QoS control procedures

Scenario 1 described in 6.1 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.

9.1.1.1 Basic procedures

9.1.1.1.1 QoS resource reservation procedure

The SCF-requested QoS resource reservation procedure illustrated in Figure 6 is initiated by a resource initiation request from the SCF.

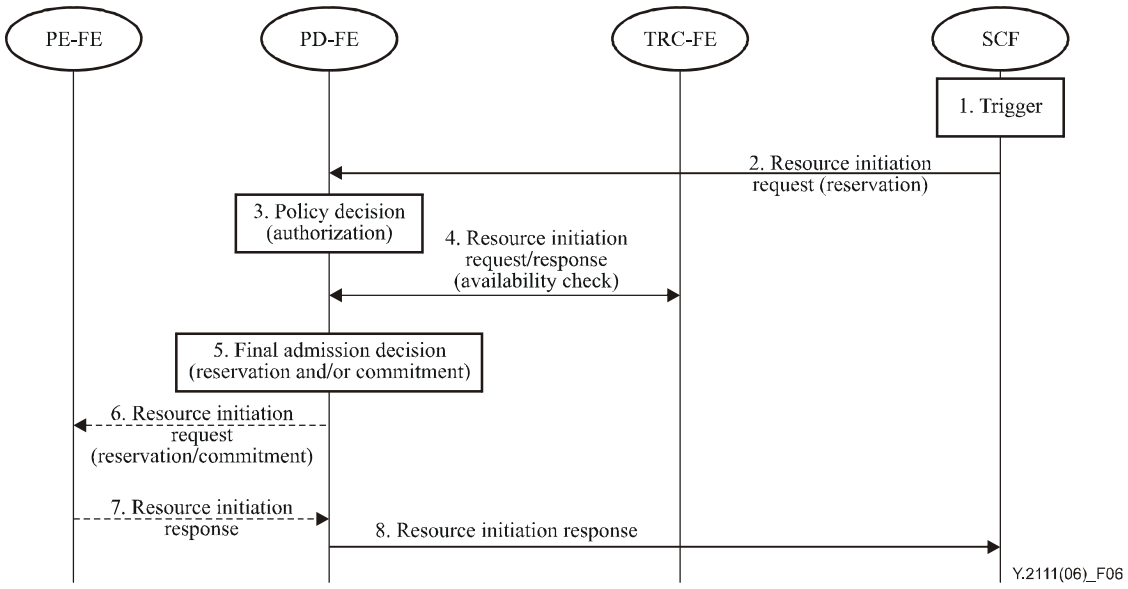


Figure 6/Y.2111 – SCF-requested QoS resource reservation procedure

1) A resource initiation request (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 a 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 shall 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 a 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) shall send a resource initiation response (i.e., RIP) back to the PD-FE.

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 a RIP with the rejection reason back to the SCF.

6) The PD-FE may send a RIR to install the final admission decisions in the PE-FE.

   The RIR from 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 9.1.1.1.2.

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

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

9.1.1.1.2 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 a RIR (commitment) is received from the SCF. The admission decision activation procedure for the two-phase scheme is illustrated in Figure 7.

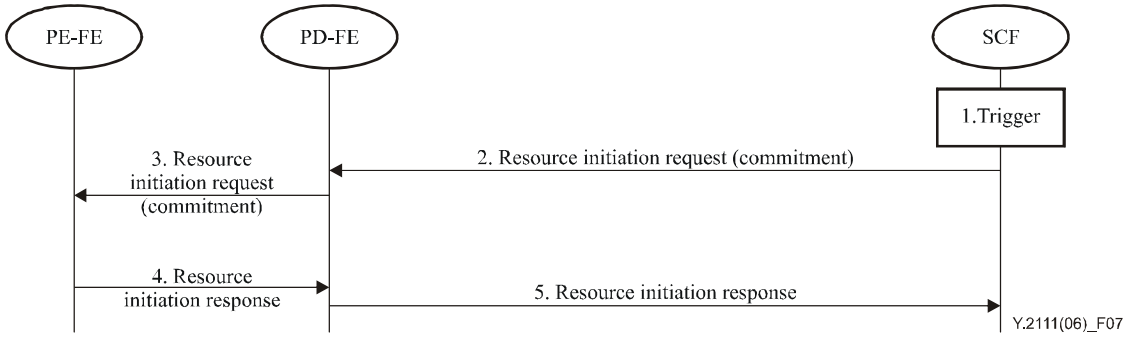


Figure 7/Y.2111 – Admission decision activation procedure

9.1.1.1.3 Admission decision de-activation procedure

The admission decision de-activation procedure illustrated in Figure 8 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.

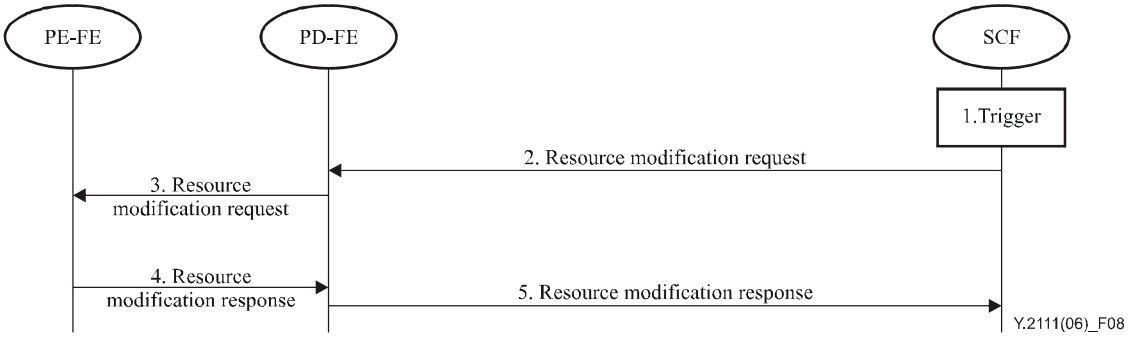


Figure 8/Y.2111 – Admission decision de-activation procedure

9.1.1.1.4 QoS resource modification procedure

The SCF-requested QoS resource modification procedure illustrated in Figure 9 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.

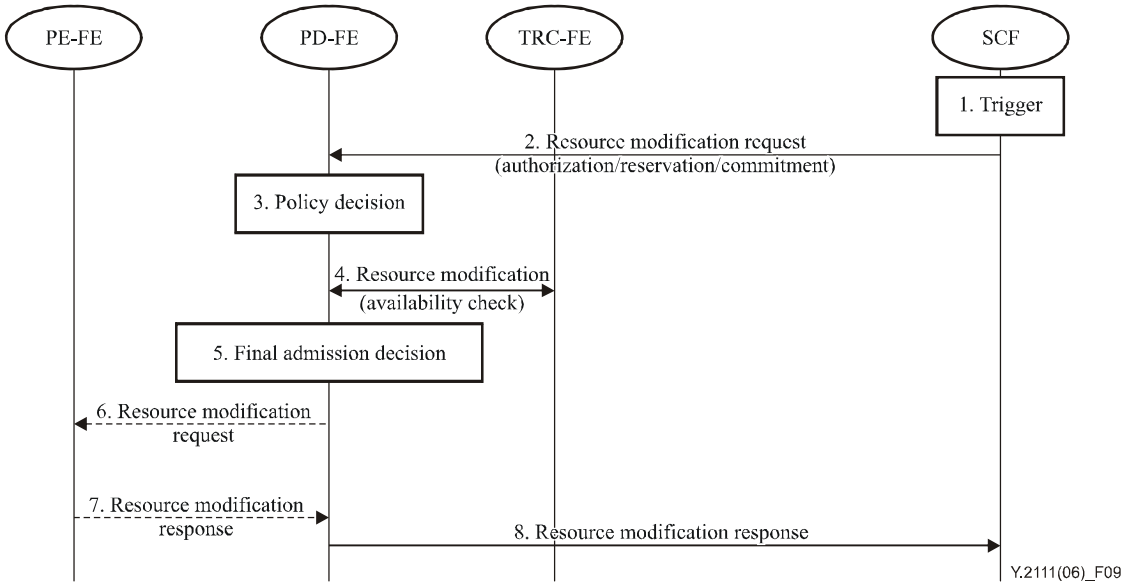


Figure 9/Y.2111 – SCF-requested QoS resource modification procedure

9.1.1.1.5 QoS resource release procedure

The SCF-requested QoS resource release procedure illustrated in Figure 10 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.

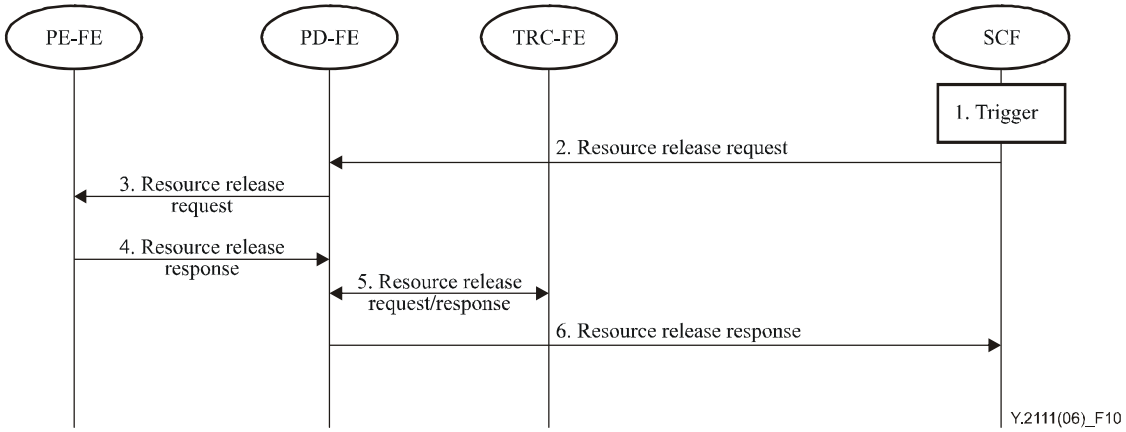


Figure 10/Y.2111 – SCF-requested QoS resource release procedure

9.1.1.2 Failure handling

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

9.1.1.2.1 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 shall send a resource notification to the PD-FE on its own initiative. The PD-FE shall forward the resource notification to the relevant SCF for alerting the affected sessions as illustrated in Figure 11.

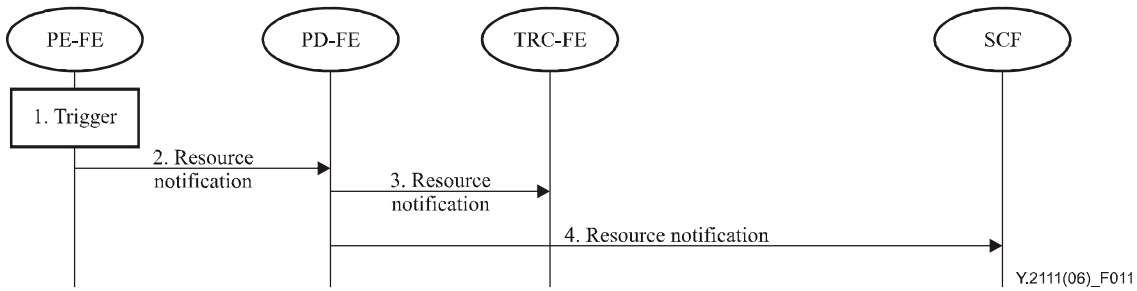


Figure 11/Y.2111 – PE-FE-indicated event notification procedure

9.1.1.2.2 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 shall send a resource notification to the PD-FE on its own initiative. The PD-FE shall 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 12.

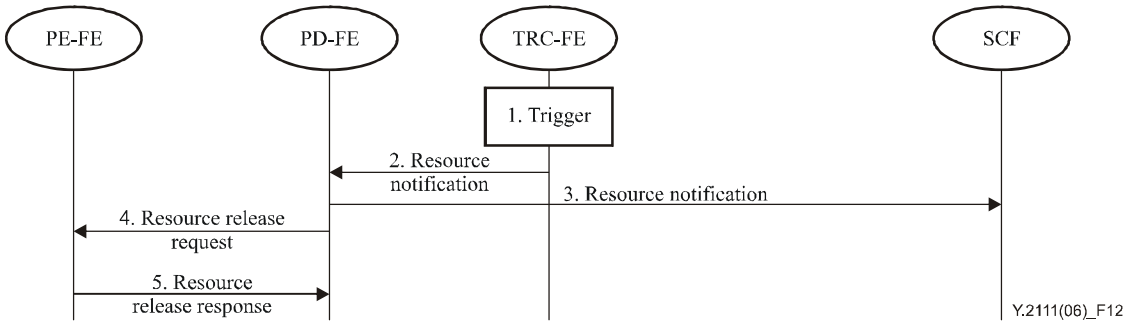


Figure 12/Y.2111 – TRC-FE-indicated event notification procedure

9.1.2 CPE-requested QoS control procedures

Scenario 2 described in 6.1 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.

9.1.2.1 Basic procedures

9.1.2.1.1 CPE-requested QoS resource reservation procedure

The CPE-requested QoS resource reservation procedure illustrated in Figure 13 is invoked by a dedicated path-coupled QoS signalling message from the CPE for a given flow.

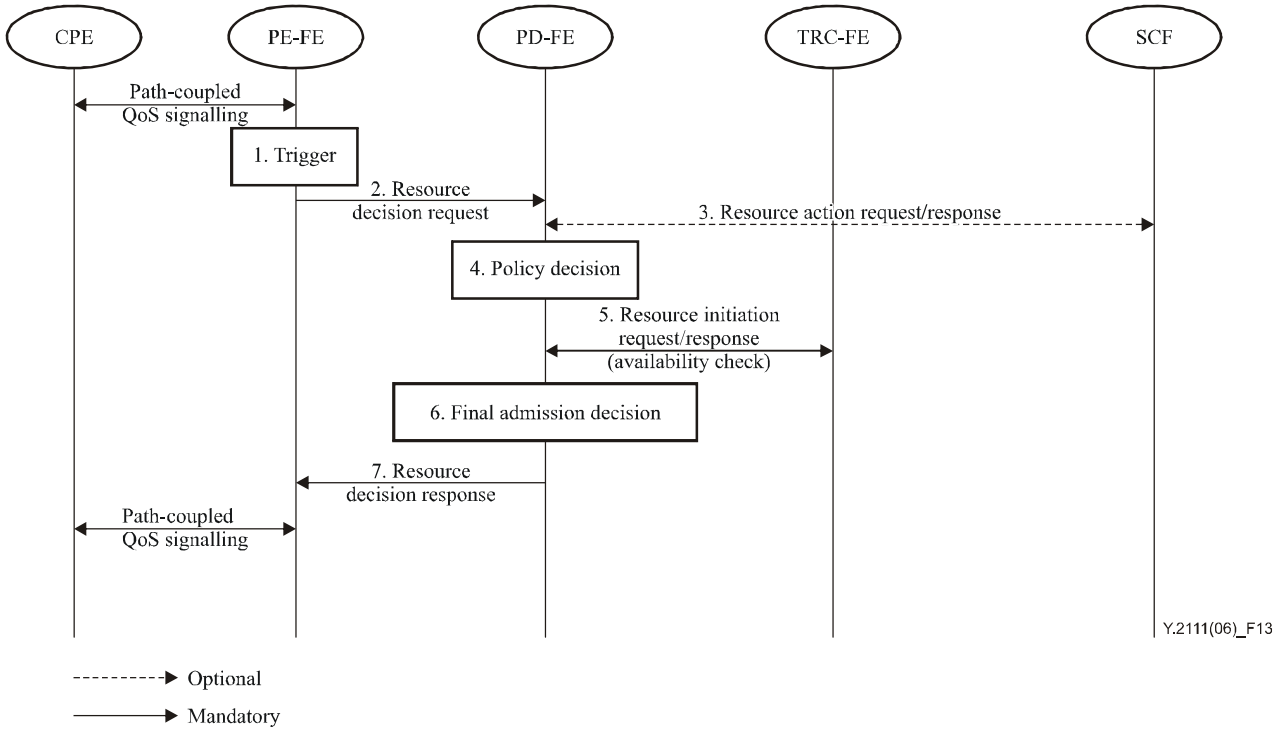


Figure 13/Y.2111 – CPE-requested QoS resource reservation procedure

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 sends a 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 shall 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 shall send a resource action request (i.e., RAR) to the SCF for retrieving the service information of the flow.

   The SCF-requested QoS initial authorization procedure is usually triggered by a service establishment signalling message. Optionally, the PD-FE may generate an authorization token for a given service and send it to the SCF. The SCF may forward the authorization token in the service signalling message to the CPE as illustrated in Figure 14.

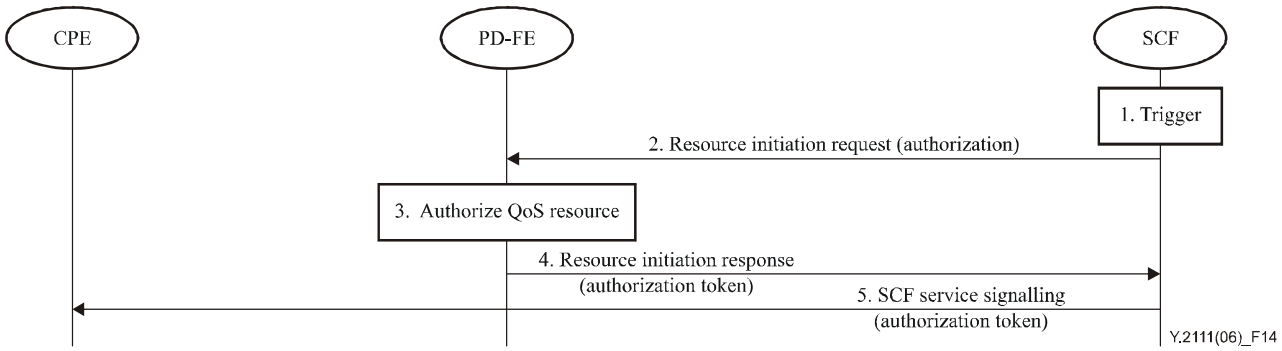


Figure 14/Y.2111 – SCF-requested QoS initial authorization procedure

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 a 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) shall send a RIP back to the PD-FE.

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 shall send a resource decision response (commitment) (i.e., RDP) to install the final admission decisions in the PE-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 15-a, -b and -c respectively. If processing in a proxy way, the PE-FE may modify, aggregate and de-aggregate the QoS signalling messages.

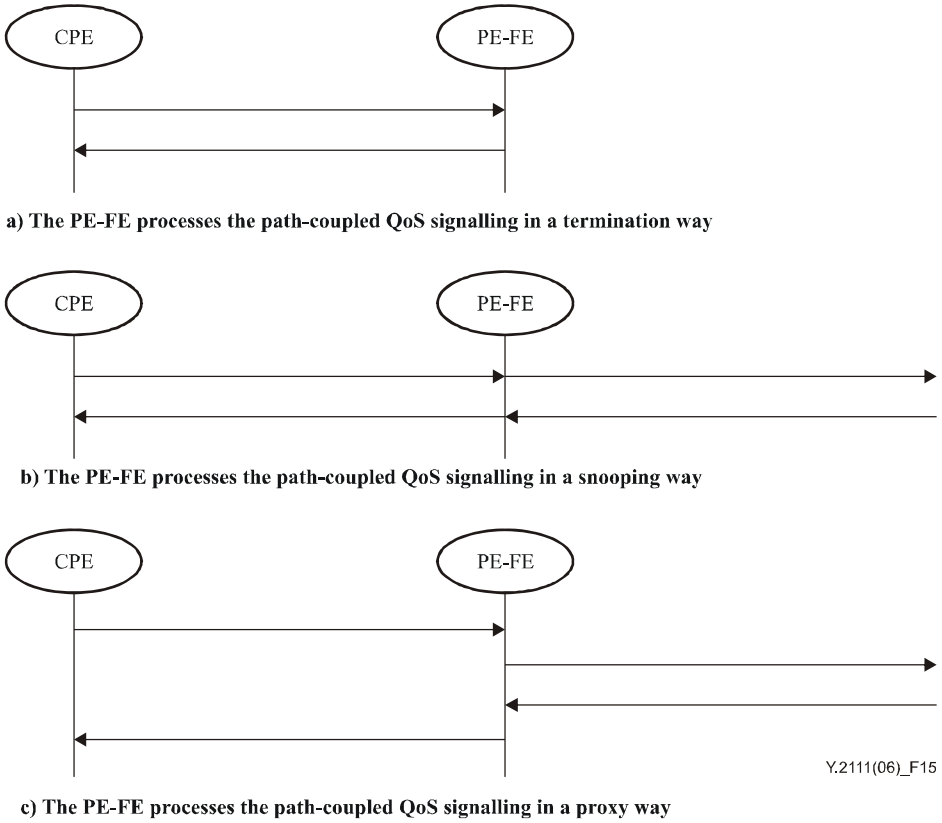


Figure 15/Y.2111 – Three possible QoS signalling processing ways at the PE-FE (not exhaustive)

9.1.2.1.2 CPE-requested QoS resource modification procedure

The CPE-requested QoS resource modification procedure illustrated in Figure 16 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.

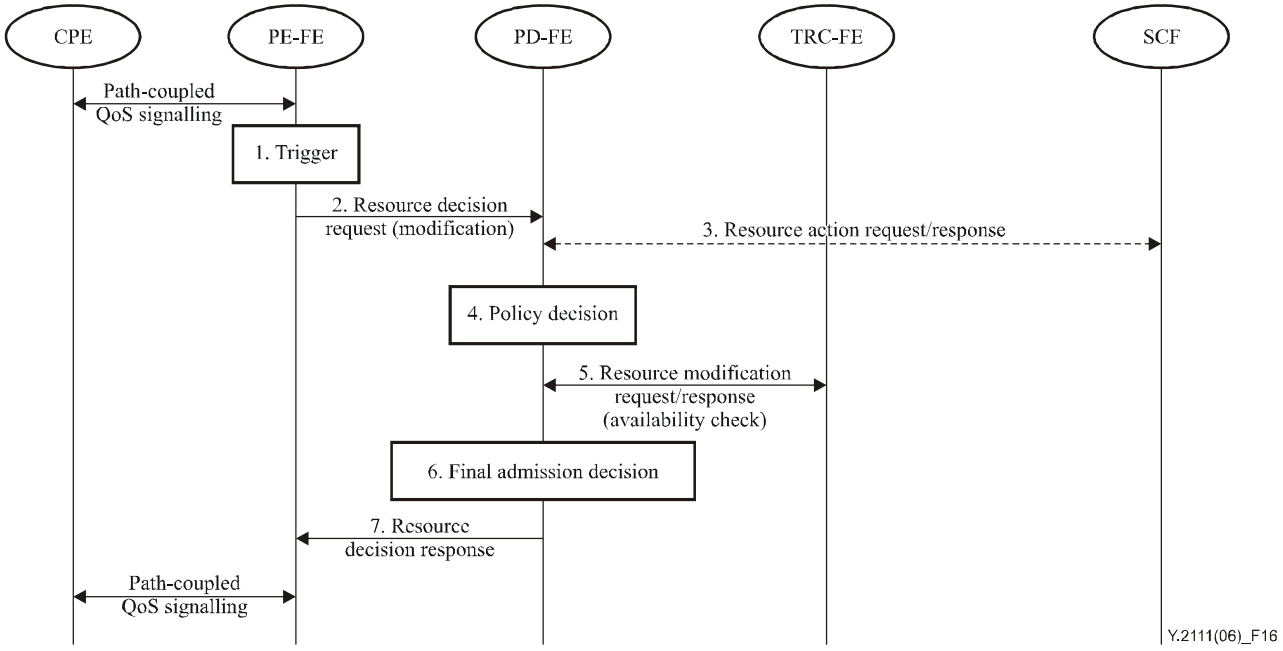


Figure 16/Y.2111 – CPE-requested QoS resource modification procedure

9.1.2.1.3 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 a RIR (commitment). The admission decision activation procedure is invoked by the RIR (commitment) from the SCF for a given service as illustrated in Figure 17.

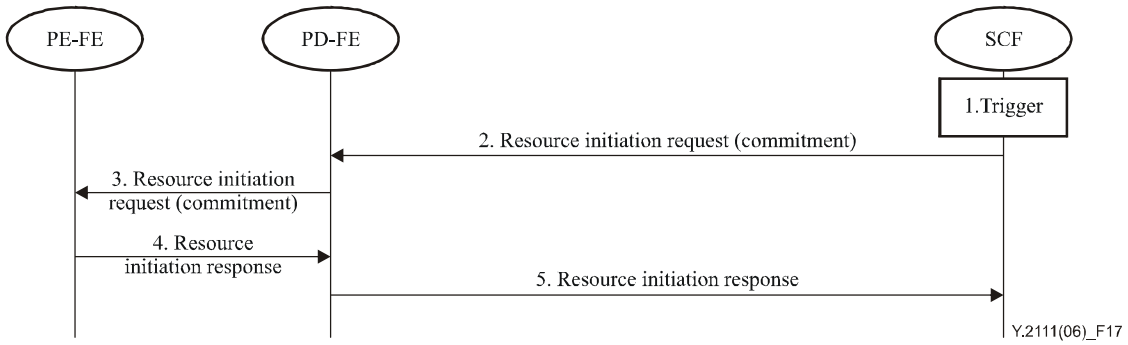


Figure 17/Y.2111 – Admission decision activation procedure

9.1.2.1.4 Admission decision de-activation procedure

The admission decision de-activation procedure illustrated in Figure 18 is invoked by a 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.

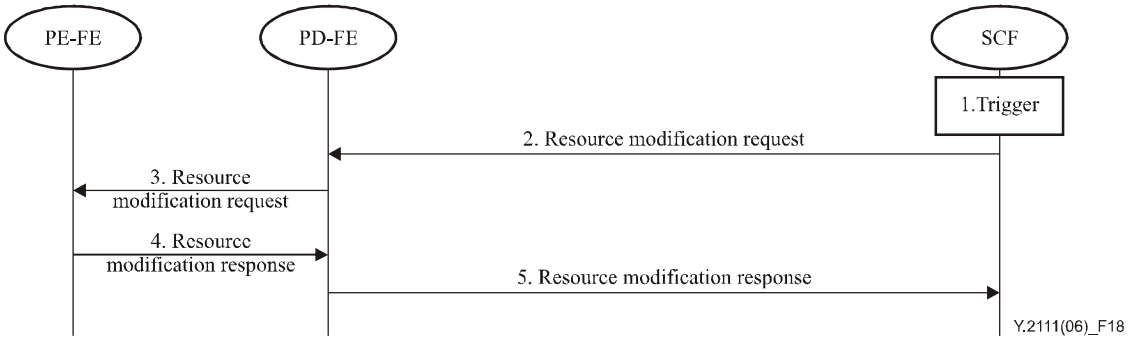


Figure 18/Y.2111 – Admission decision de-activation procedure

9.1.2.1.5 CPE-requested QoS resource release procedure

The CPE-requested QoS resource release procedure illustrated in Figure 19 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.

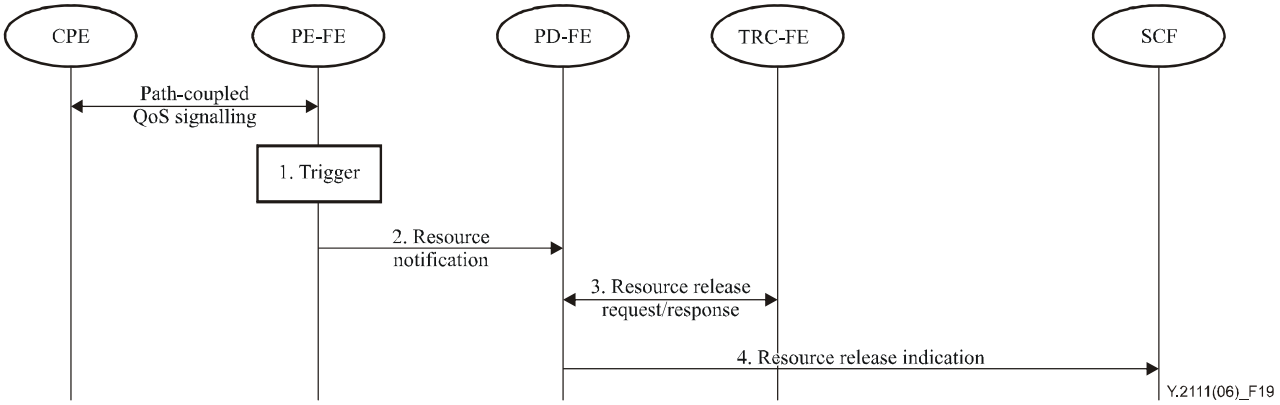


Figure 19/Y.2111 – CPE-requested QoS resource release procedure

9.1.2.1.6 SCF-requested QoS resource release procedure

The SCF-requested QoS resource release procedure illustrated in Figure 20 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.

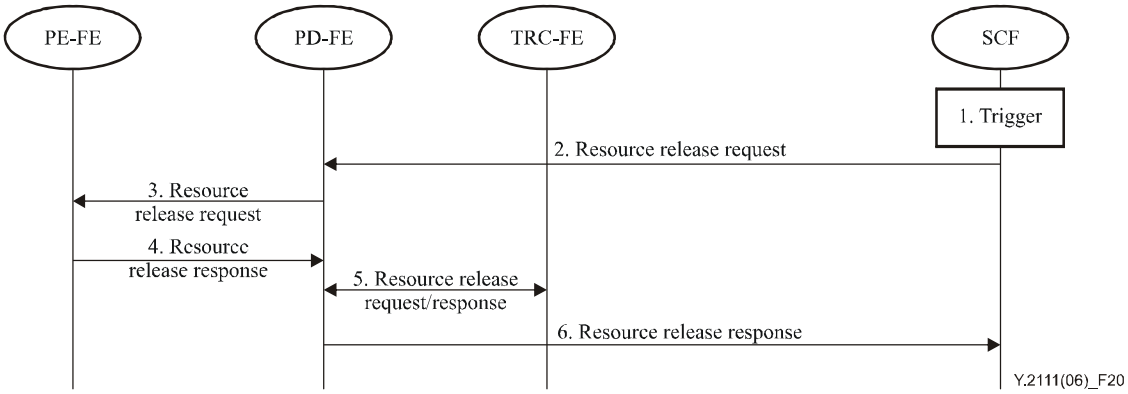


Figure 20/Y.2111 – SCF-requested QoS resource release procedure

9.1.2.2 Failure handling

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

9.1.2.2.1 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 shall 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 shall forward the Resource Notification to the SCF as illustrated in Figure 21.

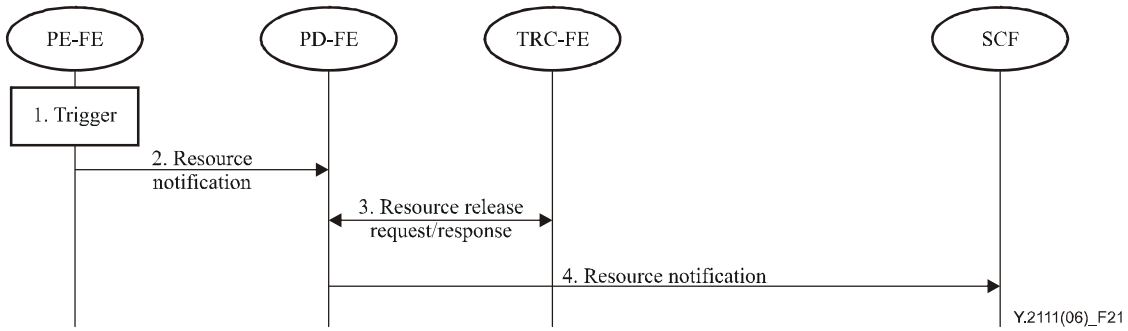


Figure 21/Y.2111 – PE-FE-indicated event notification procedure

9.1.2.2.2 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 shall 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 shall forward the RN to the SCF as illustrated in Figure 22.

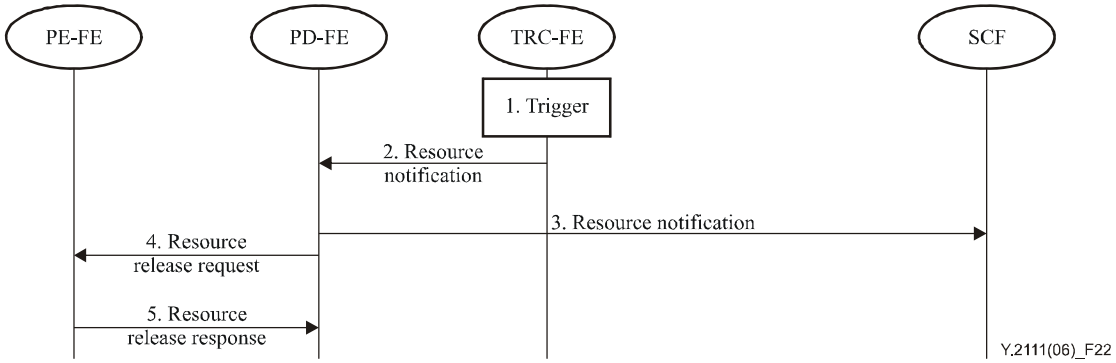


Figure 22/Y.2111 – TRC-FE-indicated event notification procedure

9.2 Procedures for NAPT control and NAT traversal

9.2.1 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 shall be invoked by RACF (e.g., PD-FE) based on the network security policy rules (e.g., network address hiding rules). The SCF shall 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 PD-FE. The PD-FE performs NAPT policy control, obtains the address binding information and performs the gate control to open/close the "gate".

9.2.1.1 Upon receipt of a session initiation request

1) The SCF shall extract the source and destination network addresses and port numbers from the signalling message body received from the calling party endpoint, shall send them to PD-FE, and shall 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 shall 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 shall locate the PE-FE based on the network address from the SCF and shall 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 shall obtain the public network address and port number from the public network address pool of this operator's network.

4) The PD-FE shall 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 shall return the network address binding information to the SCF.

5) Upon receipt of the RACF response, the SCF shall 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.

9.2.1.2 Upon the receipt of a session initiation response

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

2) Upon the receipt of source/destination network address and port and related information from the SCF, the PD-FE shall 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 shall 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 shall 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 shall return the network address binding information to the SCF. In the originating network, the PD-FE shall return the public network address binding information of selected PE-FE to the SCF. In the terminating network, the PD-FE shall return the network address binding information of selected PE-FE to the SCF.

5) Upon receipt of NAPT information from PD-FE, the SCF shall 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.

9.2.1.3 Upon receipt of media connection change request for an established session

The SCF shall 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) shall 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) shall be released by the SCF/RACF;

3) Network address(es) and port number(s) have been re-committed to the users: the binding(s) shall reflect the re-allocation;

4) No change has been made to the network address(es) and port number(s): no operation shall be conducted to the existing binding(s).

9.2.1.4 Upon receipt of a session release request

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

9.2.2 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.

9.2.2.1 NAT traversal procedure for signalling flows

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

The relevant operations shall be performed in the following stages as illustrated in Figure 23:

Registration

1) When the SCF receives a registration request, it shall 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.

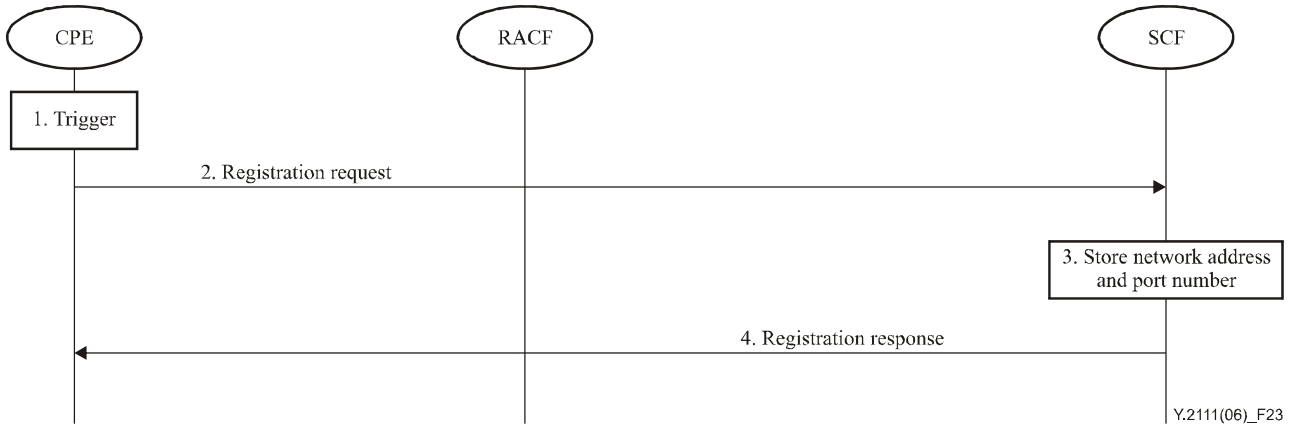


Figure 23/Y.2111 – NAT traversal procedure for signalling registration flows

Session Setup Process as illustrated in Figure 24

1) When a session setup request signalling message is received, the pertinent instance of SCF shall request the RACF to obtain public network address and port number, and shall 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 shall 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.

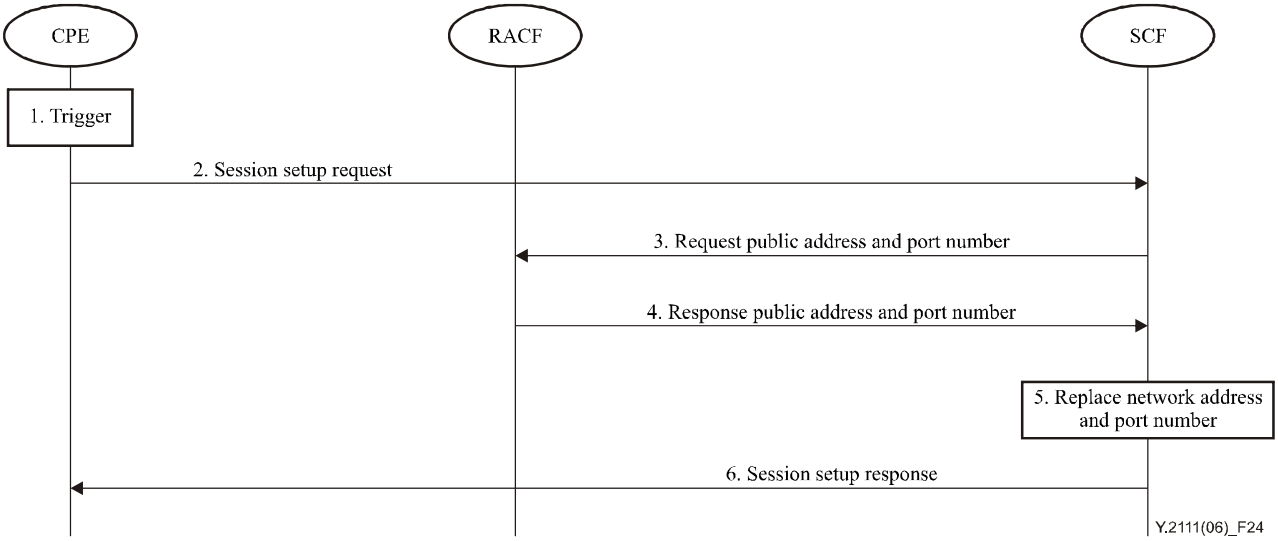


Figure 24/Y.2111 – NAT traversal procedure for signalling session setup flows

9.2.2.2 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 9.2.1. However, the NAT traversal procedure shall 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 shall 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 shall be controlled by the same procedure (e.g., RTP and RTCP for VoIP).

9.2.2.3 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 shall not 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 shall be used.

10 Inter-operator communications for end-to-end QoS control

There are two scenarios for passing the QoS information for a given service over an end-to-end path.

1) In scenario 1, the QoS requirements for a given service can be passed over the end-to-end path through application layer signalling or through the Ri reference point.

2) In scenario 2, the QoS requirements for a given service can be passed over the end-to-end path through path-coupled QoS signalling (e.g., RSVP-like).

In both scenarios, if the media flow is not transferred through a transit network owned by a third-party operator, inter-operator RACF communications may not be needed. Because application layer signalling or path-coupled QoS signalling can pass the QoS information between different operators' domains, the RACF in each operator's domain can work independently, without any inter-operator RACF communications via the Ri reference point.

However in scenario 1, if the media flow is transferred through a transit network owned by a third-party operator, the QoS information for a given service cannot be passed through application

layer signalling to the RACF in the transit network. The RACF in the transit network is required for the end-to-end QoS, but generally no application functions exist in the transit network. In this case, inter-operator RACF communications via the Ri reference point might be needed for invoking the RACF in the transit network with resource requests, see Figure 25.

In scenario 2, if the media flow is transferred through a transit network owned by a third-party operator, inter-operator RACF communications may also not be needed. Because path-coupled QoS signalling can pass the QoS information to the transit network, the RACF in each operator's domain can work independently, without any inter-operator RACF communications via the Ri reference point.

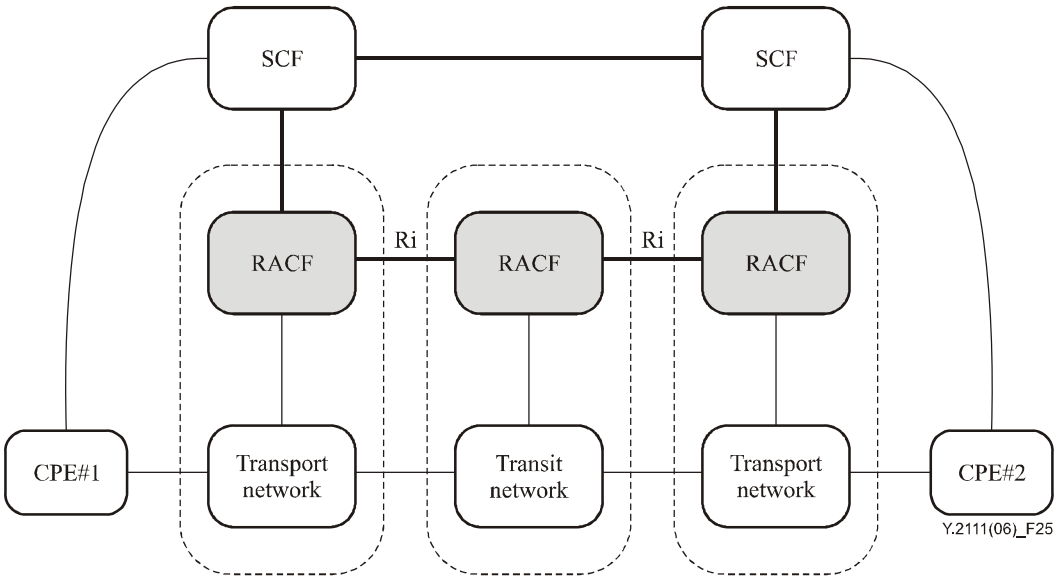


Figure 25/Y.2111 – Inter-operator RACF communications

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 [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) [RFC 2246] and IPsec [RFC 4301], [RFC 2403], [RFC 2404], [RFC 2405], [RFC 4304], [RFC 4305], [RFC 4307], [RFC 4308], [RFC 2410], and [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 [Y.2701]. In addition, networks can employ back-end authentication, authorization and accounting (AAA) servers, which keep the information necessary for these functions.

Denial of service (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 illegitimate access to RACF:

   - RACF shall take the threats identified in 11.1 into account, and must include measures to counter relevant attacks.
   - In particular, mechanisms must be explicitly defined for mitigation of the flooding attack. Even in the presence of a DoS attack, RACF must retain its availability.

- Any two entities located in different trust environments (e.g., PD-FE and SCF) must 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 RACF or any of its components is replicated, an entity that communicates with any such replica must use the same authentication information. With that, an eavesdropper must be unable to repeat a recorded authentication handshake with another replica.
- During the association, all messages must 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 must be protected. The decisions should be made for specific reference points and they should leave open a choice of standard cryptographic algorithms to be used in support of confidentiality or integrity.
- Non-repudiation must be supported for all requests (unless specifically overridden by a PD-FE policy rule in effect).
- A reference point between untrusted domains should make use of commonly used firewall functions.
- Except for the DoS *flooding* attack, which is systemic, the above requirements must be implemented using existing secure-channel mechanisms such as TLS or IPsec (or both) to ensure that well-tested security mechanisms are used.

Appendix I

Examples of the implementation of the RACF architecture

This appendix provides examples of the 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 (Figure I.1). Another is the approach in which the RACF performs the QoS coordination at the RACF level without the intermediation of the SCF (Figure I.2). There is also a specific case where both access and core networks are managed by the same operator (Figure I.3). The implementation and physical configuration of 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.

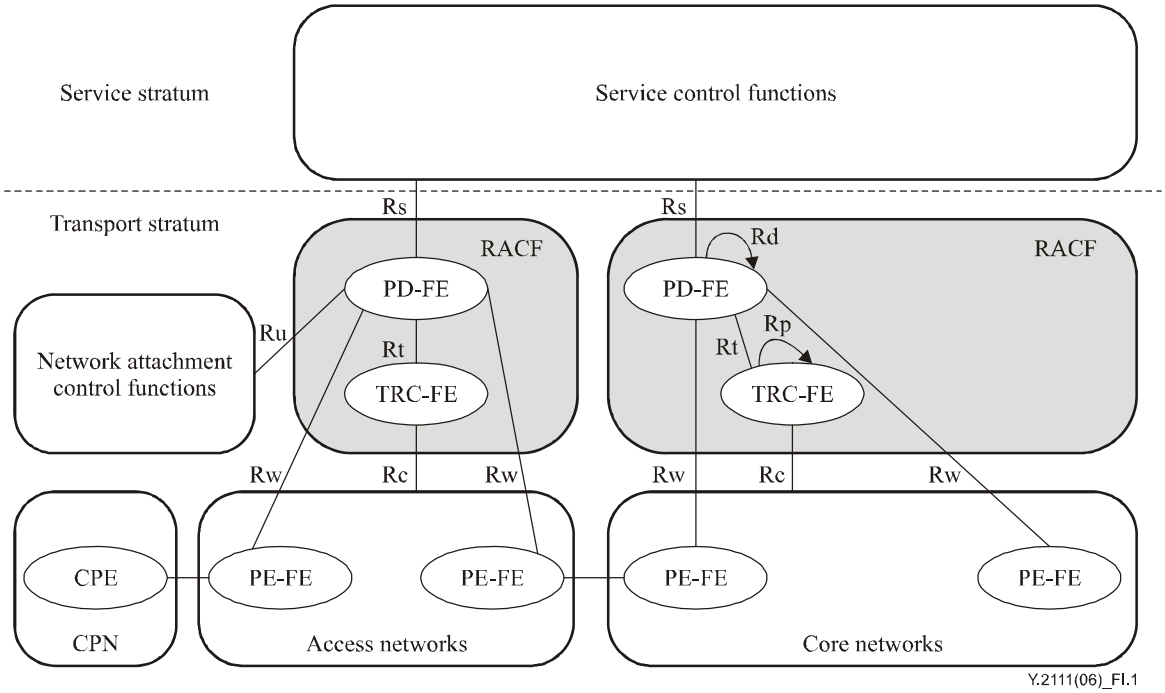


Figure I.1/Y.2111 – Example 1

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 interface are for further study.

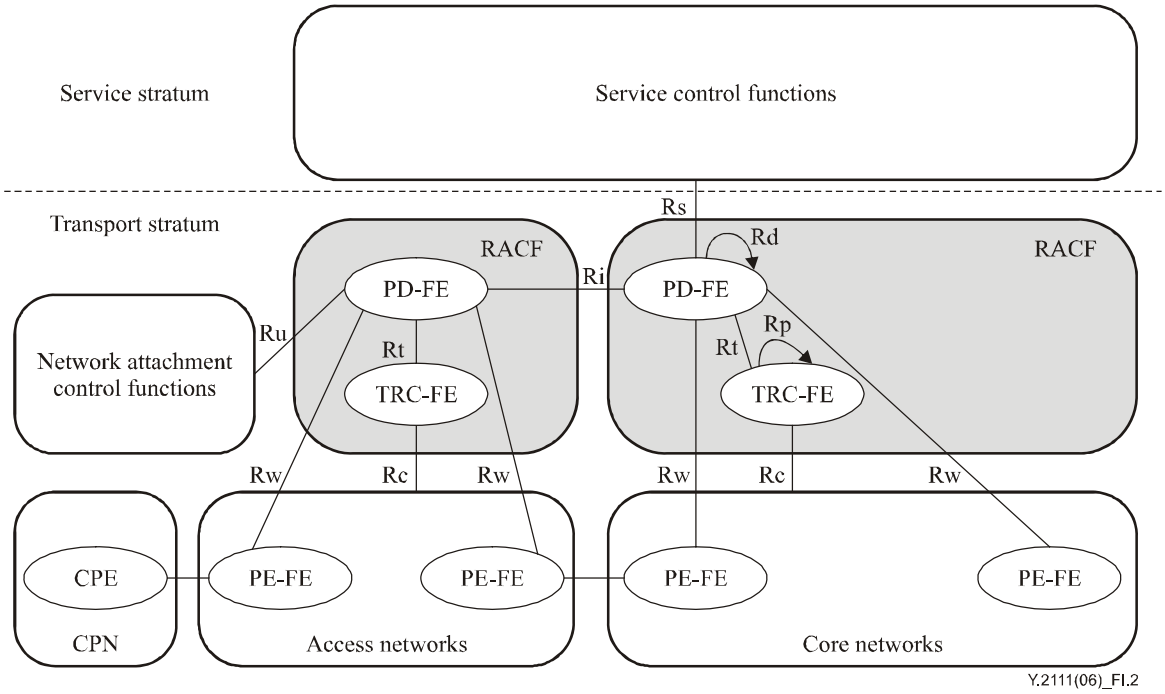


Figure I.2/Y.2111 – Example 2

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.

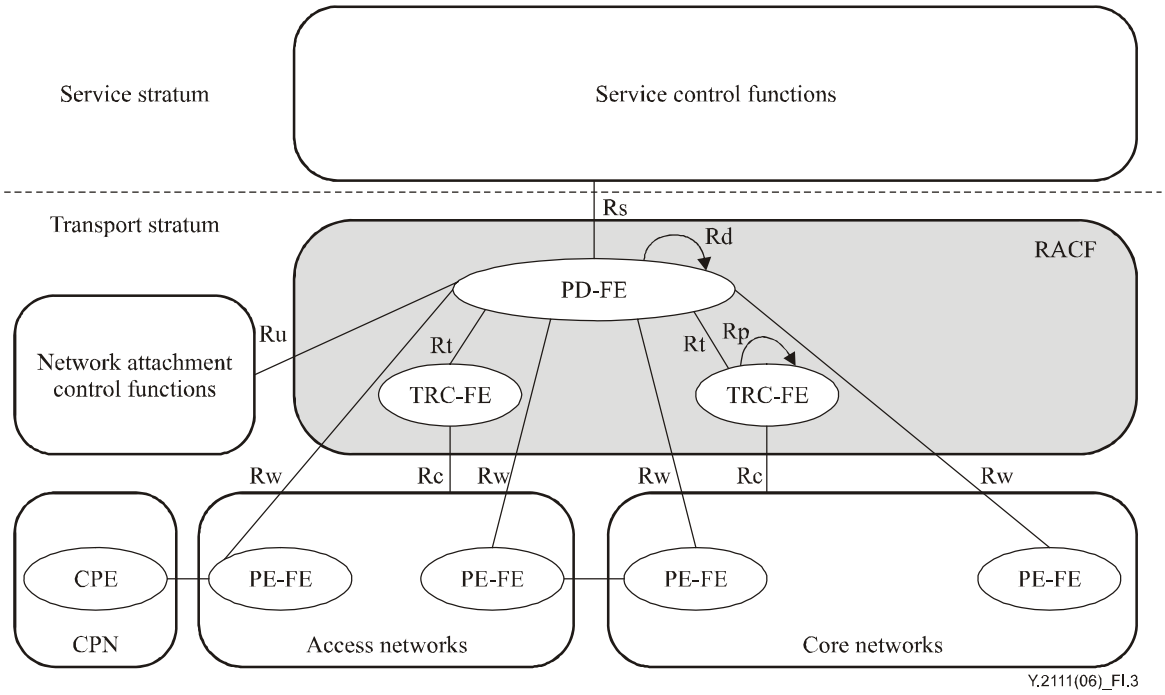


Figure I.3/Y.2111 – Example 3

Appendix II

TRC-FE over different transport technologies

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

II.1 TRC-FE over 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 [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 TRC-FE over 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 protocol. (Diffserv-aware) MPLS TE [RFC 2702], [RFC 3272], [RFC 3346], [RFC 3564] and [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 a network topology and resource database (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 TRC-FE over 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 network topology and resource database (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 TRC-FE over 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 setup bandwidth request uplink information. The QoS classes for QoS signalling define four QoS services: unsolicited grant service (UGS) used for CBR-like service flows, real-time polling service (rtPS) used for rt-VBR-like service flows, non-real-time polling service (nrtPS) used for non-real-time service flows, and best effort service (BE). 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 a network topology and resource database (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 resource database (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 TRC-FE

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 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 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.

BIBLIOGRAPHY

[Q.Sup51] ITU-T Q-series Supplement 51 (2004), *Signalling requirements for IP-QoS*.

[Y.1221] ITU-T Recommendation Y.1221 (2002), *Traffic control and congestion control in IP-based networks*.

[Y.1541] ITU-T Recommendation Y.1541 (2006), *Network performance objectives for IP-based services*.

[Y.2171] ITU-T Recommendation Y.2171 (2006), *Admission control priority levels in Next Generation Networks*.

[Y.2701] *Draft ITU-T Recommendation Y.2701, Security requirements for NGN release 1 (http://www.itu.int/md/T05-SG13-R-0024/en).*

[RFC 2205] IETF RFC 2205 (1997), *Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification*.

[RFC 2246] IETF RFC 2246 (1999), *The TLS Protocol Version 1.0*.

[RFC 2403] IETF RFC 2403 (1998), *The Use of HMAC-MD5-96 within ESP and AH*.

[RFC 2404] IETF RFC 2404 (1998), *The Use of HMAC-SHA-1-96 within ESP and AH*.

[RFC 2405] IETF RFC 2405 (1998), *The ESP DES-CBC Cipher Algorithm With Explicit IV*.

[RFC 2410] IETF RFC 2410 (1998), *The NULL Encryption Algorithm and Its Use With IPsec*.

[RFC 2412] IETF RFC 2412 (1998), *The OAKLEY Key Determination Protocol*.

[RFC 2475] IETF RFC 2475 (1998), *An Architecture for Differentiated Services*.

[RFC 2702] IETF RFC 2702 (1999), *Requirements for Traffic Engineering Over MPLS*.

[RFC 3261] IETF RFC 3261 (2002), *SIP: Session Initiation Protocol*.

[RFC 3272] IETF RFC 3272 (2002), *Overview and Principles of Internet Traffic Engineering*.

[RFC 3312] IETF RFC 3312 (2002), *Integration of Resource Management and Session Initiation Protocol (SIP).*

[RFC 3346] IETF RFC 3346 (2002), *Applicability Statement for Traffic Engineering with MPLS.*

[RFC 3520] IETF RFC 3520 (2003), *Session Authorization Policy Element.*

[RFC 3564] IETF RFC 3564 (2003), *Requirements for Support of Differentiated Services-aware MPLS Traffic Engineering.*

[RFC 4124] IETF RFC 4124 (2005), *Protocol Extensions for Support of Diffserv-aware MPLS Traffic Engineering*.

[RFC 4301] IETF RFC 4301 (2005), *Security Architecture for the Internet Protocol.*

[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).*

[RFC 4305] IETF RFC 4305 (2005), *Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH).*

[RFC 4306] IETF RFC 4306 (2005), *Internet Key Exchange (IKEv2) Protocol*.

[RFC 4307] IETF RFC 4307 (2005), *Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2).*

[RFC 4308] IETF RFC 4308 (2005), *Cryptographic Suites for IPsec*.

[RFC 4566] IETF RFC 4566 (2006), *SDP: Session Description Protocol*.

[TS 123 207] ETSI TS 123 207 V6.6.0 (2005), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); End-to-end Quality of Service (QoS) concept and architecture*.

[TS 123 228] ETSI TS 123 228 V7.3.0 (2006), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); IP Multimedia Subsystem (IMS); Stage 2*.

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	Telephone transmission quality, telephone installations, local line networks
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, 2007