

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.3303.3

(08/2013)

SERIES Q: SWITCHING AND SIGNALLING

Signalling requirements and protocols for the NGN –
Resource control protocols

**Resource control protocol No. 3 – Protocols at
the Rw interface between a policy decision
physical entity (PD-PE) and a policy
enforcement physical entity (PE-PE): Diameter
profile version 3**

Recommendation ITU-T Q.3303.3



International
Telecommunication
Union
Documents

Document Sharing Hub

ITU-T Q-SERIES RECOMMENDATIONS
SWITCHING AND SIGNALLING

SIGNALLING IN THE INTERNATIONAL MANUAL SERVICE	Q.1–Q.3
INTERNATIONAL AUTOMATIC AND SEMI-AUTOMATIC WORKING	Q.4–Q.59
FUNCTIONS AND INFORMATION FLOWS FOR SERVICES IN THE ISDN	Q.60–Q.99
CLAUSES APPLICABLE TO ITU-T STANDARD SYSTEMS	Q.100–Q.119
SPECIFICATIONS OF SIGNALLING SYSTEMS No. 4, 5, 6, R1 AND R2	Q.120–Q.499
DIGITAL EXCHANGES	Q.500–Q.599
INTERWORKING OF SIGNALLING SYSTEMS	Q.600–Q.699
SPECIFICATIONS OF SIGNALLING SYSTEM No. 7	Q.700–Q.799
Q3 INTERFACE	Q.800–Q.849
DIGITAL SUBSCRIBER SIGNALLING SYSTEM No. 1	Q.850–Q.999
PUBLIC LAND MOBILE NETWORK	Q.1000–Q.1099
INTERWORKING WITH SATELLITE MOBILE SYSTEMS	Q.1100–Q.1199
INTELLIGENT NETWORK	Q.1200–Q.1699
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR IMT-2000	Q.1700–Q.1799
SPECIFICATIONS OF SIGNALLING RELATED TO BEARER INDEPENDENT CALL CONTROL (BICC)	Q.1900–Q.1999
BROADBAND ISDN	Q.2000–Q.2999
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR THE NGN	Q.3000–Q.3999
General	Q.3000–Q.3029
Network signalling and control functional architecture	Q.3030–Q.3099
Network data organization within the NGN	Q.3100–Q.3129
Bearer control signalling	Q.3130–Q.3179
Signalling and control requirements and protocols to support attachment in NGN environments	Q.3200–Q.3249
Resource control protocols	Q.3300–Q.3369
Service and session control protocols	Q.3400–Q.3499
Service and session control protocols – supplementary services	Q.3600–Q.3649
NGN applications	Q.3700–Q.3849
Testing for next generation networks	Q.3900–Q.3999

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

Recommendation ITU-T Q.3303.3

Resource control protocol No. 3 – Protocols at the Rw interface between a policy decision physical entity (PD-PE) and a policy enforcement physical entity (PE-PE): Diameter profile version 3

Summary

Recommendation ITU-T Q.3303.3 provides the stage 3 specification of the interface between policy decision physical entities (PD-PE) and the policy enforcement physical entity (PE-PE) using the Diameter protocol. The functional requirements and the stage 2 specification for this interface are defined in Recommendation ITU-T Y.2111. The Diameter profile version 3 specified in this document has additional attribute-value pairs to comply with the additional requirements indicated in Recommendation ITU-T Y.2111 (2011) and support emergency telecommunication service (ETS) requirements.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T Q.3303.3	2008-05-22	11
2.0	ITU-T Q.3303.3 v2	2012-02-06	11
3.0	ITU-T Q.3303.3 v3	2013-08-13	11

Keywords

AVP, diameter, RACF, Rw.

FOREWORD

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

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

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

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

NOTE

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

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

INTELLECTUAL PROPERTY RIGHTS

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

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

© ITU 2014

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

Table of Contents

		Page
1	Scope	1
2	References.....	1
3	Definitions	2
	3.1 Terms defined elsewhere	2
	3.2 Terms defined in this Recommendation.....	2
4	Abbreviations and acronyms	3
5	Rw interface.....	5
	5.1 Policy definition and operations.....	5
6	Resource control procedures.....	7
	6.1 SCE-requested resource control procedures.....	7
	6.2 UE-requested resource control procedures.....	15
	6.3 Emergency telecommunications service support	18
7	Rw protocol specification	19
	7.1 Protocol support.....	19
	7.2 Use of the Diameter base protocol	19
	7.3 AVPs.....	20
	7.4 Commands.....	46
	7.5 State machine.....	50
	Bibliography.....	52

Recommendation ITU-T Q.3303.3

Resource control protocol No. 3 – Protocols at the Rw interface between a policy decision physical entity (PD-PE) and a policy enforcement physical entity (PE-PE): Diameter profile version 3

1 Scope

This Recommendation provides the stage 3 specification of the protocol at the interface between a policy decision physical entity (PD-PE) and a policy enforcement physical entity (PE-PE). The functional requirements and the stage 2 specifications for this interface are contained in clause 9.2 of [ITU-T Y.2111] and in [b-ITU-T Q-Sup.51].

This interface is used to control policy enforcement functions in the transport devices, including QoS resource control (e.g., packet marking, filtering and policing), gate control, and network address and port translation/network address translation (NAPT/NAT) traversal control. The PE-PE may reside in any injection node across access networks, core networks and the network border gateway.

This Recommendation defines:

- The information to be exchanged between the PD-PE and the PE-PE over the Rw interface.
- An Rw interface definition based on the Diameter protocol.

2 References

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

- [ITU-T Q.3301.1 v3] Recommendation ITU-T Q.3301.1 v3 (2013), *Resource control protocol No. 1, version 3 – Protocol at the Rs interface between service control entities and the policy decision physical entity*.
- [ITU-T Y.2111] Recommendation ITU-T Y.2111 (2011), *Resource and admission control functions in next generation networks*.
- [ETSI TR 121 905] ETSI TR 121 905 V10.3.0 (2011), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Vocabulary for 3GPP Specifications (3GPP TR 21.905 version 10.3.0 Release 10)*
- [IETF RFC 2474] IETF RFC 2474 (1998), *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*.
- [IETF RFC 3520] IETF RFC 3520 (2003), *Session Authorization Policy Element*.
- [IETF RFC 4005] IETF RFC 4005 (2005), *Diameter Network Access Server Application*.
- [IETF RFC 4006] IETF RFC 4006 (2005), *Diameter Credit-Control Application*.
- [IETF RFC 4960] IETF RFC 4960 (2007), *Stream Control Transmission Protocol*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following term defined elsewhere:

3.1.1 attribute-value pair (AVP) [IETF RFC 6733]: An attribute-value pair corresponds to an Information Element in a Diameter message.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 binding: The process of associating the resource request for IP media flows with pertinent resource control session and policy decisions according to the information received from the UE or the service control entity (SCE).

NOTE – The binding may be performed in the PE-PE and/or the PD-PE based on the resource control mode (i.e., push or pull modes).

3.2.2 hard-state reservation: A type of reservation whereby the requested resources are reserved without a time limit.

3.2.3 IP media flow: A unidirectional flow of IP packets pertaining to a certain media type with the same source IP address, source port number, destination IP address, destination port number and the same transport protocol. Port numbers are only applicable if used by the transport protocol.

3.2.4 policy configuration: A set of policy rules (conditions and actions) predefined by network operators, which does not vary from the individual resource request.

3.2.5 policy decision: A set of filters and parameters specific to the enforcement of resource control results on IP media flow, which is produced on a per session basis upon receipt of the resource control request from the SCE or the PE-PE.

3.2.6 resource control policy: A set of rules concerning the conditions and actions of resource control operations. The rule-sets can be provisioned by the network operator manually or automatically.

3.2.7 resource control session: A session established by the PD-PE upon the trigger from a service/session control signalling protocol that requires a service layer session set-up with explicit session description before the use of the service; or by the PE-PE upon the trigger from a transport signalling protocol that requires a transport layer session set-up with explicit session description before the use of the service.

3.2.8 resource information: A set of information collected from the transport networks to be used as a basis for resource admission decisions at the transport resource control physical entity (TRC-PE), including information about the network resource status (e.g., resource utilization, network topology and connectivity).

NOTE – The resource admission decisions are used as a basis for quality of service (QoS) resource requirements in the process of policy decisions at the PD-PE.

3.2.9 service information: A set of information conveyed from the SCE to the PD-PE over the Rs interface to be used as a basis for the UE service-based resource requirements of in the process of policy decisions at the PD-PE, including information about the SCE session (e.g., application identifier, type of media, bandwidth, IP address and port number).

3.2.10 service signalling protocol: The signalling protocol used to control the service layer session.

NOTE – One example of a service signalling protocol is session initiation protocol (SIP) with session description protocol (SDP).

3.2.11 soft-state reservation: A type of reservation whereby the requested resources are reserved for a finite amount of time.

3.2.12 transport bearer: A transport layer connection of defined QoS characteristics (e.g., bandwidth, delay and bit error rate).

NOTE – One example of a transport bearer is the IP-connectivity access network (IP-CAN) bearer in general packet radio service (GPRS) access networks (see [ETSI TR 121 905] for the definition of bearer) or the multi-protocol label switching (MPLS) label switched path (LSP) in core networks. A transport bearer may incorporate one or more IP media flows according to certain criteria e.g., transport QoS class.

3.2.13 transport signalling protocol: The signalling protocol used to control the transport layer session.

NOTE – One example of a transport signalling protocol is the packet data protocol (PDP) context within a GPRS access network.

3.2.14 transport subscription information: A set of information received from the network attachment control functions (NACF) to the PD-PE over the Ru interface to be used as a basis for verification of the UE transport service profile in the process of policy decisions at the PD-PE, including information about the UE transport profile (e.g., maximum bandwidth, transport service class).

3.2.15 UE transport session: The association between a user equipment (UE) and a transport stratum.

NOTE – The association is identified by a UE IP address together with a UE's identity information, if available. A UE transport session may incorporate one or more transport bearers. Support for multiple transport bearers per UE transport session is transport specific. A UE transport session exists for as long as the UE IP address is assigned and announced to the IP network. One example of a UE transport session is the IP-CAN session in certain access networks (e.g., GPRS).

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AAA	AA-Answer
AAR	AA-Request
APN	Access Point Name
ARP	Allocation and Retention Priority
ASA	Abort-Session-Answer
ASR	Abort-Session-Request
AVP	Attribute-Value Pair
BGW	Border Gateway
BRAS	Broadband Remote Access Server
CCA	Credit-Control-Answer
CCR	Credit-Control-Request
CDMA	Code Division Multiple Access
CEA	Capabilities-Exchange-Answer

Copyrighted material

CER	Capabilities-Exchange-Request
CMTS	Cable Modem Termination System
DSL	Digital Subscriber Line
DSLAM	DSL Access Multiplexer
ETS	Emergency Telecommunications Service
EPS	Evolved Packet System
GCID	GPRS Charging ID
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
IANA	Internet Assigned Numbers Authority
ICID	IMS Charging Identifier
IMS	IP Multimedia Subsystem
IP-CAN	IP-Connectivity Access Network
LSP	Label Switched Path
MPLS	Multi-Protocol Label Switching
NACE	Network Attachment Control Entity
NACF	Network Attachment Control Functions
NAPT	Network Address and Port Translation
NAT	Network Address Translation
NASREQ	Network Access Server Requirements
PCC	Policy and Charging Control
P-CSCF	Proxy-Call Session Control Function
PDG	Packet Data Gateway
PDP	Packet Data Protocol
PD-PE	Policy Decision Physical Entity
PDSN	Packet Data Serving Node
PE-PE	Policy Enforcement Physical Entity
PIA	Policy-Install-Answer
PIR	Policy-Install-Request
QoS	Quality of Service
RAA	Re-Auth-Answer
RACF	Resource and Admission Control Function
RAR	Re-Auth-Request
RTCP	Real-time Transport Control Protocol
SCE	Service Control Entity
SDI	Session Description Information
SDP	Session Description Protocol

SGSN	Serving GPRS Support Node
SIP	Session Initiation Protocol
STA	Session-Termination-Answer
STR	Session-Termination-Request
TFT	Traffic Flow Template
UE	User Equipment

5 **Rw interface**

5.1 **Policy definition and operations**

5.1.1 **Policy decision and policy configuration**

Dynamic policy decision and static policy configuration are defined in clause 7.1.1 of [ITU-T Y.2111]:

- Dynamic policy decision: A set of filters and parameters specific to the enforcement of resource control results on individual IP media flow, which is produced on a per session basis upon receipt of the resource control request.
- Static policy configuration: A set of policy rules (conditions and actions) predefined by network operators, which does not vary from the individual resource request.

Both dynamic policy decision and static policy configuration are organized in the following format:

- Rule name.
- Rule precedence.
- IP media flow description (e.g., IP 5-tuple (port number can be a range) and direction).
- Quality of service (QoS) information (e.g., authorized bandwidth, QoS class) (see Notes).
- Resource control actions (e.g., open or closed).
- NAT traversal/NAPT information (e.g., address latching, address translation information).
- Charging correlation information.
- Usage metering and statistics reporting.
- Firewall working mode (see Notes).

NOTE 1 – Certain QoS information, charging correlation information and firewall working mode can be a form of predefined policy rules or received from the Rs interface.

NOTE 2 – Within the context of the ETSI policy and charging control (PCC) architecture, the above information elements are implemented as the PCC rule parameters. The rule name is used to identify a set of predefined static policy configuration or a set of dynamic policy decisions between the PD-PE and the PE-PE.

The rule precedence indicates which of these rules is applicable in the case of different policy rules with an overlapping IP media flow filter. The rule precedence is configured by the network operator according to the network policy. If the predefined static policy configuration and dynamic policy decision are with an overlapping IP media flow filter, the dynamic policy decision shall override the predefined static policy configuration independent of rule procedure.

The IP media flow description describes packet filters that policy decisions (e.g., gate operation, QoS, NAPT control and charging correlation information) are applied to. The description shall contain IP address information and direction, e.g., IP 5-tuple (the port number can be a range, and source or destination IP address can be wildcarded). In addition, it may identify the service or the

service component, e.g., HTTP or RTP for specific functions, such as for flow based charging or deep packet inspection.

The QoS information describes requested QoS resources, e.g., authorized bandwidth and QoS class, which is used for resource allocation, packet marking and policing. Certain QoS information can be a set of policy rules predefined by the network operator. The QoS information includes the QoS class identifier (authorized QoS class for the service data flow), the allocation and retention priority (ARP) and the authorized bitrates for uplink and downlink.

The resource control actions indicate the resource reservation and gate operation. For example, when the flow status is "disabled" in the initiation command, the PE-PE shall reserve the requested resource only; when the flow status is "enabled" in the initiation command, the PE-PE shall commit the requested resource and pass through the packets matching the filters (i.e., open the gate).

The NAT traversal/NAPT information indicates the corresponding actions and information (e.g., address latching and address translation information) if the far-end NAT and/or near-end NAPT are enabled.

The charging correlation information may include SCE record information for enabling charging correlation between the service and transport layer if the SCE has provided this information via the Rs interface. For IP multimedia subsystem (IMS), this includes the IMS charging identifier (ICID) and flow identifiers. The usage metering and statistics reporting provide information about the duration of the time, the number of octets sent and received for a transport session and/or an IP media flow. The "number of octets" excludes all transport overheads; i.e., IP header and transport protocol (e.g., TCP, UDP) header information is excluded.

The firewall working mode specifies the level of packet filtering operation for an IP media flow, a transport bearer and/or a user equipment (UE) transport session.

5.1.2 Policy operations

Policy operations shall support the installation, activation, modification and deactivation/termination of dynamic policy decisions, and may support the installation, activation, update and deactivation/termination of static policy configurations.

Installation of dynamic policy decisions provides the information of policy decisions to the PE-PE via the Rw interface, which may enable the resource reservation only without immediate resource commitment (i.e., non-gate opening).

Activation of dynamic policy decisions provides the enabling information of policy decisions to the PE-PE via the Rw interface, which may enable the resource commitment (i.e., open the gate). Based on the resource request from the SCE and/or network policies, the installation and activation (i.e., reservation and commitment as defined in [ITU-T Y.2111]) can be performed together or separately.

Modification of dynamic policy decisions provides the modified information of policy decisions to the PE-PE via the Rw interface, which may change the actions of an active resource control session immediately.

The deactivation/termination of dynamic policy decisions provides the disabling information of policy decisions to the PE-PE via the Rw interface, which may revoke an active resource control session.

The activation and deactivation of predefined policy configurations provide an identifier of the relevant rule to the PE-PE via the Rw interface to enable and disable the policy rules.

The installation and update of predefined policy configurations provides an identifier with the relevant rules to the PE-PE via the Rw interface. The alternative is to use the provisioning approach for static policy configuration; the provisioning approach is outside the scope of this Recommendation.

When an IP media flow is terminated by the PE-PE or UE, all active policy decisions and static policy rules on that flow are deactivated/terminated without explicit instructions from the PD-PE.

Two resource control modes shall be supported to provision the aforementioned policies:

- push mode: The policy installation is initiated by control elements (e.g., SCE or PD-PE). Upon receipt of a request from the SCE or a trigger within the PD-PE, the PD-PE shall push down the relevant policy decisions directly.
- pull mode: The policy installation is requested by transport devices (i.e., PE-PE) due to the trigger of the UE or local conditions. Upon receipt of a request from the PE-PE, the PD-PE shall reply the relevant policy decisions to the PE-PE.

Both push mode and pull mode shall support the installation, activation, modification and deactivation of dynamic policy decisions. Static policy configuration may also use the push mode and the pull mode, as needed.

A session identifier shall be used to identify the association of a resource control request and the corresponding policy decisions between the PD-PE and the PE-PE. This identifier shall be globally unique in order to support one-to-many and many-to-one communication modes as defined in clause 9.2.2 of [ITU-T Y.2111], for example, it may consist of a logical PD-PE instance identifier, a logical SCE instance identifier, a requester name and local session ID to make its global uniqueness.

For policy control in support of emergency telecommunications service (ETS), see clause 6.3.

6 Resource control procedures

6.1 SCE-requested resource control procedures

6.1.1 Procedures at the PD-PE

6.1.1.1 Resource initiation

6.1.1.1.1 Resource control mode

The PD-PE shall determine which resource control mode is used upon receipt of an initial AA-Request (AAR) from the SCE, based on the network configuration and/or the access network type. If the PD-PE operates in the push mode for this new resource control session, the PD-PE shall send a Policy-Install-Request (PI-Request) command containing policy decisions to the corresponding PE-PE for initiating a new Diameter session between the PD-PE and the PE-PE, following the initial resource control operations described in clauses 6.1.1.1.2 to 6.1.1.1.5. The PD-PE serves as the Diameter server and the PE-PE serves as the Diameter client for this resource control session.

The PI-Request may include an Auth-Session-State attribute-value pair (AVP) to indicate the PD-PE's preference for stateful or stateless operation. When the PD-PE performs the stateful operation, for initial AA-Requests in which the Session-Id is new, the Media-Component-Number(s) and Flow-Number(s) are also interpreted by the PD-PE as new. When the PD-PE performs the stateless operation, all media components are viewed as new ones regardless of the Session-Id status. The stateful and stateless operations towards the SCE are described in clause 6.1.1 of [ITU-T Q.3301.1 v3].

NOTE – As specified in [IETF RFC 6733], the Session-Id is globally unique and is meant to uniquely identify a user session without reference to any other information. The Session-Id begins with the sender's identity encoded in the Diameter identity type.

6.1.1.1.2 Soft-state and hard-state

The PD-PE shall interpret the presence of the Authorization-Lifetime AVP in the AA-Request received from the SCE as a request for a soft-state reservation and the absence of this AVP as a request for a hard-state reservation. The PD-PE may, however, return the Reservation-Lifetime AVP and the Auth-Grace-Period AVP defining a limited lifetime of the reservation although the AA-Request did not contain the Authorization-Lifetime AVP. The PD-PE thereby offers a soft-state reservation although the request was for hard-state. The PD-PE may also choose not to return the Reservation-Lifetime AVP and the Auth-Grace-Period AVP although the AA-Request contained the Authorization-Lifetime AVP. The PD-PE thereby offers a hard-state reservation although the request was for soft-state reservation.

As specified in clause 8.9 of [IETF RFC 6733], the server (i.e., the PD-PE) may return the Reservation-Lifetime AVP and the Auth-Grace-Period AVP set to values for which the sum is equal to, or smaller than, the value of the Authorization-Lifetime AVP provided by the SCE.

The PI-Request may contain the Authorization-Lifetime AVP to indicate the soft-state reservation to the PE-PE.

NOTE – Failure recovery functionality is FFS.

6.1.1.1.3 Transport subscription profile verification

The PD-PE shall verify the transport subscription profile received from the NACF using one of the following three identifiers with Address-Realm AVP as the index.

- 1) User-Name AVP
- 2) Framed-IP-Address AVP
- 3) Framed-IPv6-Prefix AVP

The PD-PE shall derive the QoS information based on the AF-Application-Identifier AVP, the Reservation-Service-Priority AVP and the Media-Type AVP and Media-Component-Description AVP of the initial AA-Request received from the SCE, and verify the transport subscription profile to which the request applies for each IP media flow. In this verification process, the derived parameters shall match the information obtained from NACF via the Ru interface. If the transport subscription profile does not contain any data, the PD-PE shall apply a default profile to the request.

The Ru interface is outside the scope of this Recommendation.

6.1.1.1.4 Transport resource detection and admission

The PD-PE shall request the TRC-PE for transport resource availability detection and admission decision such as Max-Requested-Bandwidth-DL/UL AVP via the Rt interface and utilize the result of resource admission decision for the policy decision. If IP media flows are grouped in certain forms, the PD-PE shall request the TRC-PE to authorize the QoS only if the IP media flows are distributed to transport bearers in a way that is allowed.

The Rt interface is outside the scope of this Recommendation.

6.1.1.1.5 Initial policy decisions

The PD-PE shall make initial policy decisions for all IP media flows conveyed by the initial AA-Request from the SCE based on all information described in clause 8.2.5.2 of [ITU-T Y.2111], including:

- Service information received from the SCE.
- Transport subscription profile.

- Service-based network policies.
- Transport resource availability and admission decision information received from the TRC-PE.

An initial request can be admitted by the PD-PE if, for all IP media flows in the session, all conditions are satisfied. If the request is admitted, the PD-PE shall send an AA-Answer back to the SCE and include the Result-Code AVP set to the value Diameter_SUCCESS. Otherwise, the PD-PE may include the available resource information in the AA-Answer if the reason of failed authorization is due to insufficient resources.

The PD-PE may specify the Priority-Level AVP (as part of the ARP AVP) as one main AVP of the PI-Request in order to assign a priority to the request according to the information received from the SCE and/or the network policy. The PD-PE may further specify the Priority-Level AVP (as part of the ARP AVP) in QoS-information AVP(s) in order to assign priority to individual media. If the Priority-Level AVP (as part of the ARP AVP) is not specified, the requested priority is DEFAULT.

NOTE – The ARP priority level represents an ordered range of values. The ARP priority level attribute represents the actual priority for the service/user with the value 1 as the highest and can thus be upgraded and downgraded.

Upon successful policy decision, for the stateful operation, the PD-PE shall store the Diameter base protocol Session-Id received in the initial AA-Request, and the Media-Component-Number(s) and Flow-Number(s). It shall also create an instance of the state machine for each IP media flow in the session and store the state of each IP media flow; for stateless operation, the PD-PE shall store the above information temporarily until receiving the answer from the PE-PE; moreover, the PD-PE shall generate a Class AVP with all the above information and send it to the PE-PE for maintaining the session state information.

In stateless operation, the PD-PE does not store the received Session-Id. Instead, it generates, based on local policy data (possibly the contents of the AA-Request and of messages received over other interfaces), one or more Class AVPs containing the information needed for it to reconstruct its state when it receives additional messages relating to the same user session. This information might include, for example:

- A unique string identifying the session corresponding to the initial AA-Request;
- The address(es) of the TRC-PE(s) involved in the session; and
- The address of the PE-PE involved in the session; and
- Other session information.

In addition, the policy decisions shall contain the following information:

a) IP media flow description

The PD-PE shall derive the uplink and downlink packet classifiers from the IP addresses and port numbers for uplink and downlink IP flows provided by the SCE. The PD-PE shall not modify the address and port information received from the SCE.

The PD-PE shall send the destination address and port number for each IP media flow as part of the Charging-Rule-Definition AVP.

b) QoS information

The QoS information (consisting of maximum QoS class and bandwidth requirements) for IP media flows is extracted from the service information received from the SCE, e.g., from the media type, bandwidth information, service class and SCE application ID.

- The PD-PE may select the QoS class that is the highest class applicable for the media. The PD-PE shall use the same QoS class for both the uplink and the downlink directions when both directions are used. The selection of network QoS class is also dependent on network policies. In addition, the PD-PE may derive the transport QoS



- class directly according to certain network technologies and convey the information through ToS-Traffic-Class AVP (for GPRS, DiffServ and MPLS).
- The PD-PE shall authorize the contained bandwidth value of Max-Requested-Bandwidth-DL/UL in the initial AA-Request received from the SCE according to network policies, transport subscription profile and resource availability. By default, the bandwidth value contains all overhead coming from the IP-layer and the layers above, e.g., IP, UDP, RTP and RTP payload by default.
 - The Max-Requested-Bandwidth-DL/UL shall be considered as the peak data rate, the values of Maximum-Burst-Size, Committed-Data-Rate, Committed-Burst-Size and Excess-Burst-Size AVPs in the Traffic-Descriptor-DL/UL AVP may be derived as needed for certain types of traffic and network technologies for traffic policing.

c) Resource control actions

Based on the Flow-Status AVP in the initial AA-Request received from the SCE, the PD-PE shall decide resource control actions, either Reservation-only or ReservationandCommitment together.

The Reservation-only action requests the PE-PE to enforce the initial policy decisions (e.g., reserve the authorized bandwidth) without passing the packets. It is used when the value of the Flow-Status AVP is "closed". The ReservationandCommitment action requests the PE-PE to enforce the initial policy decisions (e.g., reserve the authorized bandwidth) and pass the packets. It is used when the value of the Flow-Status AVP is "open". The Flow-Status AVP in the PI-Request indicates the resource control action for each individual IP media flow or group of IP media flows if needed and applicable; for example, in the case the same set of policy decisions (e.g., QoS class) is applied to all of them, which shall be specified in the Charging-Rule-Definition AVP and in the Media-Sub-Component AVP(s). The Flow-Status AVP shall be set to the same value in both AVPs:

- Reservation-only: The value of the Flow-Status AVP shall be set to DISABLED (3).
- ReservationandCommitment: The value of the Flow-Status AVP shall be set to ENABLED-UPLINK (0), ENABLED-DOWNLINK (1) or ENABLED (2).

Any value of the Flow-Status AVP received in an initial AA-Request (in which the Session-Id is new) different from ENABLED-UPLINK, ENABLED-DOWNLINK, ENABLED or DISABLED shall result in an error without any resource control action through Rw.

d) NAT traversal and NAPT information

In order to request the address latching and address translation operations in the PE-PE, when hosted NAT traversal is detected by the SCE (e.g., the Latching-Indication AVP is set to LATCH (0) by the SCE), the PD-PE shall include the latching-Indication AVP with the value LATCH (0) and the Binding-Information AVP with the Binding-Input-List AVP received from the AA-Request into the PI-Request; when the near-end NAPT is enabled by the network operator, the PD-PE shall populate the Binding-Information AVP with the Binding-Input-List for the affected IP media flows and set the Latching-Indication AVP to LATCH (0).

6.1.1.2 Resource modification

Upon receipt of the AA-Request message from the SCE with modified service information or local triggers due to network policies, configuration and conditions, the PD-PE shall perform the transport subscription verification and transport resource detection and admission, and update the policy decision as described in clauses 6.1.1.1.3 to 6.1.1.1.5 for all new/modified media components, based on the state information stored locally in stateful operation or conveyed in the Class AVP in stateless operation. When the PD-PE pushes updated policy decisions to the PE-PE,

the new/modified Charging-Rule-Definition AVP(s) shall be provided; in addition, the Logical-Access-ID AVP may be provided to request a particular way for how IP media flows are to be distributed to transport bearers. The RA-Request shall be used to convey the updated policy decision in the stateful operation; meanwhile, the PI-Request shall be used to convey the updated policy decision in stateless operation.

Depending on the value of the Flow-Status AVP received from the SCE, the PD-PE shall interpret the session modification as one of the following:

- 1) Modification of requested resources;
- 2) Commitment of requested resources;
- 3) Removal of requested resources.

The modification of requested resources may request the addition of IP media flows or the modification of the attributes of existing IP media flows (e.g., bandwidth and/or the lifetime of a resource control session in case of soft-state reservation) without passing through the packets (i.e., the gate is closed). When an IP media flow is put on hold, the PD-PE shall retain all session state information and may send the request to the PE-PE for closing the gate with Flow-Status AVP set to DISABLED (3) – the possible real-time transport control protocol (RTCP) gate shall be left open to keep the connection alive. The commitment of requested resources may request the allocation/activation of previously reserved resources and/or of additional requested resources (e.g., new media components) and open the gates for all related IP media flows. The removal of requested resources may request the revocation of previously committed and/or reserved resources and close the gates for all related IP media flows.

The corresponding resource control actions shall be included in the updated policy decision according to the above modification requests. The Flow-Status AVP in the RA-Request indicates the resource control action for each individual IP media flow, which shall be specified in the Charging-Rule-Definition AVP(s). The Flow-Status AVP shall be set to the same value in both these AVPs:

- Modification of requested resources: The value of the Flow-Status AVP shall be set to DISABLED (3).
- Commitment of requested resources: The value of the Flow-Status AVP shall be set to ENABLED-UPLINK (0), ENABLED-DOWNLINK (1) or ENABLED (2).
- Removal of requested resources: The value of the Flow-Status AVP shall be set to REMOVED (4).

6.1.1.3 Complete release of resources

Complete release of resources may be initiated by the PD-PE upon receipt of a termination request from the SCE or triggered by predefined static policies inside the PD-PE, or by the PE-PE triggered by predefined static policies inside the PE-PE.

Upon receipt of a Session-Termination-Request from the SCE in stateful operation, or receipt of an AA-Request message containing no Media-Component-Description AVP in stateless operation, the PD-PE shall release all relevant resources and session state and send an Abort-Session-Request message (AS-Request) to the PE-PE in stateful operation, or send a PI-Request to the PE-PE with PI-Request-Type AVP set to the value "TERMINATION_REQUEST" in stateless operation in order to revoke any transport plane functions enforced over the R_w interface in the PE-PE as a result of this session.

Upon receipt of a CC-Request from the PE-PE with CC-Request-Type AVP set to the value "TERMINATION_REQUEST", the PD-PE shall release all relevant resources and session state and send an Abort-Session-Request message (AS-Request) to the SCE in stateful operation, or send a

PI-Request with PI-Request-Type AVP set to the value "TERMINATION_REQUEST" to the SCE in stateless operation in order to notify the termination of this session.

When session termination is triggered by local policies and conditions, the PD-PE shall release all relevant resources and session state and send an Abort-Session-Request message (AS-Request) to the SCE and PE-PE respectively in the stateful operation, or send a PI-Request with PI-Request-Type AVP set to the value "TERMINATION_REQUEST" to the SCE and PE-PE respectively in stateless operation in order to notify the termination of this session.

6.1.1.4 Event notification

The PD-PE may request to be notified of certain events (e.g., bearer failure) by specifying them in the Event-Triggers AVP of the initial PI-Request command or of RA-Request command for subsequent modification.

6.1.2 Procedures at the PE-PE

6.1.2.1 Resource initiation

Upon receipt of a PI-Request message from the PD-PE with a new Session-Id, the PE-PE shall establish a new session and install the initial policy decision.

The PE-PE shall examine the content of any Auth-Session-State AVP and the Authorization-Lifetime AVP. If such an AVP is present and indicates stateful operation, the PE-PE shall include the same Session-Id value in subsequent messages relating to this session. If a received Auth-Session-State AVP indicates stateless operation, the PE-PE shall store the value of the Class AVP and include the stored Class AVP in any message it sends to the PD-PE relating to the same session.

When the Flow-Status AVP is set to the value DISABLED in the initial PI-Request, the PE-PE shall install the initial policy decisions without any commitment operations and the gates shall be closed for all related IP media flows. When the Flow-Status AVP is set to the value ENABLED, ENABLED-UPLINK or ENABLED-DOWNLINK in the initial PI-Request, the PE-PE shall commit the requested resources and open the gates for all related IP media flows using the packet filters defined in the Flow-Description AVP.

Any value of the Flow-Status AVP received in an initial PI-Request (in which the Session-Id is new) different from ENABLED-UPLINK, ENABLED-DOWNLINK, ENABLED or DISABLED shall result in an error. If the Flow-Status AVP has the value REMOVED, the PE-PE shall return a PI-Answer containing a Failed-AVP AVP and a Result-Code AVP with the value Diameter_INVALID_AVP_VALUE. Detailed policy enforcement operations are described in clause 6.1.2.5.

The PE-PE may examine the Priority-Level AVP (as part of the ARP AVP) in the PI-Request and/or within a Charging-Rule-Definition AVP of the PI-Request to determine the precedence for the handling of resource control sessions and the importance of relevant IP media flows.

If the Bearer-Identifier or Logical-Access-ID AVP is present, the PE-PE shall only allocate the IP media flows to transport bearers in a way that is allowed.

When the Latching-Indication AVP is set, the PE-PE shall populate the address translation information to the Binding-Information AVP and include them in the PI-Answer command to the PD-PE.