International Telecommunication Union

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

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/.

Table of Contents

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*.

[IETF RFC 6733] IETF RFC 6733 (2012), *Diameter Base 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

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 Rw 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.

6.1.2.2 Resource modification

Upon receipt of an RA-Request with an existing Session-Id in the stateful operation or a PI-Request with Class AVP identifying an existing session, the PE-PE shall enforce the updated policy decisions and may perform the following operations:

– Install policy decision for a new IP media flow without committing the requested resources if the Flow-Status AVP is set to DISABLED.

– Install policy decision and commit the requested resources for a new IP media flow if the Flow-Status AVP is set to ENABLED, ENABLED-UPLINK or ENABLED-DOWNLINK (e.g., open the gates).

– Modify policy decision for an existing IP media flow without committing the requested resources if the Flow-Status AVP is set to DISABLED (e.g., increase or decrease the allocated bandwidth, but the RTCP gate may retain the open status).

– Modify policy decision and commit the requested resources for an existing IP media flow if the Flow-Status AVP is set to ENABLED, ENABLED-UPLINK or ENABLED-DOWNLINK (e.g., open the gates with modified bandwidth).

– Commit the requested resources for an existing IP media flow if the Flow-Status AVP is set to ENABLED, ENABLED-UPLINK or ENABLED-DOWNLINK (e.g., open the gates with reserved bandwidth).

– Revoke the installed policy decisions and release the committed or reserved resources for all related IP media flows if the Flow-Status AVP is set to REMOVED.

– Refresh a soft-state if an Authorization-Lifetime AVP is present in the RA-Request and PI-Request as a hint of the maximum lifetime that it is requesting.

The PE-PE may also disable the commitment of requested resources by closing the gate but retaining the session state information and transport resources if the Flow-Status AVP is set to DISABLED for a prior enabled IP media flow.

If the Latching-Indication AVP is set to "RELATCH", the PE-PE shall populate the address translation information to the Binding-Information AVP in the RA-Answer or PI-Answer command based on the updated Input-List AVP received from the PD-PE.

6.1.2.3 Complete release of resources

If the last transport bearer or IP media flow within an UE transport session is being terminated, the PE-PE shall send a CC-Request command to the PD-PE with CC-Request-Type AVP set to the value "TERMINATION_REQUEST".

If session termination is initiated by the PD-PE, upon receipt of AS-Request in stateful operation, or PI-Request with PI-Request-Type AVP set to the value "TERMINATION_REQUEST" in stateless operation, the PE-PE shall disable the relevant gates and release the network resource.

6.1.2.4 Event notification

If an event subscribed by PD-PE through PI-Request or RA-Request occurs, the PE-PE shall send a CC-Request command to the PD-PE containing:

– the value of the Event-Triggers AVP, indicating the event that occurred; and

– optionally, the appropriate Termination-Cause AVP value.

6.1.2.5 Policy enforcement operations

6.1.2.5.1 QoS mapping

When QoS information (e.g., QoS-Class-Identifier AVP, Max-Requested-Bandwidth-UL/DL AVPs) is received from the PD-PE, the PE-PE shall perform the mapping between network QoS and the transport QoS by the Translation/mapping function, which maps the generic QoS class into the transport QoS class for a specific network technology (e.g., translation into UMTS QoS class for GPRS access networks, or translation into DiffServ code point for DS-TE enabled MPLS); alternatively, the transport QoS class may be received directly from the PD-PE via ToS-Traffic-Class AVP. The mapping rules are subject to relevant standards and network operator's local policy (e.g., the table for UMTS QoS mapping is defined in [b-3GPP TS 29.212]). Typically, the mapping rules can be preconfigured in the PE-PE and may be updated via the policy provisioning system or the Rw interface, as needed.

The PE-PE shall decide on a transport bearer to carry the requested traffic based on the matching transport QoS class.

In addition, the PE-PE shall make a selection of an existing transport bearer to allocate the resource for the corresponding IP media flows, or make a decision to create a new transport bearer for the corresponding IP media flows based on the matching QoS class.

6.1.2.5.2 Gate operation

The policy decision to open or close the gate shall lead to the enabling or disabling of the passage for the corresponding IP packets. When the gate is closed, all packets of the related IP flows shall be dropped; when the gate is opened, the packets of the related IP flows are allowed to pass through. The Flow-Status AVP of the policy decision shall describe if the possible uplink and possible downlink gate is opened or closed.

Upon receipt of either PI-Request or RA-Request command from the PD-PE for the initiation or modification of a policy decision, the PE-PE shall examine the gate decision specified by the Flow-Status AVP in the Charging-Rule-Definition AVP and perform the gate operation for each IP media flow:

– Open the gate for uplink direction, downlink direction, or both directions respectively if the Flow-Status AVP is set to ENABLED-UPLINK or ENABLED-DOWNLINK, or ENABLED.
– Close the gate if the Flow-Status AVP is set to DISABLED, but the possible RTCP gate may be kept open.
– Close all relevant gates including the RTCP gate if the Flow-Status AVP is set to REMOVED.

6.1.2.5.3 User plane operation

The PE-PE shall enforce the policy decision of resource control based "gating" functionality according to additional information received from the PD-PE. When the policy decision is installed and activated, the PE-PE shall evaluate the packets against IP media flow filters provided by the PD-PE or predefined in the static policy rules for all transport bearers in the order of precedence of the policy decisions or the predefined static policy rules. When a packet matches an IP media flow filter, the policy decisions for that filter shall be applied, such as:

– Bandwidth allocation/policing information provided by Max-Requested-Bandwidth-UL/DL AVPs and Traffic-Descriptor-UL/DL AVPs.
– Packet marking/remarking information provided by ToS-Traffic-Class AVP.
– QoS resource statistics and reporting information provided by Metering-Method AVP.

– Firewall and packet inspection information provided by Dynamic-Firewall-Working-Mode AVP.
– NAPT translation and address latching/translation information provided by Binding-Information AVP.

The IP Packets shall be transported within the specific transport bearer (e.g., a VLAN, LSP) where the selected policy decision is mapped. The IP packets that do not match any IP media flow filters provided by the policy decisions shall be silently discarded.

6.2 UE-requested resource control procedures

6.2.1 Procedures at the PD-PE

6.2.1.1 Initial authorization

The PD-PE shall determine the resource control mode first when receiving the initial AA-Request from the SCE as described in clause 6.1.1.1.1. When the UE requests the transport resource via the transport signalling, the pull mode shall be employed in support of resource control procedures.

After performing the relevant operations described in clauses 6.1.1.1.2 to 6.1.1.1.4, in the pull mode, the PD-PE may push down certain initial policy decision information to the PE-PE via the Rw interface by the PI-Request command to facilitate the PD-PE discovery and binding and speeding up the policy enforcement operations. In this case, the procedures of session initiation described in clause 6.2.1.2 may not be needed; and the PE-PE may perform the initial authorization directly.

Alternatively, the PD-PE shall just respond with an AA-Answer to the SCE via the Rs interface, following the procedure described in clause 6.2.1.2.

Depending on the network configuration, as an option, the PD-PE identity information may be populated into the Authorization-Token AVP. This PD-PE identifier shall be in the format of a fully qualified domain name.

6.2.1.2 Resource initiation

The PD-PE shall perform the binding operation to establish the association between the initial CC-Request and the initial authorization of resource control session based on the information provided by the request. Detailed bearer binding mechanisms are described in clause 6.2.1.6.

In response to the initial CC-Request, the PD-PE shall send a CC-Answer command with the initial policy decisions including IP media flow descriptions, QoS information and NAT traversal/NAPT information to the PE-PE.

The PD-PE derives the Selected Bearer-Control-Mode AVP based on the received Network-Request-Support AVP, the Bearer-Control-Mode AVP, access network information, subscriber information and operator policy. The Selected Bearer-Control-Mode AVP may be provided to the PE-PE using the PCC rules provision procedure at IP-connectivity access network (IP-CAN) session establishment. The PE-PE should forward it to the UE. The selected Bearer-Control-Mode AVP value will be applicable for the whole IP-CAN session (in GPRS, it is applicable to all packet data protocol (PDP) contexts within the activated PDP Address/APN pair).

6.2.1.3 Resource modification

In response to the CC-Request, the PD-PE shall perform the binding operation as described in clause 6.2.1.6, and shall send a CC-Answer command to the PE-PE with the policy decision for new or modified IP media flows including IP media flow descriptions, QoS information and NAT traversal/NAPT information.

Additionally, the PD-PE shall be able to push down updated policy decisions triggered by the SCE or local policies without explicit request of the PE-PE in the pull mode. The relevant procedures are the same as session modification of the push mode described in clause 6.1.1.2.

Depending on the value of the Flow-Status AVP received from the SCE or PE-PE through AA-Request or CA-Request, 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 detailed procedures are described in clause 6.1.1.2. For certain access networks, such as GPRS, alternative approaches may be used, such as described in [b-3GPP TS 29.212].

6.2.1.4 Complete release of resources

The session termination may be initiated by the PE-PE through CC-Request with CC-Request-Type AVP set to the value "TERMINATION_REQUEST" upon receipt of a transport signalling message from the UE or triggered by predefined static policies inside the PE-PE, or by the PD-PE upon receipt of a ST-Request from the SCE or triggered by predefined static policies inside the PD-PE. The detailed procedures are described in clause 6.1.1.3.

6.2.1.5 Event notification

The detailed procedures are described in clause 6.1.1.4.

6.2.1.6 Binding operations

The binding operations are performed by the PD-PE to establish an association between a resource control session and a corresponding transport bearer(s) when the transport bearers are initiated by the UE via the transport signalling message.

Upon receipt of CC-Request, the PD-PE shall perform the binding operation to identify the pre-authorized resource control session along with the policy decisions. The PD-PE shall compare the flow identifier conveyed by the request from the PE-PE with the pre-authorized flow filter information stored in the PD-PE; in addition, the PD-PE may utilize other information to assist the binding if available, including the user identification, globally unique IP address. If more than one flow identifier is included, the PD-PE shall also verify that the media components identified by the flow identifiers are allowed to be transferred in the same UE transport session.

The flow identifier can be provided by the Flow-Description AVP of CC-Request, which includes the source/destination IP addresses and port numbers. As an alternative, the authorization token can be used to convey the flow identifier(s).

The pre-authorized flow filter in the PD-PE is obtained from the Flow-Description AVP of AA-Request received from the SCE during the initial authorization.

6.2.2 Procedures at the PE-PE

6.2.2.1 Resource initiation

Upon receipt of an initial transport signalling message from the UE for establishing a new UE transport session, the PE-PE shall send a CC-Request command with CC-Request-Type AVP set to the value "INITIAL_REQUEST".

The PE-PE shall provide flow identifiers to allow the PD-PE to identify the policy decisions to be applied; in addition, it may provide other information such as the type of IP-CAN, user identification, the type of the access network (e.g., UTRAN, GERAN, WLAN) and the globally unique IP address of the UE. The PE-PE may also include the Access-Network-Charging-Address

and Access-Network-Charging-Identifier-Gx AVPs in the CC-Request. For GPRS, information about the UE (e.g., IMEISV), QoS negotiated, serving GPRS support node (SGSN) Address, SGSN country and network codes, APN, traffic flow template (TFT) and an indication of the presence of PDP context should be included in the CC-Request.

Furthermore, if the UE and the network support the network-initiated bearer request procedure, the PE-PE shall indicate this by supplying the Network Request Support AVP. If the UE indicated a preferred bearer control mode, the PE-PE shall indicate this mode within the Bearer-Control Mode AVP.

For IP-CAN types that support multiple IP-CAN bearers (as in the case of GPRS), the PE-PE shall provide the Bearer-Identifier AVP at the IP-CAN session establishment. In this case, the PE-PE shall also include the Bearer-Operation AVP set to the value "Establishment".

6.2.2.2 Resource modification

Upon receipt of a transport signalling message from the UE to modify an existing UE transport session, the PE-PE shall send a CC-Request command to the PD-PE with CC-Request-Type AVP set to the value "UPDATE_REQUEST".

For example, the session modification with a transport signalling message can occur in the following cases in the GPRS:

– When a new PDP context is being established by the UE initiated in an already existing PDP session.

– When a PDP context is being modified or terminated by the UE.

For certain types of access networks, e.g., GPRS, additional bearer identifier and bearer operation information may be provided to identify the transport bearer as described in [b-3GPP TS 29.212].

When a particular IP media flow or transport bearer is terminated by the UE or by the PE-PE based on the policy decision or on predefined policies, the PE-PE shall send a CC-Request command to the PD-PE with CC-Request-Type AVP set to the value "UPDATE_REQUEST" and the relevant Flow-Status AVP set to "REMOVED".

The PE-PE may include the Access-Network-Charging-Address and Access-Network-Charging-Identifier-Gx AVPs in the CC-Request. For an IP-CAN Session modification where an existing IP-CAN Bearer is modified, the PE-PE shall supply within the PCC rule request the specific event which caused the IP-CAN session modification (within the Event-Trigger AVP) and any previously provisioned PCC rule(s) affected by the IP-CAN session modification. The PCC rules and their status shall be supplied to PD-PE within the Charging-Rule-Report AVP.

6.2.2.3 Complete release of resources

The detailed procedures are described in clause 6.1.2.3. In addition, for GPRS, the PE-PE shall also apply the procedures as described in clause 4.5.7 of [b-3GPP TS 29.212] to indicate the IP-CAN session termination.

6.2.2.4 Event notification

The detailed procedures are described in clause 6.1.2.4.

6.2.2.5 Policy enforcement operations

The detailed procedures are described in clause 6.1.2.5.

In addition, the PE-PE may make local decision based on stored policy decision information of an active UE transport session, when the UE requests for an UE transport session modification via the transport signalling message.

6.2.2.6 Binding operations

The binding operations are performed by the PE-PE to identify the correct PD-PE and subsequently request policy decision information from the PD-PE.

The PE-PE shall determine the IP address of the corresponding PD-PE from the information of transport signalling message received from the UE. The information shall include flow identifier and may include other information such as user identification, globally unique IP address, etc.; as an alternative option, the Authorization Token may be used to provide the PD-PE identifier for binding operation. This identifier shall be in the format of a fully qualified domain name.

6.3 Emergency telecommunications service support

6.3.1 Policy procedures for ETS over Rw

6.3.1.1 Provisioning of policy rules for ETS

The provision of policy rules and operation corresponding to both ETS and non-ETS service shall be performed as described in clause 5.1.

When the PD-PE derives policy rules corresponding to ETS, the Priority-Level AVP (as part of the ARP AVP) shall be set as appropriate for the prioritized service, e.g., ETS.

NOTE 1 – The Pre-emption-Capability AVP and Pre-emption-Vulnerability AVP (if received as part of the ARP AVP) are not applicable. The use of these AVPs in non-3GPP specified networks is FFS.

NOTE 2 – The QCI AVP is not applicable. The use of this AVP in non-3GPP specified networks is FFS.

When the PD-PE derives policy rules corresponding to non-ETS service, the PD-PE shall generate the policy rules as per normal procedures. At the time that a priority service (e.g., ETS) is invoked, the PD-PE shall upgrade the Priority-Level (as part of the ARP AVP) for the policy rules corresponding to non-ETS service. The PD-PE shall change the Priority-Level (as part of the ARP AVP) for ETS to an appropriate value according to the PD-PE decision.

When the PD-PE receives a AA-Request containing the priority information (priority indication and priority level) from the SCE and upon verifying the priority information, the PD-PE shall derive the applicable policy rules and assign the Priority Level (as part of the ARP AVP) corresponding to ETS based on that information.

Once the PD-PE receives a notification of a change in priority information (e.g., priority level), the PD-PE shall make the corresponding policy decisions (i.e., priority level change as part of ARP AVP) and, if applicable, shall initiate a RA-Request to provision the modified information.

NOTE – The priority level is one among other input data such as operator policy for the PD-PE to set the Priority Level (as part of the ARP AVP).

6.3.1.2 Invocation/revocation of ETS

If the PD-PE receives service information including an ETS session indication and the priority level from the SCE, the PD-PE shall:

– Derive the policy rules corresponding to ETS, based on the information received over the Rs interface, and set the appropriate Priority Level AVP (as part of the ARP AVP) in the corresponding policy rules in a RA-Request towards the PE-PE.

– Trigger the IP-CAN to subsequently apply priority treatment for transport layer media packets.

If the PD-PE detects that the SCE released the ETS session, the PD-PE shall:

– Delete the policy rules and QoS information corresponding to ETS via a RA-Request towards the PE-PE.

The PD-PE shall provision the PE-PE with the applicable policy rules upon ETS activation and deactivation as described in clause 5.1. The provision of the QoS information applicable for the policy rules shall be performed as described in clause 5.1.

7 Rw protocol specification

The Rw protocol is based on Diameter [IETF RFC 6733].

7.1 Protocol support

The Diameter Base Protocol as specified in [IETF RFC 6733] is used to support information transfer on the Rw interface. [IETF RFC 6733] shall apply except as modified by the additional methods, commands, AVPs, and result and event codes specified in this Recommendation. Unless otherwise indicated, the procedures of [IETF RFC 6733] (including error handling and unrecognized information handling) are unmodified.

In addition to the AVPs from the Diameter base protocol [IETF RFC 6733], the Diameter messages sent over the Rw interface use the AVPs defined in clause 7.3.

The Rw Diameter application is defined as an IETF vendor-specific Diameter application, with application ID 16777256. Vendor identifiers are assigned by Internet Assigned Numbers Authority (IANA) [b-IANA]; the vendor identifier assigned to ITU-T is 11502. This Recommendation also uses the Diameter application defined in [b-3GPP TS 29.212] for the 3GPP Gx interface, where the vendor is 3GPP. The vendor identifier assigned by IANA to 3GPP is 10415. In addition, a pair of new Diameter commands is complemented in order to support policy control functions defined in [ITU-T Y.2111].

With regard to the Diameter protocol defined over the Rw interface, the PD-PE acts as a Diameter server, in the sense that it is the network element that handles authorization requests for a particular realm. The PE-PE acts as the Diameter client, in the sense that it is the network element requesting authorization to use bearer path network resources.

7.2 Use of the Diameter base protocol

With the clarifications listed in the following clauses, the Diameter Base Protocol defined by [IETF RFC 6733] shall apply.

7.2.1 Securing Diameter messages

To secure transport of Diameter messages, the method defined in [b-ETSI TS 133 210] shall be used.

7.2.2 Accounting functionality

Accounting functionality (Accounting Session State Machine, related command codes and AVPs) is not used on the Rw interface.

7.2.3 Use of sessions

As described in clauses 6.1 and 6.2, operation for a given session may be stateful or stateless.

For stateful operation, a valid Session-Id AVP shall be present in all messages passing between the PD-PE and the PE-PE, as described in [IETF RFC 6733]. If a Diameter session of resource control is initiated by the PD-PE, the Policy-Install-Request (PIR) and Policy-Install-Answer (PIA) shall be used. If a Diameter session of resource control is modified by the PD-PE, the RA-Request and RA-Answer shall be used. If a Diameter session of resource control is terminated by the PD-PE, the Abort-Session-Request (ASR) and Abort-Session-Answer (ASA) commands defined in [IETF RFC 6733] shall be used. If a Diameter session of resource control is initiated/modified/terminated by the PE-PE, the Credit-Control-Request (CCR) and Credit-Control-

Answer (CCA) with the CC-Request-Type AVP set to "INITIAL-REQUEST"/"UPDATE-REQUEST"/"TERMINATION-REQUEST" shall be used.

For stateless operation, it is always indicated definitively by a value of NO_STATE_MAINTAINED in an Auth-Session-State AVP by the PD-PE in the initial PI-Request or in the CC-Answer to the PE-PE. If a Diameter session is initiated/modified/terminated by the PD-PE, PI-Request and PI-Answer containing the Class AVP with the PI-Request-Type AVP set to "INITIAL-REQUEST"/"UPDATE-REQUEST"/"TERMINATION-REQUEST" shall be used. If a Diameter session is initiated/modified/terminated by the PE-PE, CC-Request and CC-Answer containing the Class AVP with the CC-Request-Type AVP set to "INITIAL-REQUEST"/ "UPDATE-REQUEST"/"TERMINATION-REQUEST" shall be used.

7.2.4 Transport protocol

Diameter messages over the Rw interface shall make use of SCTP [IETF RFC 4960] and shall utilize the new SCTP checksum method specified in [IETF RFC 3309].

7.2.5 Routing considerations

This clause specifies the use of the Diameter routing AVPs Destination-Realm and Destination-Host for routing.

The PD-PE obtains the contact address of the PE-PE for a given flow through the means identified in clause 8.3.1 of [ITU-Y.2111] in the push mode. The PE-PE obtains the contact address of the PD-PE for a given flow through the means identified in clause 8.3.2 of [ITU-T Y.2111] in the pull mode. Both the Destination-Realm and Destination-Host AVPs shall be present in the request.

7.2.6 Advertising application support

The Capabilities-Exchange-Request (CER) and Capabilities-Exchange-Answer (CEA) commands are specified in the Diameter Base Protocol [IETF RFC 6733].

The PD-PE and PE-PE shall advertise the support of the Rw specific application by including the value 16777256 of the application identifier in the Auth-Application-Id AVP within the Vendor-Specific-Application-Id grouped AVP of the Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands.

The vendor identifier value of 11502 (ITU-T) shall be included in the Vendor-Id AVP of the Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands, and in the Vendor-Id AVP within the Vendor-Specific-Application-Id grouped AVP of the Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands. Additionally, the PD-PE and the PE-PE shall advertise the support of additional Vendor-ID AVPs by including the values 13019 (ETSI) and 10415 (3GPP) in two different Supported-Vendor-Id AVPs of the CER and CEA commands.

NOTE 1 – The Vendor-Id AVP which is included in Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands shall indicate the manufacturer of the Diameter node as per [IETF RFC 6733].

NOTE 2 – Regarding the open state of the Diameter session, CER/CEA is not used.

7.3 AVPs

Table 1 summarizes the AVPs used in this Recommendation, beyond those defined in the Diameter Base Protocol.

7.3.1 New AVPs

Table 1 describes the new AVPs defined solely within this Recommendation. The ITU-T Vendor-Id (11502) shall be used in the Vendor-Id field of the AVP header.

Table 1 – New Diameter AVPs defined by this Recommendation

Attribute name	AVP code	Clause defined	Value type	AVP flag rules (Note 1)				May encrypt (Note 2)
				Must	May	Should not	Must not	
PI-Request-Type	1010	7.3.3.1	Enumerated	M, V	P			Y
PI-Request-Number	1011	7.3.3.2	Unsigned32	M, V	P			Y
Traffic-Descriptor-UL	1012	7.3.3.3	Grouped	V	P			Y
Traffic-Descriptor-DL	1013	7.3.3.4	Grouped	V	P			Y
Maximum-Burst-Size	1014	7.3.3.5	Unsigned32	V	P			Y
Committed-Data-Rate	1015	7.3.3.6	Unsigned32	V	P			Y
Committed-Burst-Size	1016	7.3.3.7	Unsigned32	V	P			Y
Excess-Burst-Size	1017	7.3.3.8	Unsigned32	V	P			Y
Removal-Cause	1018	7.3.3.9	Enumerated	M, V	P			Y
Traffic-Information	1019	7.3.65	Grouped	M, V	P			Y
Multicast ACL	1020	7.3.66	Grouped	V	P			Y

NOTE 1 – The AVP header bit denoted as 'M', indicates whether support of the AVP is required. The AVP header bit denoted as 'V', indicates whether the optional Vendor-ID field is present in the AVP header. The AVP header bit denoted as 'P', indicates the need for encryption for end-to-end security. For further details, see [IETF RFC 6733].

NOTE 2 – The 'Y' means that if a message containing that AVP is to be sent via a Diameter agent (proxy, redirect or relay) then the message MUST NOT be sent unless there is end-to-end security between the originator and the recipient and integrity/confidentiality protection is offered for this AVP OR the originator has locally trusted configuration that indicates that end-to-end security is not needed. For further details, see [IETF RFC 6733].

7.3.2 Imported AVPs

Table 2 describes the Diameter AVPs that are used within this Recommendation that have been defined by [ITU-T Q.3301.1 v3], providing their AVP code values, types, possible flag values and whether or not the AVP may be encrypted. Flag values are described in the context of this Recommendation, rather than in the context of the application where they were defined. The Vendor-Id header of all AVPs identified in Table 2 shall be set to ITU-T (11502). AVPs that are defined in [ITU-T Q.3301.1 v3] and not listed in Table 2 should not be sent by Diameter implementations conforming to the current Recommendation and, in the case where they are sent, they shall be ignored by the receiving entities.

Table 2 – Additional Diameter AVPs – Set I

Attribute name	AVP code	Clause defined	Value type	AVP flag rules (Note 1)				May Encr. (Note 2)
				Must	May	Should not	Must not	
Dynamic-Firewall-Working-Mode	1002	7.3.3.10	Enumerated	V	P			Y
QoS-Downgradeable	1001	7.3.3.11	Enumerated	V	P			Y

NOTE 1 – The AVP header bit denoted as 'M', indicates whether support of the AVP is required. The AVP header bit denoted as 'V', indicates whether the optional Vendor-ID field is present in the AVP header. The AVP header bit denoted as 'P', indicates the need for encryption for end-to-end security. For further details, see [IETF RFC 6733].

NOTE 2 – The 'Y' means that if a message containing that AVP is to be sent via a Diameter agent (proxy, redirect or relay) then the message MUST NOT be sent unless there is end-to-end security between the originator and the recipient and integrity/confidentiality protection is offered for this AVP OR the originator has locally trusted configuration that indicates that end-to-end security is not needed. For further details, see [IETF RFC 6733].

NOTE 3 – The Set I is the Diameter AVPs imported from [ITU-T Q.3301.1 v3].

Table 7-3 describes the Diameter AVPs that are used within this Recommendation that have been defined by [b-ETSI TS 183 017], providing their AVP code values, types, possible flag values and whether or not the AVP may be encrypted. Flag values are described in the context of the current Recommendation, rather than in the context of the application where they were defined. The Vendor-Id header of all AVPs identified in Table 3 shall be set to ETSI (13019). AVPs that are defined in [b-ETSI TS 183 017] and not listed in Table 3 should not be sent by Diameter implementations conforming to the current Recommendation and, in the case where they are sent, they shall be ignored by the receiving entities.

Table 3 – Additional Diameter AVPs – Set II

Attribute name	AVP code	Clause defined	Value type	AVP flag rules (Note 1)				May Encr. (Note 2)
				Must	May	Should not	Must not	
Binding-Information	450	7.3.3.13	Grouped	V			M	Y
Binding-Input-List	451	7.3.3.14	Grouped	V			M	Y
Binding-Output-List	452	7.3.3.15	Grouped	V			M	Y
V6-Transport-Address	453	7.3.3.16	Grouped	V			M	Y
V4-Transport-Address	454	7.3.3.17	Grouped	V			M	Y
Port-Number	455	7.3.3.18	Unsigned32	V			M	Y
Latching-Indication	457	7.3.3.19	Enumerated	V			M	Y

NOTE 1 – The AVP header bit denoted as 'M' indicates whether support of the AVP is required. The AVP header bit denoted as 'V' indicates whether the optional Vendor-ID field is present in the AVP header. For further details, see [IETF RFC 6733].

NOTE 2 – The 'Y' means that if a message containing that AVP is to be sent via a Diameter agent (proxy, redirect or relay) then the message MUST NOT be sent unless there is end-to-end security between the originator and the recipient and integrity/confidentiality protection is offered for this AVP OR the originator has locally trusted configuration that indicates that end-to-end security is not needed. For further details, see [IETF RFC 6733].

NOTE 3 – The Set II is the Diameter AVPs imported from [b-ETSI TS 183 017] (Gq').

Table 4 describes the Diameter AVPs that are used within this Recommendation that have been defined by [b-ETSI ES 283 034], providing their AVP code values, types, possible flag values and whether or not the AVP may be encrypted. Flag values are described in the context of this Recommendation, rather than in the context of the application where they were defined. The

Vendor-Id header of all AVPs identified in Table 4 shall be set to ETSI (13019). AVPs that are defined in [b-ETSI ES 283 034] and not listed in Table 4 should not be sent by Diameter implementations conforming to this Recommendation and, if they are sent, they shall be ignored by the receiving entities.

Table 4 – Additional Diameter AVPs – Set III

Attribute name	AVP code	Clause defined	Value type	AVP flag rules (Note 1)				May Encr. (Note 2)
				Must	May	Should not	Must not	
Address-Realm	301	7.3.3.60	OctetString	V			M	Y
Logical-Access-Id	302	7.3.3.61	OctetString	V	M			Y
Physical-Access-Id	313	7.3.3.62	UTF8String	V	M			Y

NOTE 1 – The AVP header bit denoted as 'M' indicates whether support of the AVP is required. The AVP header bit denoted as 'V' indicates whether the optional Vendor-ID field is present in the AVP header. For further details, see [IETF RFC 6733].

NOTE 2 – The 'Y' means that if a message containing that AVP is to be sent via a Diameter agent (proxy, redirect or relay) then the message MUST NOT be sent unless there is end-to-end security between the originator and the recipient and integrity/confidentiality protection is offered for this AVP OR the originator has locally trusted configuration that indicates that end-to-end security is not needed. For further details, see [IETF RFC 6733].

NOTE 3 – The Set III is the Diameter AVPs imported from [b-ETSI ES 283] (e4).

Table 5 describes the Diameter AVPs that are used within this Recommendation that have been defined by [b-ETSI TS 129 209], providing their AVP code values, types, possible flag values and whether or not the AVP may be encrypted. Flag values are described in the context of the Recommendation, rather than in the context of the application where they were defined. The Vendor-Id header of all AVPs identified in Table 5 shall be set to 3GPP (10415). AVPs that are defined in [b-ETSI TS 129 209] and not listed in Table 5 should not be sent by Diameter implementations conforming to the current Recommendation and, if they are sent, they shall be ignored by the receiving entities.

Table 5 – Additional Diameter AVPs – Set IV

Attribute name	AVP code	Clause defined (Note 3)	Value type	AVP flag rules (Note 1)				May Encr. (Note 2)
				Must	May	Should not	Must not	
AF-Charging-Identifier	505		OctetString	M, V	P			Y
Flow-Description	507		IPFilterRule	M, V	P			Y
Flow-Number	509		Unsigned32	M, V	P			Y
Flows	510		Grouped	M, V	P			Y
Flow-Status	511		Enumerated	M, V	P			Y
Max-Requested-Bandwidth-DL	515		Unsigned32	M, V	P			Y
Max-Requested-Bandwidth-UL	516		Unsigned32	M, V	P			Y
Media-Component-Number	518		Unsigned32	M, V	P			Y

NOTE 1 – The AVP header bit denoted as 'M' indicates whether support of the AVP is required. The AVP header bit denoted as 'V' indicates whether the optional Vendor-ID field is present in the AVP header. The AVP header bit denoted as 'P', indicates the need for encryption for end-to-end security. For further details, see [IETF RFC 6733].

NOTE 2 – The 'Y' means that if a message containing that AVP is to be sent via a Diameter agent (proxy, redirect or relay) then the message MUST NOT be sent unless there is end-to-end security between the originator and the recipient and integrity/confidentiality protection is offered for this AVP OR the originator has locally trusted configuration that indicates that end-to-end security is not needed. For further details, see [IETF RFC 6733].

NOTE 3 – The clause number given is that in [b-ETSI TS 129 209] rather than the current Recommendation. The definitions are repeated in clauses 7.3.3.14 to 7.3.3.36 below.

NOTE 4 – The Set IV is the Diameter AVPs imported from [b-ETSI TS 129 209] (Gq).

Table 6 describes the Diameter AVPs that are used within this Recommendation that have been defined by [b-3GPP TS 29.212], providing their AVP code values, types, possible flag values and whether or not the AVP may be encrypted. Flag values are described in the context of the current Recommendation, rather than in the context of the application where they were defined. The Vendor-Id header of all AVPs identified in Table 6 shall be set to 3GPP (10415). AVPs that are defined in [b-3GPP TS 29.212] and not listed in Table 6 should not be sent by Diameter implementations conforming to the current Recommendation and, if they are sent, they shall be ignored by the receiving entities.

Table 6 – Additional Diameter AVPs – Set V

Attribute name	AVP code	Clause defined	Value type	AVP flag rules (Note 1)				May Encr. (Note 2)	Acc. Type (Note 3)
				Must	May	Should not	Must not		
Access-Network-Charging-Identifier-Gx	1022		Grouped	M, V	P			Y	All
Allocation-Retention-Priority	1034	7.3.3.66	Grouped	V	P		M	Y	All
Bearer-Control-Mode	1023		Enumerated	M, V	P			Y	All
Bearer-Identifier	1020		OctetString	M, V	P			Y	GPRS
Bearer-Operation	1021		Enumerated	M, V	P			Y	GPRS

Table 6 – Additional Diameter AVPs – Set V

Attribute name	AVP code	Clause defined	Value type	AVP flag rules (Note 1)				May Encr. (Note 2)	Acc. Type (Note 3)
				Must	May	Should not	Must not		
Bearer-Usage	1000		Enumerated	M, V	P			Y	GPRS EPS
Charging-Rule-Install	1001		Grouped	M, V	P			Y	All
Charging-Rule-Remove	1002		Grouped	M, V	P			Y	All
Charging-Rule-Definition	1003		Grouped	M, V	P			Y	All
Charging-Rule-Base-Name	1004		UTF8String	M, V	P			Y	All
Charging-Rule-Name	1005		OctetString	M, V	P			Y	All
Charging-Rule-Report	1018		Grouped	M, V	P			Y	All
Event-Trigger	1006		Enumerated	M, V	P			Y	All
IP-CAN-Type	1027		Enumerated	M, V	P			Y	Note 4
Guaranteed-Bitrate-DL	1025		Unsigned32	M, V	P			Y	All
Guaranteed-Bitrate-UL	1026		Unsigned32	M, V	P			Y	All
Metering-Method	1007		Enumerated	M, V	P			Y	All
Network-Request-Support	1024		Enumerated	M, V	P			Y	All
Precedence	1010		Unsigned32	M, V	P			Y	All
Pre-emption-Capability	1047		Enumerated	V	P		M	Y	Note 4
Pre-emption-Vulnerability	1048		Enumerated	V	P		M	Y	Note 4
Priority-Level	1046	7.3.3.67	Unsigned32	V	P		M	Y	All
Reporting-Level	1011		Enumerated	M, V	P			Y	All
PCC-Rule-Status	1019		Enumerated	M, V	P			Y	All
QoS-Information	1016		Grouped	M, V	P			Y	All
QoS-Class-Identifier	1028		Enumerated	M, V	P			Y	Note 4
TFT-Filter	1012		IPFilterRule	M, V	P			Y	GPRS
TFT-Packet-Filter-Information	1013		Grouped	M, V	P			Y	GPRS
ToS-Traffic-Class	1014		OctetString	M, V	P			Y	GPRS
Rule-Failure-Code	1031		Enumerated	M, V	P			Y	All

Table 6 – Additional Diameter AVPs – Set V

NOTE 1 – The AVP header bit denoted as 'M' indicates whether support of the AVP is required. The AVP header bit denoted as 'V' indicates whether the optional Vendor-ID field is present in the AVP header. The AVP header bit denoted as 'P', indicates the need for encryption for end-to-end security. For further details, see [IETF RFC 6733].

NOTE 2 – The 'Y' means that if a message containing that AVP is to be sent via a Diameter agent (proxy, redirect or relay) then the message MUST NOT be sent unless there is end-to-end security between the originator and the recipient and integrity/confidentiality protection is offered for this AVP OR the originator has locally trusted configuration that indicates that end-to-end security is not needed. For further details, see [IETF RFC 6733].

NOTE 3 – All AVPs with Access type indicated as GPRS are only mandatory to GPRS networks.

NOTE 4 – These AVPs may be only applied to the networks specified in 3GPP.

NOTE 5 – The Set V is the Diameter AVPs imported from [b-3GPP TS 29.212].

Table 7 describes the Diameter AVPs that are used within this Recommendation that have been defined by [b-ETSI TS 129 061], providing their AVP code values, types, possible flag values and whether or not the AVP may be encrypted. Flag values are described in the context of the current Recommendation, rather than in the context of the application where they were defined. The Vendor-Id header of all AVPs identified in Table 7 shall be set to 3GPP (10415). AVPs that are defined in [b-ETSI TS 129 061] and not listed in Table 7 should not be sent by Diameter implementations conforming to the current Recommendation and, if they are sent, they shall be ignored by the receiving entities.

Table 7 – Additional Diameter AVPs – Set VI

Attribute name	AVP code	Clause defined (Note 2)	Value type	AVP flag rules (Note 1)				May Encr. (Note 2)
				Must	May	Should not	Must not	
3GPP-GPRS-Negotiated-QoS-Profile	5		UTF8String	M, V	P			Y
3GPP-RAT-Type	21		OctetString	M, V	P			Y
3GPP-SGSN-Address	6		UTF8String	M, V	P			Y
3GPP-SGSN-IPv6-Address	15		UTF8String	M, V	P			Y
3GPP-SGSN-IPv6-Address	15		UTF8String	M, V	P			Y
3GPP-SGSN-MCC-MNC	18		UTF8String	M, V	P			Y

NOTE 1 – The AVP header bit denoted as 'M', indicates whether support of the AVP is required. The AVP header bit denoted as 'V', indicates whether the optional Vendor-ID field is present in the AVP header. The AVP header bit denoted as 'P', indicates the need for encryption for end-to-end security. For further details, see [IETF RFC 6733].

NOTE 2 – The 'Y' means that if a message containing that AVP is to be sent via a Diameter agent (proxy, redirect or relay) then the message MUST NOT be sent unless there is end-to-end security between the originator and the recipient and integrity/confidentiality protection is offered for this AVP OR the originator has locally trusted configuration that indicates that end-to-end security is not needed. For further details, see [IETF RFC 6733].

NOTE 3 – All AVPs listed in this table are only applicable and mandatory to GPRS.

NOTE 4 – The use of Radius VSA as a Diameter vendor AVP is described in Diameter NASREQ ([IETF RFC 4005]) and the P flag may be set.

NOTE 5 – The Set VI is the Diameter AVPs imported from [b-ETSI TS 129 061].

Table 8 describes the Diameter AVPs defined for the network access server requirements (NASREQ) application [IETF RFC 4005] and used in this Recommendation, providing their AVP code values, types, possible flag values and whether the AVP may or not be encrypted. Flag values

are described in the context of the current Recommendation rather than in the context of the application where they are defined. AVPs defined in [IETF RFC 4005] but not listed in Table 8 should not be sent by Diameter applications conforming to the current Recommendation and shall be ignored by the receiving entities. No Vendor-Id shall be included in the AVP header.

Table 8 – Additional Diameter AVPs – Set VII

Attribute name	AVP code	Clause defined (Note 3)	Value type	AVP flag rules (Note 1)				May Encr. (Note 2)
				Must	May	Should not	Must not	
Framed-IP-Address	8		OctetString	M	P		V	Y
Framed-IPv6-Prefix	97		OctetString	M	P		V	Y
Called-Station-ID	30		UTF8String	M	P		V	Y

NOTE 1 – The AVP header bit denoted as 'M', indicates whether support of the AVP is required. The AVP header bit denoted as 'V', indicates whether the optional Vendor-ID field is present in the AVP header. The AVP header bit denoted as 'P', indicates the need for encryption for end-to-end security. For further details, see [IETF RFC 6733].

NOTE 2 – The 'Y' means that if a message containing that AVP is to be sent via a Diameter agent (proxy, redirect or relay) then the message MUST NOT be sent unless there is end-to-end security between the originator and the recipient and integrity/confidentiality protection is offered for this AVP OR the originator has locally trusted configuration that indicates that end-to-end security is not needed. For further details, see [IETF RFC 6733].

NOTE 3 – The clause number given is that in [IETF RFC 4005] rather than the current Recommendation. The definitions are repeated for the information in clauses 7.3.3.12 and 7.3.3.13.

NOTE 4 – The Set VII is the Diameter AVPs imported from the [IETF RFC 4005].

Table 9 describes the Diameter AVPs defined for the Credit-Control application [IETF RFC 4006] and used in the current Recommendation, providing their AVP code values, types, possible flag values and whether the AVP may or not be encrypted. Flag values are described in the context of the current Recommendation rather than in the context of the application where they are defined. AVPs defined in [IETF RFC 4006] but not listed in Table 9 should not be sent by Diameter applications conforming to the current Recommendation and shall be ignored by the receiving entities. No Vendor-Id shall be included in the AVP header.

Table 9 – Additional Diameter AVPs – Set VIII

Attribute name	AVP code	Clause defined (Note 3)	Value type	AVP flag rules (Note 1)				May Encr. (Note 2)
				Must	May	Should not	Must not	
CC-Request-Number	415		Unsigned32	M	P		V	Y
CC-Request-Type	416		Enumerated	M	P		V	Y
Rating-Group	432		Unsigned32	M	P		V	Y
Service-Identifier	439		Unsigned32	M	P		V	Y
Subscription-Id	443		Grouped	M	P		V	Y
User-Equipment-Info	458		Grouped		P, M		V	Y

NOTE 1 – The AVP header bit denoted as 'M', indicates whether support of the AVP is required. The AVP header bit denoted as 'V', indicates whether the optional Vendor-ID field is present in the AVP header. The AVP header bit denoted as 'P', indicates the need for encryption for end-to-end security. For further details, see [IETF RFC 6733].

NOTE 2 – The 'Y' means that if a message containing that AVP is to be sent via a Diameter agent (proxy, redirect or relay) then the message MUST NOT be sent unless there is end-to-end security between the originator and the recipient and integrity/confidentiality protection is offered for this AVP OR the originator has locally trusted configuration that indicates that end-to-end security is not needed. For further details, see [IETF RFC 6733].

NOTE 3 – The clause number given is that in [IETF RFC 4005] rather than the current Recommendation. The definitions are repeated for the information in clauses 7.3.3.12 and 7.3.3.13.

NOTE 4 – The Set VIII is the Diameter AVPs imported from the [IETF RFC 4006].

7.3.3 Definition of AVPs

NOTE – The items in bold in a grouped AVP are new AVPs added by the current Recommendation.

7.3.3.1 PI-Request-Type AVP

The PI-Request-Type AVP (ITU-T AVP Code 1010) is of type Enumerated and contains the reason for sending the Policy-Install Request command. It must be present in all Policy-Install-Request messages. The following values are defined for the PI-Request-Type AVP:

INITIAL_REQUEST 1

An Initial request is used to initiate a resource control session from the Diameter Server side, and contains resource control information that is relevant to the initiation.

UPDATE_REQUEST 2

An Update request contains resource-control information for an existing resource control session. Update Policy-Install requests should be sent every time at the expiry of the allocated quota or validity time. Further, additional service-specific events may trigger a spontaneous Update request.

TERMINATION_REQUEST 3

A Termination request is sent to terminate a resource control session and contains resource control information relevant to the existing session.

7.3.3.2 PI-Request-Number AVP

The PI-Request-Number AVP (ITU-T AVP Code 1011) is of type Unsigned32 and identifies this request within one session. As Session-Id AVPs are globally unique, the combination of Session-Id and PI-Request-Number AVPs is also globally unique and can be used in matching policy-install messages with confirmations. An easy way to produce unique numbers is to set the value to 0 for a policy-install request of type INITIAL_REQUEST and EVENT_REQUEST and to set the value to 1 for the first UPDATE_REQUEST, to 2 for the second, and so on until the value for TERMINATION_REQUEST is one more than for the last UPDATE_REQUEST.

7.3.3.3 Traffic-Descriptor-UL AVP

The Traffic-Descriptor-UL AVP (ITU-T AVP Code 1012) is of type Grouped, and it indicates complementary traffic characteristics in addition to maximum bandwidth. It is used to control the bandwidth of traffic flows at the uplink direction.

AVP Format:

```
Traffic-Descriptor ::= < AVP Header: 1012 >
                       [ Maximum-Burst-Size ]
                       [ Committed-Data-Rate ]
                       [ Committed-Burst-Size ]
                       [ Excess-Burst-Size ]
```

7.3.3.4 Traffic-Descriptor-DL AVP

The Traffic-Descriptor-DL AVP (ITU-T AVP Code 1013) is of type Grouped, and it indicates complementary traffic characteristics in addition to maximum bandwidth. It is used to control the bandwidth of traffic flows at the downlink direction.

AVP Format:

```
Traffic-Descriptor ::= < AVP Header: 1013 >
                       [ Maximum-Burst-Size ]
                       [ Committed-Data-Rate ]
                       [ Committed-Burst-Size ]
                       [ Excess-Burst-Size ]
```

7.3.3.5 Maximum-Burst-Size AVP

The Maximum-Burst-Size AVP (ITU-T AVP Code 1014) is of type Unsigned32 and indicates the peak burst size in octets. It is used to provision the peak burst size for traffic policing.

7.3.3.6 Committed-Data-Rate AVP

The Committed-Data-Rate AVP (ITU-T AVP Code 1015) is of type Unsigned32 and indicates the average bandwidth in octets per second. It is used to provision the average bandwidth for traffic policing.

7.3.3.7 Committed-Burst-Size AVP

The Committed-Burst-Size AVP (ITU-T AVP Code 1016) is of type Unsigned32 and indicates the committed burst size in octets. It is used to provision the committed burst size for traffic policing.

7.3.3.8 Excess-Burst-Size AVP

The Excess-Burst-Size AVP (ITU-T AVP Code 1017) is of type Unsigned32 and indicates the excess burst size in octets. It is used to provision the excess burst size for traffic policing.

7.3.3.9 Removal-Cause AVP

The Removal-Cause AVP (ITU-T AVP Code 1018) is of type Enumerated, and it determines the cause of a session abort request or of a Re-Auth-Request (RAR) indicating a transport bearer release. The following values are defined:

Session_RELEASED (0)

This value is used when the SCE session has been deactivated as a result from normal signalling handling.

INSUFFICIENT_SERVER_RESOURCES (1)

This value is used to indicate that the server is overloaded and needs to abort the session.

INSUFFICIENT_BEARER_RESOURCES (2)

This value is used to indicate that the network resource is short of capacity and needs to abort the session.

NOTE – The overload control of the protocol message processing is not defined in the current Recommendation.

7.3.3.10 Dynamic-Firewall-Working-Mode AVP

The Dynamic-Firewall-Working-Mode AVP (ITU-T AVP code 1002) is of type Enumerated, and provides information about the working mode of the firewall with respect to the IP flows of the user session. The following values are defined:

Static_Packet_Filtering (0)

This value is used when inspecting packet header information and dropping packets based on static security policy rules. This is the default packet inspection mode applied to all flows. No specific Flow-Description is needed for this mode.

Dynamic_Packet_Filtering (1)

This value is used when inspecting packet header information and dropping packets based on static security policy rules and dynamic gate status. Specific Flow-Description is needed for this mode.

Stateful_Inspection (2)

This value is used when inspecting packet header information (e.g., IP 5-tuple) as well as connection state information, and dropping packets based on static security policy rules and dynamic gate status. Specific Flow-Description and TCP/UDP filtering information are needed for this mode.

Deep_Packet_Inspection (3)

This value is used when inspecting packet header information (e.g., IP 5-tuple), connection state information and the content of payload (e.g., HTTP, RTP header) together, and dropping packets based on static security policy rules and dynamic gate status. Specific Flow-Description, and TCP/UDP and content filtering information are needed for this mode.

The dynamic firewall working mode is an optional feature and only valid based on network policies and configuration. The IP media flow filtering information is provided by the corresponding charging-rule-definition AVPs.

7.3.3.11 QoS-Downgradable AVP

The QoS-Downgradable AVP (ITU-T AVP code 1001) is of type Enumerated, and it provides information about the usage of IP Flows. The following values are defined:

NORMAL (0)

This value is used to indicate that the normal resource allocation is being provided.

MAY_DOWNGRADE (1)

This value is used to indicate that if the resource is not enough, the QoS may downgrade to default QoS class (e.g., best effort) and no need to reject the session.

NORMAL is the default value.

7.3.3.12 Binding-Information AVP

The Binding-Information AVP (AVP code 450) is of type Grouped and is sent between the PD-PE and the PE-PE in order to convey binding information required for NA(P)T and NA(P)T-PT control.

AVP format:

```
Binding-information ::= < AVP Header: 450 13019 >
                        { Binding-Input-List };
                        [ Binding-Output-List ];
```

7.3.3.13 Binding-Input-List AVP

The Binding-Input-List AVP (AVP code 451) is of type Grouped, and contains a list of transport addresses for which a binding is requested. The PD-PE constructs the Binding-Input-List using session description information (SDI).

AVP format:

```
Binding-Input-List ::= < AVP Header: 451 13019 >
                        *[ V6-Transport-Address ];
                        *[ V4-Transport-Address ];
```

7.3.3.14 Binding-Output-List AVP

The Binding-Output-List AVP (AVP code 452) is of type Grouped, and contains a list of transport addresses which are the result of the binding operation performed by the transport plane functions.

AVP format:

```
Binding-Ouput-List ::= < AVP Header: 452 13019 >
                        *[ V6-Transport-Address ];
                        *[ V4-Transport-Address ];
```

7.3.3.15 V6-Transport-Address AVP

The V6-Transport-Address AVP (AVP code 453) is of type Grouped and contains a single IPv6 address and a single port number.

AVP format:

```
Transport-Address ::= < AVP Header: 453 13019 >
                        { Framed-IPv6-Prefix };
                        { Port };
```

7.3.3.16 V4-Transport-Address AVP

The V4-Transport-Address AVP (AVP code 454) is of type Grouped and contains a single IPv4 address and a single port number.

AVP format:

```
Transport-Address ::= < AVP Header: 454 13019 >
                        { Framed-IP-Address };
                        { Port };
```

7.3.3.17 Port-Number AVP

The Port-number AVP (AVP code 455) is of type Unsigned32 and contains the end point port number.

7.3.3.18 Latching-Indication AVP

The Latching-Indication AVP (AVP code 457) is of type Enumerated.

The following values are defined:

LATCH (0)

RELATCH (1)

The relevant address binding information is provided by the Charging-Rule-Definition AVPs.

7.3.3.19 Framed-IP-Address AVP

The Framed-IP-Address AVP (AVP code 8) is defined in the NASREQ application [IETF RFC 4005].

7.3.3.20 Framed-IPv6-Prefix AVP

The Framed-IPv6-Prefix AVP (AVP code 97) is defined in the NASREQ application [IETF RFC 4005].

7.3.3.21 Abort-Cause AVP

The Session-Abort-Cause AVP (AVP code 500) is of type Enumerated, and it determines the cause of a session abort request or of an RAR indicating a transport bearer release. The following values are defined:

BEARER_RELEASED (0)

This value is used when the bearer has been deactivated as a result from normal signalling handling. For GPRS, the bearer refers to the PDP context, whereas for xDSL, the bearer may refer to an ATM VC.

INSUFFICIENT_SERVER_RESOURCES (1)

This value is used to indicate that the server is overloaded and needs to abort the session.

INSUFFICIENT_BEARER_RESOURCES (2)

This value is used when the bearer has been deactivated due to insufficient bearer resources at a transport gateway (e.g., end node function (ENF) for xDSL and gateway GPRS support node (GGSN) for GPRS).

7.3.3.22 AF-Charging-Identifier AVP

The AF-Charging-Identifier AVP (AVP code 505) is of type OctetString, and it contains the SCE charging identifier that is sent by the SCE. This information may be used for charging correlation with transport layer.

7.3.3.23 Flow-Description AVP

The Flow-Description AVP (AVP code 507) is of type IPFilterRule, and it defines a packet filter for an IP flow with the following information:

– Direction (in or out or both).
– Source and destination IP address (possibly masked).
– Protocol.
– Source and destination port (list or ranges).

The IPFilterRule type shall be used with the following restrictions:

– Only the Action "permit" shall be used.
– No "options" shall be used.
– The invert modifier "!" for addresses shall not be used.
– The keyword "assigned" shall not be used.

If any of these restrictions is not observed by the PE-PE in the push mode or by the PD-PE in the push mode, the receiver shall make an error response to the sender containing the Experimental-Result-Code AVP with value FILTER_RESTRICTIONS.

The Flow-Description AVP shall be used to describe a single IP flow.

The direction "in" refers to uplink IP flows, and the direction "out" refers to downlink IP flows.

The direction "both" refers to bidirectional unified resource allocation.

7.3.3.24 Flow-Number AVP

The Flow-Number AVP (AVP code 509) is of type Unsigned32, and it contains the ordinal number of the IP flow(s), assigned according to the rules in Annex C of [b-ETSI TS 129 207].

7.3.3.25 Flows AVP

The Flows AVP (AVP code 510) is of type Grouped, and it indicates IP flows via their flow identifiers.

If no Flow-Number AVP(s) is supplied, the Flows AVP refers to all Flows matching the media component number.

AVP Format:

```
Flows::= < AVP Header: 510 >
          { Media-Component-Number}
         *[ Flow-Number]
```

7.3.3.26 Flow-Status AVP

The Flow-Status AVP (AVP code 511) is of type Enumerated, and it describes whether the IP flow(s) are enabled or disabled. The following values are defined:

ENABLED-UPLINK (0)

This value shall be used to enable associated uplink IP flow(s) and to disable associated downlink IP flow(s). If any downlink RTCP IP flow(s) are identified by the Flow_Usage AVP(s), those flow(s) shall be enabled.

ENABLED-DOWNLINK (1)

This value shall be used to enable associated downlink IP flow(s) and to disable associated uplink IP flow(s). If any uplink RTCP IP flow(s) are identified by the Flow_Usage AVP(s), those flow(s) shall be enabled.

ENABLED (2)

This value shall be used to enable all associated IP flow(s) in both directions.

DISABLED (3)

This value shall be used to disable all associated IP flow(s) in both directions. If any RTCP IP flow(s) are identified by the Flow_Usage AVP(s), those flow(s) shall be enabled.

REMOVED (4)

This value shall be used to remove all associated IP flow(s). The IP Filters for the associated IP flow(s) shall be removed. The associated IP flows shall not be taken into account when deriving the authorized QoS.

7.3.3.27 Flow-Usage AVP

The Flow-Usage AVP (AVP code 512) is of type Enumerated, and it provides information about the usage of IP Flows. The following values are defined:

NO_INFORMATION (0)

This value is used to indicate that no information about the usage of the IP flow is being provided

RTCP (1)

This value is used to indicate that an IP flow is used to transport RTCP.

NO_INFORMATION is the default value.

NOTE – An SCE may choose not to identify RTCP flows, e.g., in order to avoid that RTCP flows are always enabled by the server.

7.3.3.28 Max-Requested-Bandwidth-DL AVP

The Max-Requested-Bandwidth-DL AVP (AVP code 515) is of type Unsigned32, and it indicates the maximum requested bandwidth in bits per second for a downlink IP flow. The bandwidth contains all the overhead coming from the IP-layer and the layers above, e.g., IP, UDP, RTP and RTP payload.

7.3.3.29 Max-Requested-Bandwidth-UL AVP

The Max-Requested-Bandwidth-UL AVP (AVP code 516) is of type Unsigned32, and it indicates the maximum requested bandwidth in bits per second for an uplink IP flow. The bandwidth contains all the overhead coming from the IP-layer and the layers above, e.g., IP, UDP, RTP and RTP payload.

7.3.3.30 Media-Component-Number AVP

The Media-Component-Number AVP (AVP code 518) is of type Unsigned32, and it contains the ordinal number of the media component, assigned according to the rules in Annex C of [b-ETSI TS 129 207].

7.3.3.31 Access-Network-Charging-Address AVP

The Access-Network-Charging-Address AVP (AVP code 501) is of type Address, and it indicates the IP Address of the network entity within the access network performing charging (e.g., the GGSN IP address). The Access-Network-Charging-Address AVP should not be forwarded over an inter-operator interface.

7.3.3.32 Access-Network-Charging-Identifier AVP

The Access-Network-Charging-Identifier AVP (AVP code 502) is of type Grouped, and it contains a charging identifier (e.g., GPRS charging ID (GCID)) within the Access-Network-Charging-Identifier-Value AVP along with information about the flows transported within the corresponding bearer within the Flows AVP. If no Flows AVP is provided, the Access-Network-Charging-Identifier-Value applies for all flows within a resource control session.

The Access-Network-Charging-Identifier AVP can be sent from the PD-PE to the SCE. The SCE may use this information for charging correlation with service layer.

AVP Format:

```
Access-Network-Charging-Identifier::= < AVP Header: 502 >
                 { Access-Network-Charging-Identifier-Value}
                *[ Flows ]
```

7.3.3.33 Access-Network-Charging-Identifier-Value AVP

The Access-Network-Charging-Identifier-Value AVP (AVP code 503) is of type OctetString and contains a charging identifier (e.g., GCID).

7.3.3.34 Authorization-Token AVP

The Authorization-Token AVP (AVP code 506) is of type OctetString, and contains the Authorization Token defined in [IETF RFC 3520].

7.3.3.35 Bearer-Usage AVP (Applicable access type GPRS or 3GPP-EPS)

The Bearer-Usage AVP (AVP code 1000) is of type Enumerated, and it shall indicate how the bearer is being used. If the Bearer-Usage AVP has not been previously provided, its absence shall indicate that no specific information is available. If the Bearer-Usage AVP has been provided, its value shall remain valid until it is provided the next time. The following values are defined:

GENERAL (0)

This value shall indicate no specific bearer usage information is available.

IMS_SIGNALLING (1)

This value shall indicate that the bearer is used for IMS signalling only.

7.3.3.36 Charging-Rule-Install AVP (All access types)

The Charging-Rule-Install AVP (AVP code 1001) is of type Grouped, and it is used to activate, install or modify policy decisions as instructed from the PD-PE to the PE-PE.

For installing a new Policy decision or modifying a Policy decision already installed, Charging-Rule-Name AVP and Charging-Rule-Definition AVP shall be used.

For activating a specific Policy decision predefined at the PE-PE, Charging-Rule-Name AVP shall be used as a reference for that Policy decision. The Charging-Rule-Base-Name AVP is a reference that may be used for activating a group of Policy decisions predefined at the PE-PE.

For GPRS scenarios where the bearer binding is performed by the PD-PE, the Bearer Identifier AVP shall be included as part of Charging-Rule-Install AVP.

If present within Charging-Rule-Install AVP, the Bearer-Identifier AVP indicates that the Policy decisions within this Charging-Rule-Install AVP shall be installed or activated within the IP-CAN bearer identified by the Bearer-Identifier AVP.

If no Bearer-Identifier AVP is included within the Charging-Rule-Install AVP, the PE-PE shall select an IP-CAN bearer for each of the Policy decisions within this Charging-Rule-Install AVP, where the Policy decision is installed or activated.

If the path selection function is enabled, the Logical-Access-ID and Physical-Access-ID should be used to indicate the associated transport bearer (e.g., a VLAN-ID, VPN ID, or LSP Label) and physical port of IP media flows.

AVP Format:

```
Charging-Rule-Install ::= < AVP Header: 1001 >
                     *[ Charging-Rule-Definition ]
                     *[ Charging-Rule-Name ]
                     *[ Charging-Rule-Base-Name ]
                      [ Bearer-Identifier ]
                      [ Logical-Access-Id]
                      [ Physical-Access-Id]
                     *[ AVP ]
```

7.3.3.37 Charging-Rule-Remove AVP (All access types)

The Charging-Rule-Remove AVP (AVP code 1002) is of type Grouped, and it is used to deactivate or remove Policy decisions from an IP-CAN session.

Charging-Rule-Name AVP is a reference for a specific Policy decision at the PE-PE to be removed or for a specific Policy decision predefined at the PE-PE to be deactivated. The Charging-Rule-Base-Name AVP is a reference for a group of Policy decisions predefined at the PE-PE to be deactivated.

AVP Format:

```
Charging-Rule-Remove ::= < AVP Header: 1002 >
                     *[ Charging-Rule-Name ]
                     *[ Charging-Rule-Base-Name ]
                     *[ AVP ]
```

7.3.3.38 Charging-Rule-Definition AVP (All access types)

The Charging-Rule-Definition AVP (AVP code 1003) is of type Grouped, and it defines the Policy decision for a service flow sent by the PD-PE to the PE-PE. The Charging-Rule-Name AVP uniquely identifies the Policy decision and it is used to reference to a Policy decision in communication between the PE-PE and the PD-PE. The Flow-Description AVP(s) determines the traffic that belongs to the service flow.

If optional AVP(s) within a Charging-Rule-Definition AVP are omitted, but the corresponding information has been provided in previous Gx messages, the previous information remains valid. If Flow-Description AVP(s) are supplied, they replace all previous Flow-Description AVP(s). If Flows AVP(s) are supplied, they replace all previous Flows AVP(s).

Flows AVP may appear if, and only if, AF-Charging-Identifier AVP is also present.

AVP Format:

```
Charging-Rule-Definition ::= < AVP Header: 1003 >
                      { Charging-Rule-Name }
                      [ Service-Identifier ]
                      [ Rating-Group ]
                     *[ Flow-Description ]
                      [ Flow-Status ]
                      [ Flow-Usage ]
                      [ Binding-Information ]
                      [ QoS-information ]
                      [ Latching-Indication ]
                      [ Dynamic-Firewall-Working-Mode ]
                      [ QoS-Downgradable ]
                      [ Reporting-Level ]
                      [ Metering-Method ]
                      [ Precedence ]
                      [ AF-Charging-Identifier ]
                     *[ Flows ]
                     *[ AVP ]
```

7.3.3.39 Charging-Rule-Base-Name AVP (All access types)

The Charging-Rule-Base-Name AVP (AVP code 1004) is of type UTF8String, and it indicates the name of a predefined group of Policy decisions residing at the PE-PE.

7.3.3.40 Charging-Rule-Name AVP (All access types)

The Charging-Rule-Name AVP (AVP code 1005) is of type OctetString, and it defines a name for Policy decision. For Policy decisions provided by the PD-PE, it uniquely identifies a Policy decision. For Policy decisions predefined at the PE-PE, it uniquely identifies a Policy decision within the PE-PE.

7.3.3.41 Event-Trigger AVP (All access types)

The Event-Trigger AVP (AVP code 1006) is of type Enumerated. When sent from the PD-PE to the PE-PE, the Event-Trigger AVP indicates an event that shall cause a re-request of Policy decisions. When sent from the PE-PE to the PD-PE, the Event-Trigger AVP indicates that the corresponding event has occurred at the gateway. The following values are defined:

SGSN_CHANGE (0)

This value shall be used in CCA and RAR commands by the PD-PE to indicate that, upon the change of the serving SGSN, Policy decisions shall be requested. When used in a CCR command, this value indicates that the PE-PE generated the request because the serving SGSN changed. Applicable only for GPRS.

QOS_CHANGE (1)

This value shall be used in CCA and RAR commands by the PD-PE to indicate that, upon a QoS change, Policy decisions shall be requested. When used in a CCR command, this value indicates that the PE-PE generated the request because there has been a change in the requested QoS (e.g., the previously maximum authorized QoS has been exceeded). Applicable for all access-types.

RAT_CHANGE (2)

This value shall be used in CCA and RAR commands by the PD-PE to indicate that, upon a RAT change Policy, decisions shall be requested. When used in a CCR command, this value indicates that the PE-PE generated the request because of a RAT change. Applicable only for GPRS.

TFT_CHANGE (3)

This value shall be used in CCA and RAR commands by the PD-PE to indicate that, upon a TFT change, Policy decisions shall be requested. When used in a CCR command, this value indicates that the PE-PE generated the request because of a change in the TFT. Applicable only for GPRS.

PLMN_CHANGE (4)

This value shall be used in CCA and RAR commands by the PD-PE to indicate that, upon a PLMN change, Policy decisions shall be requested. When used in a CCR command, this value indicates that the PE-PE generated the request because there was a change of PLMN. Applicable only for GPRS.

LOSS_OF_BEARER (5)

This value shall be used in CCA and RAR commands by the PD-PE to indicate that, upon loss of bearer, PE-PE should inform PD-PE. When used in a CCR command, this value indicates that the PE-PE generated the request because the bearer associated with the Policy decisions indicated by the corresponding Charging Rule Report AVP was lost. Applicable for those access-types that handle multiple bearers within one single UE transport session (e.g., GPRS).

The mechanism of indicating loss of bearer to the PE-PE is transport access type specific. For GPRS, this is indicated by a PDP context modification request with Maximum Bit Rate (MBR) in a QoS profile changed to 0 kbit/s.

RECOVERY_OF_BEARER (6)

This value shall be in CCA and RAR commands by the PD-PE used to indicate that upon recovery of bearer, PE-PE should inform PD-PE. When used in a CCR command, this value indicates that the PE-PE generated the request because the bearer associated with the Policy decisions indicated by the corresponding Charging Rule Report AVP was recovered. Applicable for those access-types that handle multiple bearers within one single UE transport session (e.g., GPRS). The mechanism for indicating recovery of bearer to the PE-PE is transport-access-type specific. For GPRS, this is indicated by a PDP context modification request with maximum bit rate (MBR) in QoS profile changed from 0 kbit/s to a valid value.

TRANSPORT_CHANGE (7)

This value shall be used in CCA and RAR commands by the PD-PE to indicate that, upon a change in the transport type, Policy decisions shall be requested. When used in a CCR command, this value indicates that the PE-PE generated the request because there was a change of transport type. Applicable for all access types.

QOS_CHANGE_EXCEEDING_AUTHORIZATION (8)

This value shall be used in CCA and RAR commands by the PD-PE to indicate that only upon a requested QoS change beyond the current authorized value(s) at bearer level, PCC rules shall be requested. When used in a CCR command, this value indicates that the PE-PE generated the request because there has been a change in the requested QoS beyond the authorized value(s) for a specific

bearer. The Bearer-Identifier AVP has to be provided to indicate the affected bearer. QoS-Information AVP is required to be provided in the same request with the new value.

NO_EVENT_TRIGGER (9)

This value shall be used in CCA and RAR commands by the PD-PE to indicate that PD-PE does not require any Event-Trigger notification.

SYNCHRONIZATION_FLAG (10)

This value shall be used in an RAR command to check whether the flow information in the PE-PE is consistent with the information in the PD-PE. After the PD-PE initiates the synchronization request with an event-trigger AVP equal to SYNCHRONIZATION_FLAG (10), the PE-PE will reply with a Re-Auth-Answer (RAA) command with an event-trigger AVP equal to SYNCHRONIZATION_FLAG (10) and a result code as "success". Then the PE-PE will send a CC-Request command to the PD-PE containing the value of the Event-Triggers AVP (10) to indicate the synchronization occurred and the flow information in the Traffic-Information AVP. The PD-PE compares the flow information stored with the information received from the PE-PE and instructs the PE-PE to synchronize the resources in the PD-PE and PE-PE, e.g., initiate, release or modify.

7.3.3.42 Metering-Method AVP (All access types)

The Metering-Method AVP (AVP code 1007) is of type Enumerated, and it defines what parameters shall be metered, for example, offline charging and/or other purposes. The following values are defined:

DURATION (0)

This value shall be used to indicate that the duration of the service flow shall be metered.

VOLUME (1)

This value shall be used to indicate that the volume of the service flow traffic shall be metered.

DURATION_VOLUME (2)

This value shall be used to indicate that the duration and the volume of the service flow traffic shall be metered.

7.3.3.43 Precedence AVP (All access types)

The Precedence AVP (AVP code 1010) is of type Unsigned32, and it defines the precedence of a Policy decision in case of overlapping Policy decisions. A Policy decision with the Precedence AVP with lower value shall take the priority over a Policy decision with the Precedence AVP with higher value. The Precedence AVP is also used to indicate the evaluation precedence of the Traffic Mapping Information filters (for GPRS the TFT packet filters).

7.3.3.44 Reporting-Level AVP (All access types)

The Reporting-Level AVP (AVP code 1011) is of type Enumerated, and it defines on what level the PE-PE reports the usage for the related Policy decision. The following values are defined:

SERVICE_IDENTIFIER_LEVEL (0)

This value shall be used to indicate that the usage shall be reported on service id and rating group combination level.

RATING_GROUP_LEVEL (1)

This value shall be used to indicate that the usage shall be reported on rating group level.

7.3.3.45 TFT-Filter AVP (GPRS access type only)

The TFT-Filter AVP (AVP code 1012) is of type IPFilterRule, and it contains the flow filter for one TFT packet filter. The TFT-Filter AVP is derived from the TFT as defined in [b-ETSI TS 124 008]. The following information shall be sent:

– Action shall be set to "permit".

– Direction shall be set to "out".

– Protocol shall be set to the value provided within the TFT packet filter parameter "Protocol Identifier/Next Header Type". If the TFT packet filter parameter "Protocol Identifier/Next Header Type" is not provided within the TFT packet filter, Protocol shall be set to "ip".

– Source IP address (possibly masked). The source IP address shall be derived from TFT packet filter parameters "Source address" and "Subnet Mask". The source IP address shall be set to "any", if no such information is provided in the TFT packet filter.

– Source and destination port (single value, list or ranges). The information shall be derived from the corresponding TFT packet filter parameters. Source and/or destination port(s) shall be omitted if such information is not provided in the TFT packet filter.

– The Destination IP address shall be set to "assigned".

The IPFilterRule type shall be used with the following restrictions:

– No options shall be used.

– The invert modifier "!" for addresses shall not be used.

The direction "out" refers to downlink direction.

7.3.3.46 TFT-Packet-Filter-Information AVP (GPRS access type only)

The TFT-Packet-Filter-Information AVP (AVP code 1013) is of type Grouped, and it contains the information from a single TFT packet filter including the evaluation precedence, the filter and the Type-of-Service/Traffic-Class sent from the PE-PE to the PD-PE. The PE-PE shall include one TFT-Packet-Filter-Information AVP for each TFT packet filters applicable at a PDP context in separate TFT-Packet-Filter-Information AVPs within each Policy decision request corresponding to that PDP context. TFT-Packet-Filter-Information AVPs are derived from the TFT as defined in [b-ETSI TS 124 008].

AVP Format:

```
TFT-Packet-Filter-Information ::= < AVP Header: 1013>
                     [ Precedence ]
                     [ TFT-Filter ]
                     [ ToS-Traffic-Class ]
```

7.3.3.47 ToS-Traffic-Class AVP

The ToS-Traffic-Class AVP (AVP code 1014) is of type OctetString, and it contains the Type-of-Service/Traffic-Class of a TFT packet filter as defined in [b-ETSI TS 124 008] or the DSCP code point and marking as defined in [IETF RFC 2474].

7.3.3.48 QoS-information AVP

The QoS-information AVP (AVP code 1016) is of type Grouped, and it defines the maximum QoS that is authorized for a transport bearer or service flow. The QoS class defines the maximum authorized QoS class. The Max-Requested-Bandwidth-UL defines the maximum bit rate allowed for the uplink direction. The Max-Requested-Bandwidth-DL defines the maximum bit rate allowed for the downlink direction. The Guaranteed-Bitrate-UL defines the guaranteed bit rate allowed for the uplink direction. The Guaranteed-Bitrate-DL defines the guaranteed bit rate allowed for the downlink direction.

The Bearer Identifier AVP shall be included as part of QoS-information AVP if the authorized QoS of an IP-CAN bearer initiated by the UE is being provisioned and the PD-PE performs the bearer binding. The Bearer Identifier AVP identifies this bearer.

The Allocation-Retention-Priority AVP is an indicator of the priority of allocation and retention for the service flow. If the QoS-information AVP has been supplied previously but is omitted in a Diameter message or AVP, the previous information remains valid. If the QoS-information AVP has not been supplied previously and is omitted in a Diameter message or AVP, no enforcement of the authorized QoS shall be performed.

AVP Format:

```
QoS-information ::= < AVP Header: 1016>
                  [ QoS-class-Identifier ]
                  [ Max-Requested-Bandwidth-UL ]
                  [ Max-Requested-Bandwidth-DL ]
                  [ Guaranteed-Bitrate-UL ]
                  [ Guaranteed-Bitrate-DL ]
                  [ Bearer-Identifier ]
                  [ Traffic-Descriptor-UL ]
                  [ Traffic-Descriptor-DL ]
                  [ Allocation-Retention-Priority ]
                  [ ToS-Traffic-Class ]
```

7.3.3.49 QoS-Class-Identifier AVP

NOTE – This AVP may be only applied to the networks specified in 3GPP presently.

QoS-Class-Identifier AVP (AVP code 1028) is of type Enumerated, and it defines the maximum authorized traffic class for the transport bearer or service flow. The following values are defined:

TRAFFIC_CLASS_A (1)

This value defines that the QoS class is A.

TRAFFIC_CLASS_B (2)

This value defines that the QoS class is B.

TRAFFIC_CLASS_C (3)

This value defines that the QoS class is C.

TRAFFIC_CLASS_D (4)

This value defines that the QoS class is D.

TRAFFIC_CLASS_E (5)

This value defines that the QoS class is E.

TRAFFIC_CLASS_F (6)

This value defines that the QoS class is F.

TRAFFIC_CLASS_G (7)

This value defines that the QoS class is G.

TRAFFIC_CLASS_H (8)

This value defines that the QoS class is H.

TRAFFIC_CLASS_I (9)

This value defines that the QoS class is I.

The mapping of QCI to QoS classes of a specific-transport technology is beyond the scope of this Recommendation.

7.3.3.50 Charging-Rule-Report AVP (All access types)

The Charging-Rule-Report AVP (AVP code 1018) is of type Grouped, and it is used to report the status of a Policy decision (e.g., installation successful, removal, etc.).

Charging-Rule-Name AVP is a reference for a specific Policy decision at the PE-PE that has been successfully installed, modified or removed because of trigger from the UE. The PCC-Rule-Status AVP indicates the action being performed on the Policy decision. The Rule-Failure-Code indicates the reasons that the Policy decisions cannot be successfully installed/activated or enforced.

AVP Format:

```
Charging-Rule-Report ::= < AVP Header: 1018 >
                 *[ Charging-Rule-Name ]
                 *[ Charging-Rule-Base-Name ]
                  [ PCC-Rule-Status ]
                  [ Rule-Failure-Code ]
                 *[ AVP ]
```

Multiple instances of Charging-Rule-Report AVPs shall be used in the case it is required to report different PCC-Rule-Status values for different groups of rules within the same Diameter command.

7.3.3.51 PCC-Rule-Status AVP (All access types)

The PCC-Rule-Status AVP (AVP code 1019) is of type Enumerated, and it describes the status of a Policy decision.

The following values are defined:

ACTIVE (0)

This value is used to indicate that the PCC rule(s) are successfully installed (for those provisioned from PD-PE) or activated (for those pre-provisioned in the PE-PE)

INACTIVE (1)

This value is used to indicate that the PCC rule(s) are removed (for those provisioned from PD-PE) or inactive (for those pre-provisioned in the PE-PE).

TEMPORARY INACTIVE (2)

This value is used to indicate that, for some reason (e.g., loss of bearer), already installed or activated PCC rules are temporarily disabled.

7.3.3.52 Bearer-Identifier AVP (Applicable access type GPRS)

The Bearer-Identifier AVP (AVP code 1020) is of type OctetString, and it indicates the bearer to which specific information refers.

When present within a CC-Request Diameter command, subsequent AVPs within the CC-Request refer to the specific bearer identified by this AVP.

The bearer identifier of an IP-CAN bearer shall be unique within the corresponding IP-CAN session. The bearer identifier shall be selected by the PE-PE.

7.3.3.53 Bearer-Operation AVP (Applicable access type GPRS)

The Bearer-Operation AVP (AVP code 1021) is of type of Enumerated, and it indicates the bearer event that causes a request for Policy decisions. This AVP shall be supplied if the bearer event relates to an IP-CAN bearer initiated by the UE.

The following values are defined:

TERMINATION (0)

This value is used to indicate that a bearer is being terminated.

ESTABLISHMENT (1)

This value is used to indicate that a new bearer is being established.

MODIFICATION (2)

This value is used to indicate that an existing bearer is being modified.

7.3.3.54 Address-Realm AVP

The Address-Realm AVP (AVP code 301) is of type OctetString and contains the address realm in the form of a FQDN.

7.3.3.55 Logical-Access-ID AVP

The Logical-Access-ID AVP (AVP code 302 13019) is of type OctetString. This AVP contains either a circuit-ID (as defined in RFC 3046) or a technology-independent identifier.

NOTE – In the xDSL/ATM case, the Logical-Access-ID may explicitly contain the identity of the VP and VC carrying the traffic.

7.3.3.56 Physical-Access-ID AVP

The Physical-Access-ID AVP (AVP code 313 13019) is of type UTF8String and identifies the physical access to which the UE is connected. It includes a port identifier and the identity of the access node where the port resides.

7.3.3.57 Access-Network-Charging-Identifier-Gx AVP (All access types)

The Access-Network-Charging-Identifier-Gx AVP (AVP code 1022) is of type Grouped. It contains a charging identifier (e.g., GCID) within the Access-Network-Charging-Identifier-Value AVP and the related PCC rule name(s) within the Charging-Rule-Name AVP(s). If the IP-CAN session contains only a single IP-CAN bearer, no Charging-Rule-Name AVPs or Charging-Rule-Base-Name AVPs need to be provided. Otherwise, all the Charging-Rule-Name AVPs or Charging-Rule-Base-Name AVPs corresponding to PCC rules activated or installed within the IP-CAN bearer corresponding to the provided Access-Network-Charging-Identifier-Value shall be included.

The Access-Network-Charging-Identifier-Gx AVP can be sent from the PE-PE to the PD-PE. The PD-PE may use this information for charging correlation towards the SCF.

AVP Format:

```
Access-Network-Charging-Identifier-Gx ::= < AVP Header: 1022 >
                           { Access-Network-Charging-Identifier-Value }
                          *[ Charging-Rule-Base-Name ]
                          *[ Charging-Rule-Name ]
```

7.3.3.58 Bearer-Control-Mode AVP

The Bearer-Control-Mode AVP (AVP code 1023) is of type of Enumerated. When sent from PE-PE to PD-PE, it indicates the UE preferred bearer control mode. When sent from PD-PE to PE-PE, it indicates the PD-PE selected bearer control mode.

If the Bearer-Control-Mode AVP has not been previously provided by the PE-PE, its absence shall indicate the value UE_ONLY. If the Bearer-Control AVP has been provided, its value shall remain valid until it is provided the next time.

The following values are defined:

UE_ONLY (0)

This value is used to indicate that the UE shall request any additional bearer establishment.

NW_ONLY (1)

This value is used to indicate that the PE-PE shall request any additional bearer establishment.

UE_NW (2)

This value is used to indicate that both the UE and PE-PE may request any additional bearer establishment and add own traffic mapping information to an IP-CAN bearer.

7.3.3.59 Network-Request-Support AVP

The Network-Request-Support AVP (AVP code 1024) is of type of Enumerated, and it indicates the UE and network support of the network requested bearer control mode.

If the Network-Request-Support AVP has not been previously provided, its absence shall indicate the value NETWORK_REQUEST NOT SUPPORTED. If the Network-Request-Support AVP has been provided, its value shall remain valid until it is provided the next time.

The following values are defined:

NETWORK_REQUEST NOT SUPPORTED (0)

This value is used to indicate that the UE and the access network do not support the bearer establishment request procedure.

NETWORK_REQUEST SUPPORTED (1)

This value is used to indicate that the UE and the access network support the bearer establishment request procedure.

7.3.3.60 Guaranteed-Bitrate-DL AVP

The Guaranteed-Bitrate-DL AVP (AVP code 1025) is of type Unsigned32, and it indicates the guaranteed bitrate in bits per second for a downlink service data flow. The bandwidth contains all the overhead coming from the IP-layer and the layers above, e.g., IP, UDP, RTP and RTP payload.

7.3.3.61 Guaranteed-Bitrate-UL AVP

The Guaranteed-Bitrate-UL AVP (AVP code 1026) is of type Unsigned32, and it indicates the guaranteed bitrate in bits per second for an uplink service data flow. The bandwidth contains all the overhead coming from the IP-layer and the layers above, e.g., IP, UDP, RTP and RTP payload.

7.3.3.62 IP-CAN-Type AVP

NOTE – This AVP may be only applied to the network specified in 3GPP presently.

The IP-CAN-Type AVP (AVP code 1027) is of type Enumerated, and it shall indicate the type of connectivity access network to which the user is connected.

The IP-CAN-Type AVP shall always be present during the IP-CAN session establishment. During an IP-CAN session modification, this AVP shall be present when there has been a change in the IP-CAN type and the PD-PE requested to be informed of this event. The Event-Trigger AVP with value IP-CAN CHANGE shall be provided together with the IP-CAN-Type AVP.

The following values are defined:

3GPP (0)

This value shall be used to indicate that the IP-CAN is associated with a 3GPP access and is further detailed by the 3GPP-RAT-Type AVP.

7.3.3.63 Rule-Failure-Code AVP (all access types)

The Rule-Failure-Code AVP (3gpp AVP code 1031) is of type Enumerated. It is sent by the PE-PE to the PD-PE within a Charging-Rule-Report AVP to identify the reason a policy decision is being reported.

The following values are defined:

UNKNOWN_RULE_NAME (1)

This value is used to indicate that the pre-provisioned policy decision could not be successfully activated because the Charging-Rule-Name or Charging-Rule-Base-Name is unknown to the PE-PE.

RATING_GROUP_ERROR (2)

This value is used to indicate that the policy decision could not be successfully installed or enforced because the Rating-Group specified within the Charging-Rule-Definition AVP by the PD-PE is unknown or, invalid.

SERVICE_IDENTIFIER_ERROR (3)

This value is used to indicate that the policy decision could not be successfully installed or enforced because the Service-Identifier specified within the Charging-Rule-Definition AVP by the PD-PE is invalid, unknown, or not applicable to the service being charged.

GW/PE-PE_MALFUNCTION (4)

This value is used to indicate that the policy decision could not be successfully installed (for those provisioned from the PD-PE) or activated (for those pre-provisioned in the PE-PE) or enforced (for those already successfully installed) due to GW/PE-PE malfunction.

RESOURCES_LIMITATION (5)

This value is used to indicate that the policy decision could not be successfully installed (for those provisioned from the PD-PE) or activated (for those pre-provisioned in the PE-PE) or enforced (for those already successfully installed) due to a limitation of resources at the PE-PE.

MAX_NR_BEARERS_REACHED (6)

This value is used to indicate that the policy decision could not be successfully installed (for those provisioned from the PD-PE) or activated (for those pre-provisioned in the PE-PE) or enforced (for those already successfully installed) due to the fact that the maximum number of bearers has been reached for the IP-CAN session.

7.3.3.64 Traffic-Information AVP

The Traffic-Information AVP (ITU-T AVP code 1019) is of type Grouped, and it describes the detailed information from the transport equipment when the pull mode is used.

AVP Format:

```
Traffic-Information ::= < AVP Header: 1019 >
                     *[ Flow-Description ]
                      [ Flow-Status ]
                      [ QoS-Information ]
                      [ User-Name ]
                      [ Called-Station-ID ]
                      [ Framed-IP-Address ]
                      [ Framed-IPv6-Prefix ]
                      [ Address-Realm ]
                      [ Logical-Access-Id ]
                      [ Physical-Access-ID ]
```

7.3.3.65 Multicast ACL AVP

The Multicast ACL AVP (ITU-T AVP code 1020) is of type Grouped, and it consists of multicast addresses/address ranges representing the multicast groups which a subscriber is allowed to join.

7.3.3.66 Allocation-Retention-Priority AVP (All access types)

The Allocation-Retention-Priority AVP (AVP code 1034) is of type Grouped, and is used to indicate the priority of allocation and retention, the pre-emption capability and pre-emption vulnerability if provided within the QoS-Information-AVP.

AVP Format:

```
Allocation-Retention-Priority ::= < AVP Header: 1034 >
                 { Priority-Level }
                 [ Pre-emption-Capability ]
                 [ Pre-emption-Vulnerability ]
```

7.3.3.67 Priority-Level AVP (All access types)

The Priority-Level AVP (AVP code 1046) is of type Unsigned32. The AVP is used for deciding whether a bearer establishment or modification request can be accepted or needs to be rejected in case of resource limitations (typically used for admission control of GBR traffic). The AVP can also be used to decide which existing bearers to pre-empt during resource limitations. The priority level defines the relative importance of a resource request.

Values 1 to 15 are defined, with value 1 as the highest level of priority.

Values 1 to 8 should only be assigned for services that are authorized to receive prioritized treatment within an operator domain. Values 9 to 15 may be assigned to resources that are authorized by the home network and thus applicable when a UE is roaming (not applicable for fixed network access).

7.3.3.68 Pre-emption-Capability AVP

NOTE – This AVP may be only applied to the network specified in 3GPP presently.

The Pre-emption-Capability AVP (AVP code 1047) is of type Enumerated. If it is provided within the QoS-Information AVP, the AVP defines whether a service flow can get resources that were already assigned to another service flow with a lower priority level.

The following values are defined:

PRE-EMPTION_CAPABILITY_ENABLED (0)

This value indicates that the service flow or bearer is allowed to get resources that were already assigned to another service flow or bearer with a lower priority level.

PRE-EMPTION_CAPABILITY_DISABLED (1)

This value indicates that the service flow or bearer is not allowed to get resources that were already assigned to another service flow or bearer with a lower priority level. This is the default value applicable if this AVP is not supplied.

7.3.3.69 Pre-emption-Vulnerability AVP

NOTE – This AVP may be only applied to the network specified in 3GPP presently.

The Pre-emption Vulnerability AVP (AVP code 1048) is of type Enumerated. If it is provided within the QoS-Information AVP, the AVP defines whether a service flow can lose the resources assigned to it in order to admit a service flow with higher priority level.

The following values are defined:

PRE-EMPTION_VULNERABILITY_ENABLED (0)

This value indicates that the resources assigned to the service flow or bearer can be pre-empted and allocated to a service flow or bearer with a higher priority level. This is the default value applicable if this AVP is not supplied.

PRE-EMPTION_VULNERABILITY_DISABLED (1)

This value indicates that the resources assigned to the service flow or bearer shall not be pre-empted and allocated to a service flow or bearer with a higher priority level.

7.3.4 Experimental-Result-Code AVP values

This clause defines specific values of the Experimental-Result-Code AVP used in the current Recommendation.

7.3.5 Use of namespaces

This clause contains the namespaces that have either been created in the current Recommendation, and the values assigned to existing namespaces managed by IANA.

7.3.5.1 AVP codes

The current Recommendation assigns the AVP values from the AVP Code namespace managed by ITU-T and ETSI for their Diameter vendor-specific applications. See clause 7.3.3.

7.3.5.2 Experimental-Result-Code AVP values

This Recommendation assigns the Experimental-Result-Code AVP values from the AVP Code namespace managed by ETSI for its Diameter vendor-specific applications. See clause 7.3.4.

7.3.5.3 Command code values

This Recommendation assigns two new command code values and reuses existing command codes defined by ETSI and the IETF.

7.3.5.4 Application-ID value

The current Recommendation defines a new Diameter application ID value 16777256 allocated by IANA to the ITU-T Rw application.

7.4 Commands

Existing Diameter command codes from the Diameter base protocol [IETF RFC 6733] and the Diameter credit-control application [IETF RFC 4006] are used, in addition to a pair of new command codes defined by this Recommendation, which the Rw-specific Auth-Application id 16777256 is used.

7.4.1 Policy-Install-Request command

The PIR command, indicated by the Command-Code field set to 315 and the 'R' bit set in the Command Flags field, is sent by the PD-PE to the PE-PE in order to originate a resource control session in the push mode as defined in [ITU-T Y.2111], and it contains policy decision information of the QoS control, NAT traversal and NAPT control that is relevant to the initiation.

If the PD-PE has chosen stateless operation, the Auth-Session-State AVP shall be present in the PIR command for a session, and the Class AVP shall also be present. In this case, the Session-Id shall contain an arbitrary value.

Message Format:

```
<PI-Request> ::=    < Diameter Header: 315, REQ, PXY >
                    < Session-Id >
                    { Auth-Application-Id }
                    { Origin-Host }
                    { Origin-Realm }
                    { Destination-Realm }
                    { Destination-Host }
                    { PI-Request-Type }
                    { PI-Request-Number }
```

```
                    [ Origin-State-Id ]
                    [ Auth-Session-State ]
                    [ Class ]
                   *[ Event-Trigger ]
                   *[ Charging-Rule-Remove ]
                   *[ Charging-Rule-Install ]
                    [ QoS-information ]
                    [ User-Name ]
                    [ User-Equipment-Info ]
                    [ Called-Station-ID ]
                    [ Authorization-Lifetime ]
                   *[ Proxy-Info ]
                   *[ Route-Record ]
                   *[ AVP ]
```

7.4.2 Policy-Install-Answer command

The PIA command, indicated by the Command-Code field set to 315 and the 'R' bit cleared in the Command Flags field, is sent by the PE-PE to the PD-PE in response to the PIR command.

Message Format:

```
<PI-Answer> ::=      < Diameter Header: 315, PXY >
                     < Session-Id >
                     { Origin-Host }
                     { Origin-Realm }
                     { PI-Request-Type }
                     { PI-Request-Number }
                     [ Result-Code ]
                    *[ Charging-Rule-Report ]
                     [ Access-Network-Charging-Address ]
                    *[ Access-Network-Charging-Identifier-Gx ]
                     [ Experimental-Result ]
                     [ Origin-State-Id ]
                     [ Class ]
                     [ Error-Message ]
                     [ Error-Reporting-Host ]
                    *[ Failed-AVP ]
                    *[ Proxy-Info ]
                    *[ AVP ]
```

7.4.3 CC-Request (CCR) Command

The CCR command, indicated by the Command-Code field set to 272 and the 'R' bit set in the Command Flags field, is sent by the PE-PE to the PD-PE in order to request policy decisions for a bearer. The CCR command is also sent by the PE-PE to the PD-PE in order to indicate the termination of the bearer.

The Class AVP shall be present if the PD-PE has chosen stateless operation. In this case, the Session-Id shall contain an arbitrary value.

Message Format:

```
<CC-Request> ::= < Diameter Header: 272, REQ, PXY >
                     < Session-Id >
                     { Auth-Application-Id }
                     { Origin-Host }
                     { Origin-Realm }
                     { Destination-Realm }
                     { CC-Request-Type }
                     { CC-Request-Number }
                     [ Destination-Host ]
                     [ Origin-State-Id ]
                     [ Auth-Session-State ]
                     [ Class ]
                    *[ Subscription-Id ]
```

```
                    [ Bearer-Control-Mode ]
                    [ Network-Request-Support ]
                    [ Bearer-Identifier ]
                    [ Bearer-Operation ]
                    [ Framed-IP-Address ]
                    [ Framed-IPv6-Prefix ]
                    [ Address-Realm ]
                    [ Termination-Cause ]
                    [ User-Name ]
                    [ User-Equipment-Info ]
                    [ Called-Station-ID ]
                    [ Bearer-Usage ]
                   *[ Traffic-Information ]
                   *[ Charging-Rule-Report ]
                    [ 3GPP-RAT-Type ]
                    [ 3GPP-GPRS-Negotiated-QoS-Profile ]
                    [ 3GPP-SGSN-MCC-MNC ]
                    [ 3GPP-SGSN-Address ]
                    [ 3GPP-SGSN-IPv6-Address ]
                   *[ TFT-Packet-Filter-Information ]
                   *[ Event-Trigger]
                    [ Access-Network-Charging-Address ]
                   *[ Access-Network-Charging-Identifier-Gx ]
                   *[ Proxy-Info ]
                   *[ Route-Record ]
                   *[ AVP ]
```

7.4.4 CC-Answer (CCA) command

The CCA command, indicated by the Command-Code field set to 272 and the 'R' bit cleared in the Command Flags field, is sent by the PD-PE to the PE-PE in response to the CCR command. It is used to provision Policy decisions and event triggers for the bearer. The primary and secondary CCF and/or primary and secondary OCS addresses may be included in the initial provisioning.

The Class AVP shall be present if the PD-PE has chosen stateless operation. In this case, the Session-Id shall contain an arbitrary value.

Message Format:

```
<CC-Answer> ::=  < Diameter Header: 272, PXY >
                     < Session-Id >
                     { Auth-Application-Id }
                     { Origin-Host }
                     { Origin-Realm }
                     [ Result-Code ]
                     [ Experimental-Result ]
                     { CC-Request-Type }
                     { CC-Request-Number }
                     [ Bearer-Control-Mode ]
                     [ Origin-State-Id ]
                     [ Auth-Session-State ]
                     [ Class ]
                    *[ Event-Trigger ]
                    *[ Charging-Rule-Remove ]
                    *[ Charging-Rule-Install ]
                     [ QoS-information ]
                     [ Authorization-Lifetime ]
                     [ Error-Message ]
                     [ Error-Reporting-Host ]
                    *[ Failed-AVP ]
                    *[ Proxy-Info ]
                    *[ Route-Record ]
                    *[ AVP ]
```

7.4.5 Re-Auth-Request command

The RAR command, indicated by the Command-Code field set to 258 and the 'R' bit set in the Command Flags field, is sent by the PD-PE to the PE-PE in order to modify policy decisions for an existing resource control session triggered by the modification request (i.e., AAR) from the SCE or the change of network policy decisions.

NOTE – If the RAR command is received by the PE-PE without providing any operation on policy decision information, the PE-PE shall respond with a CCR command requesting policy decisions.

The PI-Request shall be used instead if the PD-PE has chosen stateless operation. In this case, the Session-Id shall contain an arbitrary value.

Message Format:

```
<RA-Request> ::= < Diameter Header: 258, REQ, PXY >
                    < Session-Id >
                    { Auth-Application-Id }
                    { Origin-Host }
                    { Origin-Realm }
                    { Destination-Realm }
                    { Destination-Host }
                    { Re-Auth-Request-Type }
                    [ Origin-State-Id ]
                    [ Auth-Session-State ]
                    [ Class ]
                    [ Removal-Cause ]
                   *[ Event-Trigger ]
                   *[ Charging-Rule-Remove ]
                   *[ Charging-Rule-Install ]
                    [ QoS-information ]
                    [ Authorization-Lifetime ]
                   *[ Proxy-Info ]
                   *[ Route-Record ]
                   *[ AVP ]
```

7.4.6 Re-Auth-Answer command

The RAA command, indicated by the Command-Code field set to 258 and the 'R' bit cleared in the Command Flags field, is sent by the PE-PE to the PD-PE in response to the RAR command.

The PI-Answer shall be used instead if the PD-PE has chosen stateless operation. In this case, the Session-Id shall contain an arbitrary value.

Message Format:

```
<RA-Answer> ::= < Diameter Header: 258, PXY >
                    < Session-Id >
                    { Origin-Host }
                    { Origin-Realm }
                    [ Result-Code ]
                   *[ Charging-Rule-Report]
                    [ Access-Network-Charging-Address ]
                   *[ Access-Network-Charging-Identifier-Gx ]
                    [ Experimental-Result ]
                    [ Origin-State-Id ]
                    [ Class ]
                    [ Error-Message ]
                    [ Error-Reporting-Host ]
                   *[ Failed-AVP ]
                   *[ Proxy-Info ]
                   *[ AVP ]
```

7.4.7 Abort-Session-Request command

The ASR command, indicated by the Command-Code field set to 274 and the 'R' bit set in the Command Flags field, is sent by the PD-PE to inform the PE-PE that all transport resources for the authorized session have become unavailable.

The PI-Request shall be used instead if the PD-PE has chosen stateless operation. In this case, the Session-Id shall contain an arbitrary value.

Message Format:

```
<AS-Request>  ::= < Diameter Header: 274, REQ, PXY >
                  < Session-Id >
                  { Origin-Host }
                  { Origin-Realm }
                  { Destination-Realm }
                  { Destination-Host }
                  { Auth-Application-Id }
                  { Abort-Cause }
                  [ Authorization-Token ]
                  [ Origin-State-Id ]
                 *[ Proxy-Info ]
                 *[ Route-Record ]
                  [ AVP ]
```

7.4.8 Abort-Session-Answer command

The ASA command, indicated by the Command-Code field set to 274 and the 'R' bit cleared in the Command Flags field, is sent by the PE-PE to the PD-PE in response to the ASR command.

The PI-Answer shall be used instead if the PD-PE has chosen stateless operation.

Message Format:

```
<AS-Answer>  ::=  < Diameter Header: 274, PXY >
                  < Session-Id >
                  { Origin-Host }
                  { Origin-Realm }
                  [ Authorization-Token ]
                  [ Result-Code ]
                  [ Experimental-Result ]
                  [ Origin-State-Id ]
                  [ Error-Message ]
                  [ Error-Reporting-Host ]
                 *[ Failed-AVP ]
                 *[ Redirected-Host ]
                  [ Redirected-Host-Usage ]
                  [ Redirected-Max-Cache-Time ]
                 *[ Proxy-Info ]
                 *[ AVP ]
```

7.5 State machine

This Recommendation reuses the authorization state machine defined in section 8.1 of the IETF Diameter Base Protocol (IETF RFC 6733]) with its own command codes and QoS AVPs as defined in clauses 7.4 and 7.3.

7.5.1 Supplemented states for PD-PE initiated session

In addition to the reused state machines, the following states are supplemented to the first two state machines in which the session state is maintained on the Diameter Server (i.e., PD-PE), and shall be supported in any QoS application implementations in support of PD-PE initiated session for push mode.

The states in Table 10 are supplemented to the state machine on the Diameter Server (i.e., PD-PE):

Table 10 – Supplemented states in Diameter SERVER, STATEFUL

State	Event	Action	New State
Idle	An application or local event triggers an initial QoS request to the PD-PE	Send PIR initial request	Pending
Pending	Received PIA with a failed Result-Code	Cleanup	Idle
Pending	Received PIA with Result-Code = SUCCESS	Update session status	Open
Pending	Error in processing received PIA with Result-Code = SUCCESS	Send ASR	Disconnect

The states in Table 11 are supplemented to the state machine on the client:

Table 11 – Supplemented states in Diameter CLIENT, STATEFUL

State	Event	Action	New State
Idle	PIR initial request received and successfully processed	Send PIA initial answer, reserve resources	Open
Idle	PIR initial request received and NOT successfully processed	Send PIA initial answer with Result-Code != SUCCESS	Idle

Bibliography

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

[b-3GPP TS 23.203] 3GPP TS 23.203 (Release 7), *Universal Mobile Telecommunications System (UMTS); Policy and charging control architecture.*

[b-3GPP TS 29.212] 3GPP TS 29.212 (Release 7), *Universal Mobile Telecommunications System (UMTS); Policy and charging control over Gx reference point.*

[b-3GPP TS 29.213] 3GPP TS 29.213 (Release 7), *Universal Mobile Telecommunications System (UMTS); Policy and charging control signalling flows and Quality of Service (QoS) parameter mapping*.

[b-3GPP TS 29.214] 3GPP TS 29.214 (Release 7), *Universal Mobile Telecommunications System (UMTS); Policy and charging Control over Rx reference point*.

[b-ETSI TS 124 008] ETSI TS 124 008 V6.19.0 (2008), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Mobile radio interface Layer 3 specification; Core network protocols; Stage 3 (3GPP TS 24.008 version 6.19.0 Release 6).*

[b-ETSI TS 129 061] ETSI TS 129 061 V6.13.0 (2007), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN) (3GPP TS 29.061 version 6.13.0 Release 6).*

[b-ETSI TS 129 207] ETSI TS 129 207 V6.5.0 (2005),*Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Policy control over Go interface (3GPP TS 29.207 version 6.5.0 Release 6).*

[b-ETSI TS 129 209] ETSI TS 129 209 V6.7.0 (2007), *Universal Mobile Telecommunications System (UMTS); Policy control over Gq interface (3GPP TS 29.209 version 6.7.0 Release 6).*

[b-ETSI TS 133 210] ETSI TS 133 210 V6.6.0 (2006), *Digital cellular telecommunications system (Phase 2+);Universal Mobile Telecommunications System (UMTS);3G security; Network Domain Security (NDS); IP network layer security (3GPP TS 33.210 version 6.6.0 Release 6).*

[b-ETSI TS 183 017] ETSI TS 183 017 V1.4.0 (2007), *Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control: Diameter protocol for session-based policy set-up information exchange between the Application Function (AF) and the Service Policy Decision Function (SPDF); Protocol Specification.*

[b-ETSI ES 283 034] ETSI ES 283 034 V1.5.0 (2008), *Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Network Attachment Sub-System (NASS); e4 interface based on the Diameter protocol.*

[b-IANA] Internet Assigned Numbers Authority, *Private Enterprise Numbers.* <http://www.iana.org/assignments/enterprise-numbers/enterprise-numbers>

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	**Switching and signalling**
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2014