International Telecommunication Union

ITU-T Q.3321.1

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(06/2010)

SERIES Q: SWITCHING AND SIGNALLING

Signalling requirements and protocols for the NGN – Resource control protocols

Resource control protocol No.1, version 2 – Protocol at the Rs interface between service control entities and the policy decision physical entity

Recommendation ITU-T Q.3321.1

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 NGN networks	Q.3900–Q.3999

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

Recommendation ITU-T Q.3321.1

Resource control protocol No. 1, version 2 – Protocol at the Rs interface between service control entities and the policy decision physical entity

Summary

Recommendation ITU-T Q.3321.1 specifies the *rcp1* protocol, a protocol between service control entities (SCEs) in the services stratum and the policy decision physical entity (PD-PE) in the resource and admission control function block. This protocol can be used to request and commit transport resources, to retrieve address mapping information that can be used to modify application signalling, and to receive reports on transport resource usage for charging. It satisfies the requirements for information flows across the Rs reference point as specified in clause 8.1 of Recommendation ITU-T Y.2111.

Recommendation ITU-T Q.3321.1 supersedes Recommendation ITU-T Q.3301.1 (03/2007).

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T Q.3321.1	2010-06-13	11

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/.

CONTENTS

Recommendation ITU-T Q.3321.1

Resource control protocol No. 1, version 2 – Protocol at the interface between service control entities and the policy decision physical entity

1 Scope

This Recommendation provides the stage 3 specification of the protocol at the interface between service control entities (SCEs) and the policy decision physical entity (PD-PE). The functional requirements and the stage 2 specifications for this interface are contained in clause 8.1 of [ITU-T Y.2111] and in [b-ITU-T Q-Sup.51]. This interface is used to control session-based policy.

Using the protocol specified in this Recommendation, the SCE can:

- provide information to the PD-PE to identify media flows and their required QoS resource characteristics (e.g., QoS class, bandwidth, priority);
- provide service priority information to the PD-PE to facilitate appropriate priority handling;
- request resource usage information through the PD-PE for charging;
- provide related service information to the PD-PE to facilitate appropriate dynamic firewall working mode selection;
- indicate whether the media should be enabled (i.e., gate opened) when resources are reserved;
- in those instances where the media should not be enabled as soon as the resources are reserved, i.e., may request that the gate be opened later;
- in the case where a NAPT function is required, request address mapping information so it can do any modifications that may be required to address information within application signalling (e.g., SDP); and
- in the case where a path-coupled resource reservation mechanism is used, indicate to the PD-PE whether it wishes to be notified when reservations are obtained and released.

When an authorization token mechanism is used, the PD-PE may supply the SCE with one or more authorization tokens which the SCE shall include in application signalling to the CPE.

2 References

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

[ITU-T Y.2111] Recommendation ITU-T Y.2111 (2008), *Resource and admission control functions in next generation networks*.

[ETSI TS 129 209] ETSI TS 129 209 V6.4.0 (2005), *Universal Mobile Telecommunications System (UMTS); Policy control over Gq interface* (3GPP TS 29.209 version 6.4.0 Release 6).

[ETSI TS 129 214] ETSI TS 129 214 V7.4.0 (2008), *Universal Mobile Telecommunications System (UMTS);Policy and charging control over Rx reference point* (3GPP TS 29.214 version 7.4.0 Release 7).

[ETSI TS 129 329] ETSI TS 129 329 V6.7.0 (2006), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Sh interface based on the Diameter protocol; Protocol details* (3GPP TS 29.329 version 6.7.0 Release 6).

[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).

[ETSI TS 183 017] ETSI TS 183 017 V1.1.1 (2006), *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*.

[ETSI ES 283 026] ETSI ES 283 026 V1.1.1 (2006), *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control; Protocol for QoS reservation information exchange between the Service Policy Decision Function (SPDF) and the Access-Resource and Admission Control Function (A-RACF) in the Resource and Protocol specification*.

[ETSI ES 283 034] ETSI ES 283 034 V1.1.1 (2006), *Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Network Attachment Sub-System (NASS); e4 interface based on the DIAMETER protocol*.

[IETF RFC 2960] IETF RFC 2960 (2000), *Stream Control Transmission Protocol*.

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

[IETF RFC 3264] IETF RFC 3264 (2002), *An Offer/Answer Model with Session Description Protocol (SDP)*.

[IETF RFC 3309] IETF RFC 3309 (2002), *Stream Control Transmission Protocol (SCTP) Checksum Change*.

[IETF RFC 3388] IETF RFC 3388 (2002), *Grouping of Media Lines in the Session Description Protocol (SDP)*.

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

[IETF RFC 3524] IETF RFC 3524 (2003), *Mapping of Media Streams to Resource Reservation Flows*.

[IETF RFC 3550] IETF RFC 3550 (2003), *RTP: A Transport Protocol for Real-Time Applications*.

[IETF RFC 3556] IETF RFC 3556 (2003), *Session Description Protocol (SDP) Bandwidth Modifiers for RTP Control Protocol (RTCP) Bandwidth*.

[IETF RFC 3588] IETF RFC 3588 (2003), *Diameter Base Protocol*.

[IETF RFC 4005] IETF RFC 4005 (2005), *Diameter Network Access Server Application*.

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

3 Definitions

This Recommendation defines the following terms:

3.1 attribute-value pair (AVP): An attribute-value pair corresponds to an Information Element in a Diameter message. See [IETF RFC 3588].

3.2 downlink: In the direction from the network toward a specified instance of user equipment.

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

NOTE – In stateful operation, hard-state reservations are terminated when the DIAMETER session is terminated. In stateless operation, hard-state reservations are terminated by explicit request.

3.4 IP flow: An IP flow is a unidirectional flow of data packets between specified transport end points (ports), sharing a common description in terms of the service requirements specified by the SCE.

NOTE – An IP flow will often have a counterpart flow in the opposite direction. In this Recommendation, the description of service requirements for an IP flow and its counterpart, if any, is mapped to a Media-Sub-Component AVP (see clause 9.3.28).

3.5 SCE session: A session established by a service/session control signalling protocol offered by the SCE that requires a session set-up with explicit session description before the use of the service.

NOTE – One example of a SCE session is an IMS session.

3.6 SCE session signalling protocol: The signalling protocol used to control the SCE session.

NOTE – One example of an SCE session signalling protocol is SIP with SDP.

3.7 soft-state reservation: A type of reservation whereby the requested resources are reserved for a finite amount of time. In stateful operation, soft-state reservations are terminated if the DIAMETER session is terminated.

3.8 uplink: In the direction from a specified instance of user equipment toward the network.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations:

AAA	AA-Answer
AAR	AA-Request
ASA	Abort-Session-Answer
ASR	Abort-Session-Request
AVP	Attribute-Value Pair
CGPD-PE	CPN Gateway Policy Decision – Physical Entity
CGPE-PE	CPN Gateway Policy Enforcement – Physical Entity
CPN	Customer Premises Network
FQDN	Fully Qualified Domain Name
GCID	GPRS Charging ID
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
IANA	Internet Assigned Numbers Authority

IMS IP Multimedia Subsystem

IP-CAN IP-Connectivity Access Network

NAPT Network Address and Port Translation

NASREQ Network Access Server Application

P-CSCF Proxy-Call Session Control Function

PD-PE Policy Decision Physical Entity

PDP Policy Decision Point

PE-PE Policy Enforcement Physical Entity

PNA Push-Notifications-Answer

PNR Push-Notification-Request

RAA Re-Auth-Answer

RACF Resource and Admission Control Functions

RAR Re-Auth-Request

RTCP Real-time Transport Control Protocol [IETF RFC 3550]

RTP Real-Time Transport Protocol [IETF RFC 3550]

SCE Service Control Entity

SDI Session Description Information

SDP Session Description Protocol [IETF RFC 4566]

SIP Session Initiation Protocol [IETF RFC 3261]

STA Session-Termination-Answer

STR Session-Termination-Request

UE User Equipment

5 Rs interface

5.1 Overview

The Rs interface is used for information exchange to apply policy between the PD-PE and the SCE, e.g., the P-CSCF. As defined in the stage 2 specifications [ITU-T Y.2111] and [b-ITU-T Q-Sup.51], this information is used by the PD-PE for policy decisions.

The Rs interface may be an intra- or inter-operator interface. One PD-PE instance shall be able to serve more than one SCE instance and one given SCE instance may interact with a number of PD-PE instances, although for any one session one SCE instance shall interact with only a single PD-PE instance.

5.2 Rs reference model

The Rs interface, as shown in Figure 5-1, is defined between the SCE and the PD-PE. The Rs interface is used for requesting transport plane resources and admission control.

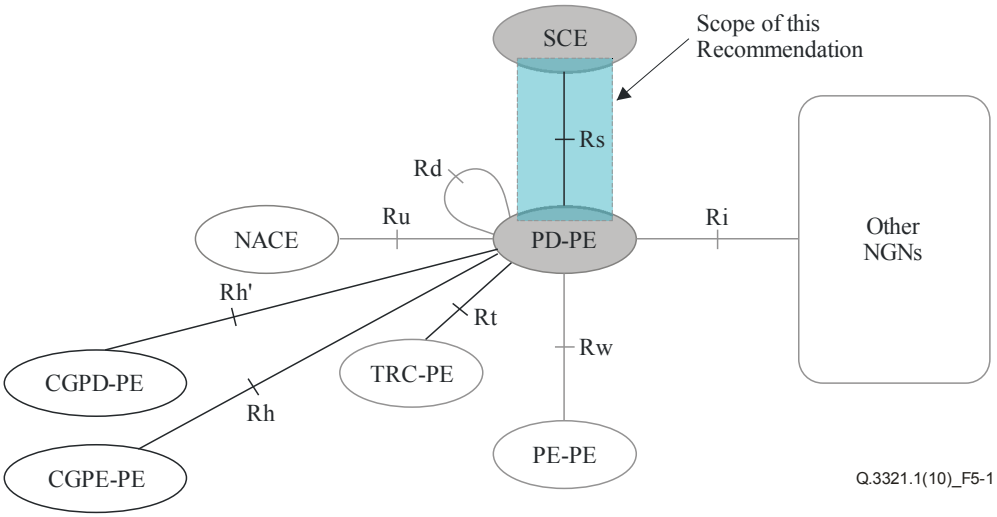

Figure 5-1 – Rs reference model

5.3 Functional elements and capabilities

5.3.1 Policy decision physical entity

The policy decision physical entity (PD-PE) is a functional element that coordinates the resource reservation requests received from the SCE. The PD-PE makes policy decisions using policy rules and forwards the session and media related information obtained from the SCE to the TRC-PE for admission control purposes. Additionally, based on information received on the Rs interface and on configuration data, the PD-PE may request the instantiation of a gate via the Rw interface. The Rw interface is outside the scope of this Recommendation. The functionality of the PD-PE is further detailed in clause 7.2.3 of [ITU-T Y.2111].

5.3.2 Service control entity

The service control entity (SCE) is a network element in the service stratum offering applications that request and use IP bearer resources. The SCE shall use the Rs interface to exchange session and media related information with the PD-PE.

6 SCE session-specific procedures

6.1 Procedures at the PD-PE

6.1.1 Initial reservation for a session

An Auth-Session-State AVP may be present in the initial AA-Request to indicate the SCE's preference for stateful or stateless operation. The PD-PE may honour the preference indicated in such an Auth-Session-State AVP, or may make an independent decision based on local policy (whether or not it has received an Auth-Session-State AVP). If an Auth-Session-State AVP was present in the initial AA-Request or if the PD-PE chooses stateless operation for the current session, the PD-PE shall return an Auth-Session-State AVP in the AA-Answer to indicate its decision.

In stateful operation, the PD-PE stores the Session-Id value received in the AA-Request. The same Session-Id value will be present in subsequent commands relating to this session, as described in [IETF RFC 3588]. The PD-PE may use the received Session-Id values to locate the session context information in order to act on the commands.

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 this initial AA-Request;

– the address(es) of the TRC-PE(s) involved in the session;

– the address of the PE-PE involved in the session; and

– other session information.

The Class AVP(s) shall be returned to the SCE in the AA-Answer. The PD-PE also forwards equivalent state-preserving tokens to the TRC-PE(s) and PE-PE when it communicates with them, and receives those tokens back again in messages from them. Details are beyond the scope of this Recommendation.

The PD-PE may acquire user profile information from the TLM-FE in the NAC-PE according to the TLM-PE-Identifier AVP if present.

If the Operation-Indication AVP is present, the PD-PE may use it to determine whether the initial AA-Request is for:

– NAT control only:

  The PD-PE shall exercise NAPT control and NAT traversal function control at the PE-PE based on the information indicated by the Binding-Information AVP and SDP-Direction AVP (optional).

– QoS resource reservation only:

  The PD-PE shall perform QoS resource reservation based on the information indicated by the Resource-Reservation-Mode AVP and media information.

– QoS resource reservation and NAT control:

  The PD-PE shall perform both of the actions requested.

If the Resource-Reservation-Mode AVP is present, the PD-PE shall use it to determine whether the initial AA-Request is for:

– authorization only (pull mode);

– authorization and reservation (push mode, first phase of two); or

– authorization, reservation and commitment (push mode, single phase operation).

The operation indicated by the Resource-Reservation-Mode AVP applies to all IP flows identified by the AA-Request. If the Resource-Reservation-Mode AVP is not consistent with the Flow-Status AVP for individual components and sub-components, the request should be rejected.

A request for authorization only (pull mode) cannot be indicated in the absence of the Resource-Reservation-Mode AVP. However, the PD-PE can infer a request for reservation without commitment if Flow-Status for a given media component or sub-component is set to DISABLED (3), and a request for commitment if Flow-Status is set to any variant of ENABLED (0), (1), or (2).

Once the PD-PE recognizes, based on the contents of an AA-Request and possibly on configuration data, that policy enforcement functions are requested on the transport plane, the PD-PE shall use the contents of the AA-Request in order to enforce any functions needed over the Rt and Rw interfaces.

If the AA-Request contains the Media-Component-Description AVP(s), the PD-PE shall trigger the Resource Reservation procedure towards the TRC-PE. If the AA-Request contains Flow-Grouping AVP(s), the PD-PE shall only authorize the QoS if the IP flows are distributed to IP-CAN bearers in a way that is allowed by the Flow-Grouping AVP(s).

Additionally, based on the contents of the AA-Request (e.g., the AA-Request may contain AVPs such as Service-Class and Binding-Information) and on local policy rules, the PD-PE may request the instantiation of a gate.

The PD-PE shall wait for the result of the above interaction(s) before returning, in a single AA-Answer message, the result of those interactions to the SCE. The AA-Answer message shall be sent only after all actions taken upon the Rt and/or Rw interfaces are achieved. The contents of the AA-Answer shall be derived as follows:

– If the Resource Reservation procedure succeeds and if the requested binding information was received via the Rw interface, the AA-Answer message sent by the PD-PE to the SCE shall contain the allocated token in the Authorization-Token AVP (in pull mode) and the Binding-Output-List AVP (if requested in the first place). The Rw interface is outside the scope of this Recommendation.

– If the Resource Reservation procedure fails (i.e., the PD-PE receives a reservation failure notification via the Rt interface), the PD-PE shall return the Experimental-Result-Code AVP with the value INSUFFICIENT_RESOURCES in the AA-Answer. The PD-PE may additionally provide an indication of QoS resources available within the Acceptable-Service-Info AVP.

– If the Resource Reservation procedure succeeds but the PD-PE did not succeed in getting a binding via the Rw interface, the PD-PE shall return the Experimental-Result-Code AVP with the value BINDING_FAILURE in the AA-Answer. Additionally, the PD-PE shall release any associated requested resources over the Rt interface. The Rt interface is outside the scope of this Recommendation.

6.1.2 Session modification

The PD-PE may receive the AA-Request message from the SCE with modified service information. Based on the contents of the AA-Request, the PD-PE shall coordinate any required modifications to the existing resource reservation over the Rt interface and/or to the existing policy enforcement settings instanced via the Rw interface. As described in clause 6.1.1, the PD-PE shall acknowledge the session modification by issuing an AA-Answer back to the SCE only after all actions taken upon the Rt and/or Rw interfaces are achieved.

The Rt and Rw interfaces are outside the scope of this Recommendation.

Depending on the value of the Flow-Status AVP received from the SCE, the PD-PE shall interpret the session modification as a commitment of requested resources or as a removal of the commitment of requested resources.

Once the PD-PE recognizes, based on the contents of an AA-Request and possibly on configuration data, that policy enforcement functions are requested on the transport plane, the PD-PE shall use the contents of the AA-Request in order to enforce any functions needed over the Rw interface.

6.1.3 Session termination

Session termination is signalled by receipt of a Session-Termination-Request message from the SCE in stateful operation, or receipt of an AA-Request message containing the Resource-Reservation-Mode AVP with a value of RESOURCE_RELEASE (3) in stateless operation. Upon receiving a signal that the session is to be terminated, the PD-PE shall trigger the session termination procedure over the Rt interface and revoke any transport plane functions enforced over the Rw interface as a result of this session. The Rt and Rw interfaces are outside the scope of this Recommendation.

6.1.4 PD-PE notifications

The Rs interface supports facilities for indicating, on request basis, relevant events such as revocation of established resource reservations. The PD-PE sends unsolicited RA-Request (RAR) messages to the SCE. Such messages are implicitly requested through policies established in the PD-PE via the Specific-Action AVP of the initial AA-Request message.

The SCE may specify, in the Specific-Action AVP of the initial AA-Request command, the events it wants to be informed of (see clause 9.3.23).

If one of the events supported at the Rs interface occurs, the PD-PE shall send an unsolicited RAR message to the SCE containing:

– the value of the Specific-Action AVP, indicating the event that occurred; and

– optionally, the appropriate Abort-Cause AVP value.

6.2 Procedures at the SCE

6.2.1 Initial reservation for a session

Upon receipt of an SCE session signalling message initiating a new SCE session, the SCE shall request an authorization for the session from the PD-PE by sending the AA-Request message. This AA-Request message shall contain a new Session-Id.

NOTE – As specified in [IETF RFC 3588], 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 DiameterIdentity type.

The AA-Request may contain an Authorization-Lifetime AVP as a hint of the maximum lifetime that it is requesting.

The AA-Request may include an Auth-Session-State AVP as a hint of the SCE's preference for stateful or stateless operation.

The SCE may include the Operation-Indication AVP to indicate whether the PD-PE must perform NAPT control and NAT traversal functions or QoS resource reservation or both after receiving the AA-Request.

The SCE shall include the corresponding Media-Component-Description AVP(s) into the message if the SDI is already available at the SCE. The SCE may include the Flow-Grouping AVP(s) to request a particular way for the IP flows described within the service description to be distributed to IP-CAN bearers.

When providing a given Media-Component-Description AVP in the initial AA-Request, the SCE may request the PD-PE to commit the requested resources by setting the Flow-Status AVP to the value ENABLED, ENABLED-UPLINK or ENABLED-DOWNLINK. Alternatively, the SCE may perform this in two phases using separate reserve and commit operations. If commitment is done in two phases, the Flow-Status AVP value of the initial AA-Request shall be set to DISABLED.

If, based on local configuration data, the SCE determines that address translation needs to occur on the user plane (e.g., the PE-PE implements NAPT (-PT) or hosted NAPT procedures), upon receipt of SDI pointing towards the endpoint served by SCE (e.g., for IMS, the P-CSCF receives an SDP offer sent by the served UE), the SCE shall include the Binding-Information AVP with the Input-List AVP set based on the received SDI. The SCE may also include the SDP-Direction AVP along with the Binding-Information AVP to indicate whether the address set in the Output-list AVP expected to be received in the AA-Answer is in the access network/local core network or in the core network/peer core network.

If required (e.g., in cases where the served endpoint is behind a hosted-NAPT), the SCE may also include the Latching-Indication AVP set to "LATCH".

Based on local configuration data, the SCE may choose to specify firewall operation for the packets associated with the user session by including the Dynamic-Firewall-Working-Mode AVP.

Based on local configuration data, the SCE may include the TLM-PE-Identifier AVP in AA-Request to indicate the TLM-PE related to the user.

For the purpose of QoS profile correlation in a PD-PE lying within an access network, the SCE shall include within the AA-Request a correlation identifier in the form of:

– the User-Name AVP or;

– the Globally-Unique-Address AVP.

The User-Name AVP is defined in the Diameter base specification, [IETF RFC 3588]. The Globally-Unique-Address AVP is defined in the Diameter Network Access Server specification, [IETF RFC 4005].

The SCE may specify the Reservation-Priority AVP in the AA-Request and/or within a Media-Component-Description AVP of the AA-Request.

The SCE may specify the Specific-Action AVP in the AA-Request with the events it wants to be informed of.

The SCE shall examine the content of any Auth-Session-State AVP it receives in the AA-Answer message. If such an AVP is present and indicates stateful operation, the SCE shall include the same Session-Id value in subsequent messages relating to this session as it is placed in the initial AA-Request.

If a received Auth-Session-State AVP indicates stateless operation, the SCE shall store the value of the Class AVP(s) also present in the AA-Answer message. The SCE shall include the stored Class AVP(s) in any message it sends to the PD-PE relating to the same session.

The SCE shall store the contents of the Binding-Output-List AVP received within the Binding-Information AVP contained in the AA-Answer message for future use.

The behaviour when the SCE does not receive the AA-Answer, or when it arrives after the internal timer waiting for it has expired, or when it arrives with an indication different from DIAMETER_SUCCESS, is outside the scope of this Recommendation and is based on operator policy.

6.2.2 Session modification

During the SCE session modification, the SCE shall send an update for the session description information to the PD-PE based on the new SDI exchanged within the SCE session signalling. The SCE does this by sending the AA-Request message, with an existing Session-Id, containing the Media-Component-Description AVP(s) containing the updated service information. The SCE may include the Flow-Grouping AVP(s) to request a particular way for the IP flows described within the service description to be distributed to IP-CAN bearers.

The SCE may perform the following operations.

– Add a new IP flow within an existing media component – provide a new Media-Sub-Component AVP within the corresponding Media-Component-Description AVP.

– Add a new IP flow within a new media component – provide a new Media-Component-Description AVP.

– Modify a media component – update the corresponding Media-Component-Description AVP (e.g., increase or decrease the allocated bandwidth).

– Modify an existing IP flow within a media component – update the corresponding Media-Sub-Component AVP.

– Modify the commit status – change the Flow-Status AVP of the corresponding Media-Component-Description AVP and/or Media-Sub-Component to one of the values ENABLED-UPLINK (0), ENABLED-DOWNLINK (1) or ENABLED (2), according to the direction in which the resources are to be committed.

– Release a media component – provide the corresponding Media-Component-Description AVP with the Flow-Status AVP set to the value REMOVED (4).
– Release an IP flow within a media component – provide the corresponding Media-Sub-Component AVP with the Flow-Status AVP set to the value REMOVED (4).
– Refresh a soft-state – provide an Authorization-Lifetime AVP in the AA-Request as a hint of the maximum lifetime that it is requesting.

The SCE may also request the PD-PE to revoke the commitment of requested resources by setting the Flow-Status AVP to the value DISABLED.

If present, the Reservation-Priority AVP associated with a reservation request or a media component shall not be modified.

If updated SDI pointing towards the endpoint served by SCE is available, and if it determines that address translation needs to occur on the user plane (e.g., the PE-PE implements NAPT(-PT) or hosted NAPT procedures), the SCE shall include the Binding-Information AVP with the Binding-Input-List AVP set based on the received SDI.

If required (e.g., in cases where the served endpoint is behind a hosted-NAPT), the SCE may also include the Latching-Indication AVP set to "RELATCH".

The SCE may modify firewall operation for the packets associated with the user session by including the Dynamic-Firewall-Working-Mode AVP.

The SCE shall store the contents of the Binding-Output-List AVP received within the Binding-Information AVP contained in the AA-Answer message for future use.

The behaviour when the SCE does not receive the AA-Answer, or when it arrives after the internal timer waiting for it has expired, or when it arrives with an indication different from DIAMETER_SUCCESS, is outside the scope of this Recommendation and is based on operator policy.

6.2.3 Session termination

When the SCE session is terminated, for stateful operation the SCE shall terminate the Diameter session by sending a Session-Termination-Request message with the associated Session-Id AVP to the PD-PE. In stateless operation, it shall request session termination by sending an AA-Request containing the associated Class AVP and the Resource-Reservation-Mode AVP with a value of RESOURCE_RELEASE (3).

6.3 IMS-related SCE procedures

6.3.1 Provision of service information by the SCE

The SCE shall send service information to the PD-PE upon every SIP message that includes an SDP answer payload. The service information shall be derived both from the SDP offer and the SDP answer. This ensures that the PD-PE receives proper information for all possible IMS session set-up scenarios, and that the PD-PE is also capable of handling session modifications.

All media components in the SDP shall be sent. Therefore, the SCE shall derive a media component within the session information from every SDP media component, as detailed in Annex B. The SDP contains sufficient information about the session, such as the end-points' IP address and port numbers and bandwidth requirements.

The SCE shall derive the Flow-Description AVP within the service information from the SDP as follows:

a) An uplink Flow-Description AVP shall be formed as follows: The destination address and port number shall be taken from the c= and m= lines of the SDP sent by the SCE in the downlink direction, while the source IP address may be formed from the address present in

the SDP received by the SCE in the uplink direction, and the source port number shall be wildcarded. For example, assuming UE A sends an SDP to UE B, the PD-PE of UE B uses the address present in this SDP for the destination address of UE B's uplink Flow-Description AVP, while the PD-PE of the UE A uses the same address for the source address of UE A's uplink Flow-Description AVP. In the case of IPv6, if the source address is not formed from the 64-bit prefix, the source address shall be wildcarded.

b) A downlink Flow-Description AVP shall be formed as follows: The destination address and port number shall be taken from the connection information parameter of the SDP received by the SCE in the uplink direction, while the source IP address may be formed (in order to reduce the possibilities of bearer misuse) from the destination address in the SDP sent by the SCE in the downlink direction (taking into account only the 64-bit prefix of an IPv6 address) and the source port number shall be wildcarded. For example, assuming UE A sends an SDP to UE B, the PD-PE of UE A uses the address present in this SDP for the destination address of UE A's downlink Flow-Description AVP, while the PD-PE of UE B uses the 64-bit prefix of the same address for the source address of UE B's downlink Flow-Description AVP. If the source address is not formed from the 64-bit prefix, the source address shall be wildcarded.

The SCE shall derive the bandwidth information within the service information, from the "b=AS" SDP parameter, as detailed in Annex B. For the possibly associated RTCP IP flows, the SCE shall use the SDP "b=RR" and "b=RS" parameters, if present, as specified in Annex B. The "b=AS", "b=RR" and "b=RS" parameters in the SDP contain all the overhead coming from the IP-layer and the layers above, e.g., IP, UDP, RTP and RTCP payload, or IP, UDP and RTCP.

6.3.2 Enabling IP flows at the SCE

Prior to the completion of the SIP session set-up, i.e., until the 200 OK INVITE is received, the SCE may enable or disable media IP flows depending on operator policy, thus allowing or forbidding early media in the forward and/or backward direction. If early media is to be disabled, the SCE may modify the values of the Flow-Status AVPs derived from SDP according to Annex B. If the SCE chooses to modify the values, the SCE shall store the last received SDP.

When the 200 OK is received, the SCE shall enable all media IP flows according to the direction attribute within the last received SDP, as specified in Annex B. When the 200 OK is received and the SCE previously provided modified values of the Flow-Status AVPs in the session information, the SCE shall provide service information with values of the Flow-Status AVPs corresponding to the last received SDP.

If the SCE receives SDP answers after the completion of the SIP session set-up, i.e., after the 200 OK INVITE is received, the SCE shall provide the Flow-Status AVPs as derived from the SDP according to Annex B.

7 Protocol specification

The Diameter Base Protocol as specified in [IETF RFC 3588] is used to support information transfer on the Rs interface. [IETF RFC 3588] shall apply except as modified by the additional methods, commands, Attribute-Value Pairs (AVPs), and result and event codes specified in this Recommendation. Unless otherwise indicated, the procedures of [IETF RFC 3588] (including error handling and unrecognized information handling) are unmodified.

In addition to the AVPs from the Diameter base application [IETF RFC 3588], the Diameter messages sent over the Rs interface use the AVPs defined in clause 9.3.

This Recommendation defines the Rs Diameter application with application ID 16777235. The vendor identifier assigned by IANA to ITU-T (http://www.iana.org/assignments/enterprise-numbers) is 11502.

This Recommendation defines no new Diameter commands, but instead reuses commands defined by the IETF and by 3GPP. To maximize interoperability, this Recommendation supports all of the mandatory attributes specified for these commands in their original documents. However, in some cases default values and behaviour are specified for the use of these attributes in the Rs application, because the application does not really require them.

With regard to the Diameter protocol defined over the Rs 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 SCE acts as the Diameter client, in the sense that it is the network element requesting authorization to use bearer path network resources.

The support of Diameter agents between the PD-PE and the SCE may not be necessary when the Rs interface is intra-operator, e.g., for IMS.

8 Use of the Diameter base protocol

With the clarifications listed in the following clauses, the Diameter Base Protocol defined by [IETF RFC 3588] shall apply.

8.1 Securing Diameter messages

For secure transport of Diameter messages, the method defined in [ETSI TS 133 210] (3GPP TS 33.210) shall be used.

8.2 Accounting functionality

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

8.3 Use of sessions

As described in clauses 6.1 and 6.2, an operation for a given session may be stateful or stateless. A stateless operation is always indicated definitively by a value of NO_STATE_MAINTAINED in an Auth-Session-State AVP returned by the PD-PE in the AA-Answer response to the initial AA-Request. For stateful operation, the Session-Id AVP shall be present in all messages passing between the SCE and the PD-PE, as described in [IETF RFC 3588]. The Session-Termination-Request (STR) and Session-Termination-Answer (STA) commands defined in [IETF RFC 3588] shall be used in order to terminate the Diameter user sessions. For stateless operation, the Class AVP returned in the AA-Answer response to the initial AA-Request shall be present in all messages passing between the SCE and the PD-PE. The Diameter user session shall be terminated by sending an AA-Request containing the Class AVP and the Resource-Reservation-Mode AVP with a value of RESOURCE_RELEASE (3).

8.4 Transport protocol

Diameter messages over the Rs interface shall make use of SCTP [IETF RFC 2960] and shall utilize the new SCTP checksum method specified in [IETF RFC 3309].

8.5 Routing considerations

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

The SCE obtains the contact address of the PD-PE for a given user through the means identified in clause 7.3.1 of [ITU-T Y.2111]. Both the Destination-Realm and Destination-Host AVPs shall be present in the request.

To ensure that messages are routed to the correct application at the destination host, the Diameter message header of each message sent shall contain either the Rs application identifier (16777235) or the Gq application identifier (16777222) as agreed during CER/CEA negotiation. (See clause 8.6.)

8.6 Advertising application support

The Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands are specified in the Diameter Base Protocol [IETF RFC 3588]. The Diameter base application identifier (0) shall be used in the Diameter message header of these messages.

The SCE and the PD-PE shall advertise the support of the Rs and/or Gq applications by including an instance of the Vendor-Specific-Application-Id grouped AVP within the Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands for each application supported, according to the following rules:

1) The SCE shall advertise support of the Rs application if it supports stateless operation and of the Gq application if it supports stateful operation. It shall advertise both applications if it supports both operating modes.
2) The PD-PE shall respond by indicating the subset of applications it is prepared to support, out of those offered by the SCE. If this subset is empty, the PD-PE's response shall be as described in section 5.3 of [IETF RFC 3588].

If both the SCE and the PD-PE indicate support of the Rs application, then the Rs application identifier (16777235) shall be used in the Diameter message header of all subsequent messages exchanged within this association. Otherwise, the Gq application identifier (16777222) shall be placed in those headers.

Support of the Rs application within the CER/CEA is indicated by supplying an instance of the Vendor-Specific-Application-Id containing a Vendor-Id AVP set to ITU-T (11502) and an Auth-Application-Id AVP set to Rs (16777235). Support of the Gq application within the CER/CEA is indicated by supplying an instance of the Vendor-Specific-Application-Id containing a Vendor-Id AVP set to 3GPP (10415) and an Auth-Application-Id AVP set to Gq (16777222).

NOTE – The Vendor-Id AVP included in Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands at the command level (as opposed to the Vendor-Id instances within the Vendor-Specific-Application-Id AVPs as described in the previous paragraph) shall indicate the manufacturer of the Diameter node as per [IETF RFC 3588].

The SCE and PD-PE shall advertise the support of AVPs specified in 3GPP, ETSI, and ITU-T documents by including the values 10415 (3GPP), 13019 (ETSI) and 11502 (ITU-T) in three different instances of the Supported-Vendor-Id AVP in the CER and CEA commands respectively.

9 Message specification

9.1 Commands

Existing Diameter command codes from the Diameter base protocol [IETF RFC 3588], the Network Access Server Diameter application ([IETF RFC 4005]) and the Sh application [ETSI TS 129 329] are used. Support for these commands is required as indicated in Tables 1 and 2.

NOTE – The notion of NAS (network access server) is not used here; [IETF RFC 4005] is just used for protocol purposes, not for its functional meaning.

Table 1 – Commands that must be supported for stateful operation

Command	Abbreviation	Defining reference	Command code	See clause
AA-Request	AAR	[IETF RFC 4005]	265	9.1.1
AA-Answer	AAA	[IETF RFC 4005]	265	9.1.2
Re-Auth-Request	RAR	[IETF RFC 3588]	258	9.1.3
Re-Auth-Answer	RAA	[IETF RFC 3588]	258	9.1.4
Session-Termination-Request	STR	[IETF RFC 3588]	275	9.1.5
Session-Termination-Answer	STA	[IETF RFC 3588]	275	9.1.6
Abort-Session-Request	ASR	[IETF RFC 3588]	274	9.1.7
Abort-Session-Answer	ASA	[IETF RFC 3588]	274	9.1.8
NOTE – [IETF RFC 3588] also requires every application to provide at least minimal support of accounting, including the ACR/ACA commands defined in that RFC.				

Table 2 – Commands that must be supported for stateless operation

Command	Abbreviation	Defining reference	Command code	See clause
AA-Request	AAR	[IETF RFC 4005]	265	9.1.1
AA-Answer	AAA	[IETF RFC 4005]	265	9.1.2
Push-Notification-Request	PNR	[ETSI TS 129 329]	309	9.1.9
Push-Notifications-Answer	PNA	[ETSI TS 129 329]	309	9.1.10
NOTE 1 – Stateless operation is supported by the Rs application only. NOTE 2 – [IETF RFC 3588] also requires every application to provide at least minimal support of accounting, including the ACR/ACA commands defined in that RFC.				

The Rs or Gq specific application identifier is used together with the command code within the Diameter header of each message, according to the rules specified in clause 8.6.

As specified by [IETF RFC 3588], the application identifier appearing in the Diameter message header shall also be placed in the Auth-Application-Id AVP at the top level or within the Vendor-Specific-Application-Id AVP, as applicable depending on the command.

9.1.1 AA-Request (AAR) command

The AAR command is imported from [IETF RFC 4005]. It is indicated by the Command-Code field set to 265 and the 'R' bit set in the Command Flags field. The AAR command includes a mandatory Auth-Application-Id AVP which shall be used to confirm the Gq or Rs application identifier value placed in the Diameter message header. As defined in [IETF RFC 4005], it also contains the mandatory Auth-Request-Type AVP. Within the Gq or Rs applications, as defined by this Recommendation, this AVP shall always be set to AUTHORIZE_ONLY (2). The other mandatory AVPs have their normal usage, which is independent of the application.

The AAR command is sent by an SCE to the PD-PE in order to request or modify the authorization for the bearer usage for the SCE session. In stateless operation, an AAR command with one or more Class AVPs and the Resource-Reservation-Mode AVP with a value of RESOURCE_RELEASE (3) is sent to terminate a session (i.e., cause release of all resources associated with a session).

The Auth-Session-State AVP may be present only in the initial AAR command for a session. The Authorization-Token and Class AVPs shall not be present in the initial AAR command for a

session. The Class AVP(s) shall be present in all subsequent AAR commands for a session if the PD-PE has chosen stateless operation.

The Connection-Status-Timer AVP may be present in the initial AAR command to indicate the frequency that the PD-PE can run the connection status procedure. The connection status procedure enables the PD-PE to query the SCE as to whether the particular Rs session is still known at the SCE level.

Message format:

```
<AA-Request> ::= < Diameter Header: 265, REQ, PXY, 167772xx >
                 < Session-Id >
                 { Auth-Application-Id }
                 { Origin-Host }
                 { Origin-Realm }
                 { Destination-Realm }
                 { Auth-Request-Type }
                 *[ Media-Component-Description ]
                 *[ Flow-Grouping ]
                  [ AF-Charging-Identifier ]
                  [ SIP-Forking-Indication ]
                 *[ Specific-Action ]
                  [ User-Name ]
                  [ Binding-Information ]
                  [ Latching-Indication ]
                  [ Dynamic-Firewall-Working-Mode ]
                  [ Resource-Reservation-Mode ]
                  [ Reservation-Priority ]
                  [ Globally-Unique-Address ]
                  [ Authorization-Lifetime ]
                 *[ Proxy-Info ]
                 *[ Route-Record ]
                  [ Service-Class ]
                  [ Connection-Status-Timer]
                  [ Origin-State-Id ]
                  [ Auth-Session-State ]
                  [ Authorization-Token ]
                 *[ Class ]
                  [SDP-Direction]
                  [Operation-Indication]
                  [TLM-PE-Identifier]
                 *[ AVP ]
```

9.1.2 AA-Answer (AAA) command

The AAA command is imported from [IETF RFC 4005]. It is indicated by the Command-Code field set to 265 and the 'R' bit cleared in the Command Flags field. The AAA command includes a mandatory Auth-Application-Id AVP which shall be used to confirm the Gq or Rs application identifier value placed in the Diameter message header. As defined in [IETF RFC 4005], it also contains the mandatory Auth-Request-Type AVP. Within the Gq or Rs applications, as defined by this Recommendation, this AVP shall always be set to AUTHORIZE_ONLY (2). The other mandatory AVPs have their normal usage, which is independent of the application.

The AAA command is sent by the PD-PE to the SCE in response to the AAR command.

The Auth-Session-State AVP may be present only in the AAA command responding to the initial AAR command. If the PD-PE has chosen stateless operation for the session, the Class AVP(s) shall be present in all AAA commands returned to the SCE.

The Connection-Status-Timer AVP should be present in the AAA command responding to the initial AAR command containing the AVP. The value of the timer in the AAA command is the final negotiated value of the timer. The connection status procedure should be initiated in the interval less

than this value, making sure that SCE can receive at least one message before the Connection-Status-Timer times out.

The method for how to determine the final negotiated value of the timer is not specified.

Message format:

```
<AA-Answer> ::=  < Diameter Header: 265, PXY, 167772xx >
                < Session-Id >
                { Auth-Application-Id }
                { Origin-Host }
                { Origin-Realm }
                { Auth-Request-Type }
                { Result-Code }
                 [ Experimental-Result ]
                 [ Auth-Session-State ]
                 [ Authorization-Token ]
                *[ Access-Network-Charging-Identifier ]
                 [ Access-Network-Charging-Address ]
                 [Acceptable-Service-Info]


                 [ Binding-Information ]
                 [ Reservation-Priority ]
                 [ Error-Message ]
                 [ Error-Reporting-Host ]
                 [ Authorization-Lifetime ]
                 [ Auth-Grace-Period ]
                *[ Class ]
                *[ Failed-AVP ]
                *[ Redirect-Host ]
                 [ Redirect-Host-Usage ]
                 [ Redirect-Max-Cache-Time ]
                *[ Proxy-Info ]
                 [ Connection-Status-Timer]
                 [ Origin-State-Id ]
                *[ AVP ]
```

9.1.3 Re-Auth-Request (RAR) command

The RAR command is imported from [IETF RFC 3588]. It is indicated by the Command-Code field set to 258 and the 'R' bit set in the Command Flags field. The RAR command includes a mandatory Auth-Application-Id AVP which shall be used to confirm the Gq or Rs application identifier value placed in the Diameter message header. As defined in [IETF RFC 3588], it also contains the mandatory Re-Auth-Request-Type AVP. Within the Gq or Rs applications, as defined by this Recommendation, this AVP shall always be set to AUTHORIZE_ONLY (0). The other mandatory AVPs specified in [IETF RFC 3588] have their normal usage, which is independent of the application.

The RAR command is sent by the PD-PE to the SCE in order to indicate a specific action. In stateless operation, the PNR command described in clause 9.1.9 shall be used instead of the RAR command.

As an option, the SCE may send an AAR command to the PD-PE to update the service information after responding to an RAR command or its PNR alternative. However, this Recommendation does not mandate application-specific authentication and/or authorization messages in response to an RAR command or its PNR alternative.

The values INDICATION_OF_LOSS_OF_BEARER, INDICATION_OF_RECOVERY_OF_ BEARER and INDICATION_OF_RELEASE_ OF_BEARER of the Specific-Action AVP shall not be combined with each other in a Re-Auth-Request or its PNR alternative.

Message format (RAR):

```
<RA-Request> ::= < Diameter Header: 258, REQ, PXY, 167772xx >
                 < Session-Id >
                 { Origin-Host }
                 { Origin-Realm }
                 { Destination-Realm }
                 { Destination-Host }
                 { Auth-Application-Id }
                 { Re-Auth-Request-Type }
                 1*{ Specific-Action }
                 *[ Access-Network-Charging-Identifier ]
                  [ Access-Network-Charging-Address ]
                 *[ Flows ]
                  [ Binding-Information ]
                  [ Dynamic-Firewall-Working-Mode ]
                  [ Abort-Cause ]
                  [ Origin-State-Id ]
                 *[ Proxy-Info ]
                 *[ Route-Record ]
                 *[ AVP ]
```

9.1.4 Re-Auth-Answer (RAA) command

The RAA command is imported from [IETF RFC 3588]. It is indicated by the Command-Code field set to 258 and the 'R' bit cleared in the Command Flags field. The mandatory AVPs specified in [IETF RFC 3588] have their normal usage, which is independent of the application.

The RAA command is sent by the SCE to the PD-PE in response to the RAR command. In stateless operation of the PD-PE, the PNA command described in clause 9.1.10 shall be used instead of the RAA command.

Message format (RAA):

```
<RA-Answer> ::=  < Diameter Header: 258, PXY, 167772xx >
                 < Session-Id >
                 { Origin-Host }
                 { Origin-Realm }
                 { Result-Code }
                  [ Experimental-Result ]
                 *[ Media-Component-Description ]
                 *[ Flow-Grouping ]
                  [ Reservation-Priority ]
                  [ AF-Charging-Identifier ]
                 *[ Specific-Action ]
                  [ Binding-Information ]
                  [ Latching-Indication ]
                  [ Dynamic-Firewall-Working-Mode ]
                  [ Origin-State-Id ]
                  [ Error-Message ]
                  [ Error-Reporting-Host ]
                 *[ Failed-AVP ]
                 *[ Redirect-Host ]
                  [ Redirect-Host-Usage ]
                  [ Redirect-Max-Cache-Time ]
                 *[ Proxy-Info ]
                 *[ AVP ]
```

9.1.5 Session-Termination-Request (STR) command

The STR command is imported from [IETF RFC 3588]. It is indicated by the Command-Code field set to 275 and the 'R' bit set in the Command Flags field. The STR command includes a mandatory Auth-Application-Id AVP which shall be used to confirm the Gq or Rs application identifier value placed in the Diameter message header. The other mandatory AVPs specified in [IETF RFC 3588] have their normal usage, which is independent of the application.

The STR command is sent by the SCE to the PD-PE to terminate an authorized session in stateful operation.

Message format:

```
<ST-Request> ::= < Diameter Header: 275, REQ, PXY, 167772xx >
                 < Session-Id >
                 { Origin-Host }
                 { Origin-Realm }
                 { Destination-Realm }
                 { Termination-Cause }
                 { Auth-Application-Id }
                  [ Destination-Host ]
                  [ Origin-State-Id ]
                  [ Reservation-Priority ]
                 *[ Proxy-Info ]
                 *[ Route-Record ]
                 *[ AVP ]
```

9.1.6 Session-Termination-Answer (STA) command

The STA command is imported from [IETF RFC 3588]. It is indicated by the Command-Code field set to 275 and the 'R' bit cleared in the Command Flags field. The mandatory AVPs specified in [IETF RFC 3588] have their normal usage, which is independent of the application.

The STA command is sent by the PD-PE to the SCE in response to the STR command.

Message format:

```
<ST-Answer>  ::= < Diameter Header: 275, PXY, 167772xx >
                 < Session-Id >
                 { Origin-Host }
                 { Origin-Realm }
                 { Result-Code }
                  [ Experimental-Result ]
                  [ Error-Message ]
                  [ Error-Reporting-Host ]
                 *[ Failed-AVP ]
                  [ Origin-State-Id ]
                  [ Reservation-Priority ]
                 *[ Redirect-Host ]
                  [ Redirect-Host-Usage ]
                  [ Redirect-Max-Cache-Time ]
                 *[ Proxy-Info ]
                 *[ AVP ]
```

9.1.7 Abort-Session-Request (ASR) command

The ASR command is imported from [IETF RFC 3588]. It is indicated by the Command-Code field set to 274 and the 'R' bit set in the Command Flags field. The ASR command includes a mandatory Auth-Application-Id AVP which shall be used to confirm the Gq or Rs application identifier value placed in the Diameter message header. The other mandatory AVPs specified in [IETF RFC 3588] have their normal usage, which is independent of the application.

The ASR command is sent by the PD-PE to inform the SCE that all bearer resources for the authorized session have become unavailable. In stateless operation, the PNR command described in clause 9.1.9 shall be used instead of the ASR command.

Message format:

```
<AS-Request>  ::= < Diameter Header: 274, REQ, PXY, 167772xx >
                  < Session-Id >
                  { Origin-Host }
                  { Origin-Realm }
                  { Destination-Realm }
                  { Destination-Host }
```

```
                { Auth-Application-Id }
                { Abort-Cause }
                { Event-Timestamp }
                 [ Origin-State-Id ]
                *[ Proxy-Info ]
                *[ Route-Record ]
                 [ AVP ]
```

9.1.8 Abort-Session-Answer (ASA) command

The ASA command is imported from [IETF RFC 3588]. It is indicated by the Command-Code field set to 274 and the 'R' bit cleared in the Command Flags field. The mandatory AVPs specified in [IETF RFC 3588] have their normal usage, which is independent of the application.

The ASA command is sent by the SCE to the PD-PE in response to the ASR command. In stateless operation of the PD-PE, the PNA command described in clause 9.1.10 shall be used instead of the ASA command.

Message format (ASA):

```
<AS-Answer>  ::=  < Diameter Header: 274, PXY, 167772xx >
                  < Session-Id >
                  { Origin-Host }
                  { Origin-Realm }
                  { Result-Code }
                   [ Experimental-Result ]
                   [ Origin-State-Id ]
                   [ Error-Message ]
                   [ Error-Reporting-Host ]
                  *[ Class ]
                  *[ Failed-AVP ]
                  *[ Redirect-Host ]
                   [ Redirect-Host-Usage ]
                   [ Redirect-Max-Cache-Time ]
                  *[ Proxy-Info ]
                  *[ AVP ]
```

9.1.9 Push-Notification-Request (PNR) command

The PNR command is imported from [ETSI TS 129 329]. It is indicated by the Command-Code field set to 309 and the 'R' bit set in the Command Flags field. As indicated in clause 7, the mandatory Vendor-Specific-Application-Id shall contain a Vendor-Id set to the ITU-T vendor ID (11502) and an Auth-Application-Id set to the Rs application ID (16777235).

NOTE – This command will never be sent within the Gq application.

In the Rs application, the mandatory User-Identity and User-Data AVPs shall be present but empty. The Session-Id shall have an arbitrary value and the Auth-Session-State AVP shall be set to NO_STATE_MAINTAINED (1). The other mandatory AVPs specified in [ETSI TS 129 329] have their normal usage, which is independent of the application.

The PNR command is used as an alternative to the RAR and ASR commands in stateless operation. When used as a substitute for RAR, it is distinguished by the presence of one or more Specific-Action AVPs. Instances of the Access-Network-Charging-Identifier, Access-Network-Charging-Address, Flows, Binding-Information, and/or Dynamic-Firewall-Working-Mode AVPs may also be present. When used as a substitute for ASR, it is distinguished by the presence of Event-Timestamp and absence of any of the other AVPs just listed, the Specific-Action AVP in particular. Unlike RAR and ASR, the command shall include one or more instances of the Class AVP to carry state information which must be returned to the PD-PE in any response.

Message format (PNR):

```
<PN-Request> ::= < Diameter Header: 309, REQ, PXY, 16777235 >
                 < Session-Id >
                 { Vendor-Specific-Application-Id }
                 { Origin-Host }
                 { Origin-Realm }
                 { Destination-Realm }
                 { Destination-Host }
                 { Auth-Session-State }
                 { User-Identity }
                 { User-Data }
                1*{ Class }
                 *[ Specific-Action ]
                 *[ Access-Network-Charging-Identifier ]
                  [ Access-Network-Charging-Address ]
                 *[ Flows ]
                  [ Binding-Information ]
                  [ Dynamic-Firewall-Working-Mode ]
                  [ Abort-Cause ]
                  [ Event-Timestamp ]
                  [ Origin-State-Id ]
                 *[ Proxy-Info ]
                 *[ Route-Record ]
                 *[ AVP ]
```

9.1.10 Push-Notification-Answer (PNA) command

The PNA command is imported from [ETSI TS 129 329]. It is indicated by the Command-Code field set to 309 and the 'R' bit cleared in the Command Flags field. As indicated in clause 7, the mandatory Vendor-Specific-Application-Id shall contain a Vendor-Id set to the ITU-T vendor ID (11502) and an Auth-Application-Id set to the Rs application ID (16777235). The mandatory Session-Id AVP shall have the same value as the Session-Id in the PNR to which this message is responding, and the mandatory Auth-Session-State AVP shall be set to NO_STATE_MAINTAINED (1). The other mandatory AVPs specified in [ETSI TS 129 329] have their normal usage, which is independent of the application.

The PNA command is sent by the SCE to the PD-PE in response to the PNR command. The PNA command must contain copies of the Class AVP(s) that were present in the PNR command to which the PNA is responding. The other contents of the PNA command are determined by the SCE depending on whether the PNR was a reauthorization request (contained Specific-Action AVP(s)) or was reporting an aborted session.

Message format (PNA):

```
<PN-Answer> ::=  < Diameter Header: 309, PXY, 16777235 >
                 < Session-Id >
                 { Vendor-Specific-Application-Id }
                 { Origin-Host }
                 { Origin-Realm }
                 { Auth-Session-State }
                1*{ Class }
                  [ Result-Code ]
                  [ Experimental-Result ]
                 *[ Media-Component-Description ]
                 *[ Flow-Grouping ]
                  [ Reservation-Priority ]
                  [ AF-Charging-Identifier ]
                 *[ Specific-Action ]
                  [ Binding-Information ]
                  [ Latching-Indication ]
                  [ Dynamic-Firewall-Working-Mode ]
                  [ Origin-State-Id ]
                  [ Error-Message ]
```

```
 [ Error-Reporting-Host ]
*[ Failed-AVP ]
*[ Redirect-Host ]
 [ Redirect-Host-Usage ]
 [ Redirect-Max-Cache-Time ]
*[ Proxy-Info ]
*[ AVP ]
```

9.2 Experimental-Result-Code AVP values

This clause defines specific values of the Experimental-Result-Code AVP used in this Recommendation. Most of these are imported from 3GPP and ETSI specifications, as indicated in the subclauses below.

9.2.1 Experimental-Result-Code AVP values imported from Gq [ETSI TS 129 209]

This subclause defines the specific values of the Experimental-Result-Code AVP imported from [ETSI TS 129 209] (vendor-id is 3GPP):

INVALID_SERVICE_INFORMATION (5061)

– The service information provided by the SCE is invalid or insufficient for the server to perform the requested action.

FILTER_RESTRICTIONS (5062)

– The Flow_Description AVP(s) cannot be handled by the server because restrictions defined in clause 9.3.17 are not observed.

9.2.2 Experimental-Result-Code AVP values imported from [ETSI ES 283 026]

This subclause defines the specific values of the Experimental-Result-Code AVP imported from [ETSI TS 283 026] (vendor-id is ETSI):

INSUFFICIENT_RESOURCES (4041)

– The PD-PE indicates insufficient resources to perform the requested action.

MODIFICATION_FAILURE (5041)

– The PD-PE indicates that the resource reservation could not be modified.

COMMIT_FAILURE (4043)

– The PD-PE indicates that the resource reservation could not be committed.

REFRESH_FAILURE (4044)

– The PD-PE indicates that the lifetime of a reservation could not be extended.

QOS_PROFILE_FAILURE (4045)

– The PD-PE determines that the request from the SCE did not fit within an applicable QoS profile.

ACCESS_PROFILE_FAILURE (4046)

– The PD-PE determines that the request from the SCE did not match the access profile of a subscriber.

PRIORITY_NOT_GRANTED (4047)

– The PD-PE determines that the priority level request from the SCE exceeded the maximum priority level contained in the applicable access profile.

9.2.3 Experimental-Result-Code AVP values imported from [ETSI TS 183 017]

This subclause defines the specific values of the Experimental-Result-Code AVP imported from [ETSI TS 183 017] (vendor-id is ETSI):

BINDING_FAILURE (5021)

– The PE-PE failed to provide the requested address binding.

9.3 AVPs

The following tables summarize the AVPs used in this Recommendation, beyond those defined in the Diameter Base Protocol ([IETF RFC 3588]).

Table 3 describes the Diameter AVPs that are used within this Recommendation that have been defined by ETSI [ETSI TS 183 017], providing their AVP Code values, types, possible flag values and whether or not the AVP may be encrypted. The Vendor-Id header of all AVPs identified in Table 3 shall be set to ETSI (13019). These AVPs are described in this Recommendation for information; however, the normative detail for these AVPs is contained in [ETSI TS 183 017].

Table 3 – Diameter AVPs imported from [ETSI TS 183 017]

				AVP flag rules (Note 1)				
Attribute name	**AVP code**	**Clause defined**	**Value type (Note 2)**	**Must**	**May**	**Should not**	**Must not**	**May encrypt**
Transport-Class	311	9.3.40	Unsigned32	V	M			Y
Binding-Information	450	9.3.9	Grouped	V			M	Y
Binding-Input-List	451	9.3.10	Grouped	V			M	Y
Binding-Output-List	452	9.3.11	Grouped	V			M	Y
V6-Transport-Address	453	9.3.42	Grouped	V			M	Y
V4-Transport-Address	454	9.3.41	Grouped	V			M	Y
Port-Number	455	9.3.30	Unsigned32	V			M	Y
Reservation-class	456	9.3.32	Unsigned32	V			M	Y
Latching-Indication	457	9.3.23	Enumerated	V			M	Y
Reservation-Priority	458	9.3.33	Enumerated	V			M	Y
Service-Class	459	9.3.37	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 3588]. NOTE 2 – The value types are defined in [IETF RFC 3588].								

Table 4 describes the Diameter AVPs imported from [ETSI ES 283 034]. The Vendor-Id header of all AVPs defined in Table 4 shall be set to ETSI (13019).

Table 4 – Diameter AVPs imported from [ETSI ES 283 034]

					AVP flag rules			
Attribute name	**AVP code**	**Clause defined**	**Value type**	**Must**	**May**	**Should not**	**Must not**	**May encrypt**
Globally-Unique-Address	300	9.3.22	Grouped	V			M	No
Address-Realm	301	9.3.5	OctetString	V			M	No
NOTE – 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 3588].								

Table 5 describes the Diameter AVPs defined by the Gq interface protocol [ETSI TS 129 209] and used within this Recommendation. These AVPs are described in this Recommendation for information; however, the normative detail for these AVPs is contained in [ETSI TS 129 209]. The Vendor-Id header of all AVPs defined in Table 5 shall be set to 3GPP (10415).

This Recommendation modifies the syntax of certain Grouped AVPs defined in [ETSI TS 129 209] by adding one or more optional AVP(s) to the syntax specified in [ETSI TS 129 209]. AVPs defined in [ETSI TS 129 209], but not listed in the following table, should not be sent by Diameter conforming to this Recommendation and shall be ignored by receiving entities.

Table 5 – Diameter AVPs imported from [ETSI TS 129 209]

				AVP flag rules (Note 1)				
Attribute name	**AVP code**	**Clause defined (Note 2)**	**Value type (Note 3)**	**Must**	**May**	**Should not**	**Must not**	**May encrypt**
Abort-Cause	500	9.3.1	Enumerated	M,V	P			Y
Access-Network-Charging-Address	501	9.3.2	Address	M,V	P			Y
Access-Network-Charging-Identifier	502	9.3.3	Grouped	M,V	P			Y
Access-Network-Charging-Identifier-Value	503	9.3.4	OctetString	M,V	P			Y
AF-Application-Identifier	504	9.3.6	OctetString	M,V	P			Y
AF-Charging-Identifier	505	9.3.7	OctetString	M,V	P			Y
Authorization-Token	506	9.3.8	OctetString	M,V	P			Y
Flow-Description	507	9.3.14	IPFilterRule	M,V	P			Y
Flow-Grouping	508	9.3.15	Grouped	M,V	P			Y
Flow-Number	509	9.3.16	Unsigned32	M,V	P			Y
Flows	510	9.3.19	Grouped	M,V	P			Y
Flow-Status	511	9.3.17	Enumerated	M,V	P			Y
Flow-Usage	512	9.3.18	Enumerated	M,V	P			Y
Specific-Action	513	9.3.39	Enumerated	M,V	P			Y
Max-Requested-Bandwidth-DL	515	9.3.24	Unsigned32	M,V	P			Y
Max-Requested-Bandwidth-UL	516	9.3.25	Unsigned32	M,V	P			Y

Table 5 – Diameter AVPs imported from [ETSI TS 129 209]

				AVP flag rules (Note 1)				
Attribute name	**AVP code**	**Clause defined (Note 2)**	**Value type (Note 3)**	**Must**	**May**	**Should not**	**Must not**	**May encrypt**
Media-Component-Description	517	9.3.26	Grouped	M,V	P			Y
Media-Component-Number	518	9.3.27	Unsigned32	M,V	P			Y
Media-Sub-Component AVP	519	9.3.28	Grouped	M,V	P			Y
Media-Type	520	9.3.29	Enumerated	M,V	P			Y
RR-Bandwidth	521	9.3.35	Unsigned32	M,V	P			Y
RS-Bandwidth	522	9.3.36	Unsigned32	M,V	P			Y
SIP-Forking-Indication	523	9.3.38	Enumerated	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. For further details, see [IETF RFC 3588]. NOTE 2 – These AVPs are defined in clauses 6.5.1 through 6.5.14 and 6.5.16 through 6.5.24 respectively of [ETSI TS 129 209]. NOTE 3 – The value types are defined in [IETF RFC 3588].								

Table 6 describes the Diameter AVPs defined for the NASREQ application [IETF RFC 4005] and used in this Recommendation, 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 this Recommendation rather than in the context of the application where they are defined. AVPs defined in [IETF RFC 4005], but not listed in Table 6, should not be sent by Diameter applications conforming to this Recommendation and shall be ignored by receiving entities. No Vendor-Id shall be included in the AVP header.

Table 6 – Diameter AVPs imported from the NASREQ application [IETF RFC 4005]

				AVP flag rules				
Attribute name	**AVP code**	**Section defined (Note)**	**Value type**	**Must**	**May**	**Should not**	**Must not**	**May encrypt**
Framed-IP-Address	8	9.3.20	OctetString				V,M	No
Framed-IPv6-Prefix	97	9.3.21	OctetString				V,M	No
NOTE – These AVPs are defined in clauses 6.11.1 and 6.11.6 respectively of [IETF RFC 4005].								

Table 7 describes the Diameter AVPs imported from [ETSI TS 129 214]. The Vendor-Id header of all AVPs defined in Table 7 shall be set to ETSI (13019).

Table 7 – Diameter AVPs imported from [ETSI TS 129 214]

				AVP flag rules (Note)				
Attribute name	**AVP code**	**Clause defined**	**Value type**	**Must**	**May**	**Should not**	**Must not**	**May encrypt**
Acceptable-Service-Info	526	9.3.46	Grouped	M,V	P			Y
NOTE – 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 3588].								

Table 8 describes the 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 8 – Diameter AVPs defined by this Recommendation

				AVP flag rules				
Attribute name	**AVP code**	**Clause defined**	**Value type**	**Must**	**May**	**Should not**	**Must not**	**May encrypt**
QoS-Downgradable	1001	9.3.31	Enumerated	V	P			Y
Dynamic-Firewall-Working-Mode	1002	9.3.13	Enumerated	V	P			Y
Resource-Reservation-Mode	1003	9.3.34	Enumerated	V	P			Y
Connection-Status-Timer	1004	9.3.12	Unsigned32	V	P			Y
SDP-Direction	1005	9.3.43	Unsigned32	V	P			Y
Operation-Indication	1006	9.3.44	Unsigned32	V	P			Y
TLM-PE-Identifier	1007	9.3.45	DiameterIdentity	V	P			Y

9.3.1 Abort-Cause AVP

The Session-Abort-Cause AVP (AVP code 500) is of type Enumerated, and determines the cause of a session abort request or of an RAR indicating an IP-CAN 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., GGSN for GPRS).

9.3.2 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.

9.3.3 Access-Network-Charging-Identifier AVP

The Access-Network-Charging-Identifier AVP (AVP code 502) is of type Grouped, and contains a charging identifier (e.g., 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 the SCE session.

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

AVP format:

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

9.3.4 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).

9.3.5 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.

9.3.6 AF-Application-Identifier AVP

The AF-Application-Identifier AVP (AVP code 504) is of type OctetString, and it contains information that identifies the particular service that the SCE service session belongs to. This information may be used by the PD-PE to differentiate QoS for different application services. For example, the AF-Application-Identifier may be used as additional information together with the Media-Type AVP when the QoS class for the bearer authorization at the Rs interface is selected. The AF-Application-Identifier may be used also to complete the QoS authorization with application specific default settings in the PD-PE if the SCE does not provide full Media-Component-Description information.

9.3.7 AF-Charging-Identifier AVP

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

9.3.8 Authorization-Token AVP

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

9.3.9 Binding-Information AVP

The Binding-Information AVP (AVP code 450) is of type Grouped and is sent between the SCE and the PD-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 ]     ;
```

9.3.10 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 SCE constructs the Binding-Input-List using session description information.

AVP format:

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

9.3.11 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 ]      ;
```

9.3.12 Connection-Status-Timer AVP

The Connection-Status-Timer AVP (ITU-T AVP code 1004) is of type Unsigned32 and is in units of seconds. The AVP is used to specify the maximum time interval between Diameter messages sent or received for a particular session. The value of zero implies infinity.

The timer value is negotiated between SCE and PD-PE, and determined by the PD-PE finally. PD-PE shall initiate a connection status procedure by issuing Re-Auth-Request (RAR) message with an Specific-Action AVP equal to INDICATION_OF_CONNECTION_STATUS(6) within the period defined by the Connection-Status-Timer AVP in the AAA message for the session.

When the SCE receives such an RAR message from PD-PE, it will check whether the session indicated by the Session-Id in the RAR message is active and respond with Re-Auth-Answer (RAA) message. The Result-Code AVP MUST be present in the RAA message, indicating success or failure.

The SCE will return DIAMETER_SUCCESS if the session is still active and will return DIAMETER_UNKNOWN_SESSION_ID if the session does not exist. In the latter case, the PD-PE shall release the session.

The SCE will assume that the session does not exist if no communication activity is detected for a period exceeding the timer period, and release the session.

The absence of this AVP means that the connection status procedure may be initiated by the PD-PE at any time.

The connection status procedure applies only to stateful operation at the PD-PE. Hence the Connection-Status-Timer AVP should not be present in an AAA command when the PD-PE indicates stateless operation.

9.3.13 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 shall be used to enable inspecting packet header information and dropping packets based on static security policy rules. This is the default packet inspection mode applied for all flows.

DYNAMIC_PACKET_FILTERING (1)

– This value shall be used to enable inspecting packet header information and dropping packets based on static security policy rules and dynamic gate status.

STATEFUL_INSPECTION (2)

– This value shall be used to enable inspecting TCP/UDP connection state information as well as packet header information and dropping packets based on static security policy rules and dynamic gate status.

DEEP_PACKET_INSPECTION (3)

– This value shall be used to enable inspecting packet header information, TCP/UDP connection state information and the content of payload together, and dropping packets based on static security policy rules and dynamic gate status.

9.3.14 Flow-Description AVP

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

- Direction (in or out).
- 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 SCE, the server shall send an error response to the SCE 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.

9.3.15 Flow-Grouping AVP

The Flow-Grouping AVP (AVP code 508) is of type Grouped, and it indicates that no other IP Flows shall be transported together with the listed IP Flows in the same IP-CAN bearer, provided that the access technology supports such a capability.

If Flow-Grouping AVP(s) have been provided in earlier service information, but are not provided in subsequent service information, the old flow grouping remains valid.

If Flow-Grouping AVP(s) have been provided in earlier service information, and new Flow-Grouping AVP(s) are provided, the new flow grouping information replaces the previous information. Previous flow grouping information is invalidated even if the new Flow-Grouping AVP(s) affect other IP flows.

A Flow-Grouping AVP containing no Flows AVP may be used to invalidate flow grouping information provided in earlier service information. A Flow-Grouping AVP containing no Flows AVP shall not be supplied together with other Flow-Grouping AVP(s).

If earlier service information has already been provided, flow grouping information in subsequent service information shall not restrict the flow grouping further for IP flows already described in the previous service information. However, new IP flows described for the first time in the subsequent service information may be added to existing flow groups or in new flow groups.

AVP format:

```
Flow-Grouping ::= < AVP Header: 508 >
                    *[Flows]
```

9.3.16 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) associated with a specific media sub-component, assigned according to the rules described in Annex C.

9.3.17 Flow-Status AVP

The Flow-Status AVP (AVP code 511) is of type Enumerated, and 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 non-RTCP IP flow(s).

ENABLED-DOWNLINK (1)

– This value shall be used to enable associated downlink IP flow(s) and to disable associated uplink non-RTCP IP flow(s).

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 non-RTCP IP flow(s) in both directions.

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.

RTCP flows shall be enabled in both directions for all Flow-Status AVP values, except for the value REMOVED (4).

9.3.18 Flow-Usage AVP

The Flow-Usage AVP (AVP code 512) is of type Enumerated, and 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.

9.3.19 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) are supplied, the Flows AVP refers to all Flows matching the media component number.

AVP format:

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

9.3.20 Framed-IP-Address AVP

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

9.3.21 Framed-IPv6-Prefix AVP

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

9.3.22 Globally-Unique-Address AVP

The Globally-Unique-Address AVP (AVP code 300) is of type Grouped.

AVP format:

```
Globally-Unique-Address ::= < AVP Header: 300 13019 >
     [Framed-IP-Address]
     [Framed-IPv6-Prefix]
     [Address-Realm]
```

9.3.23 Latching-Indication AVP

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

The following values are defined:

LATCH (0)

RELATCH (1)

9.3.24 Max-Requested-Bandwidth-DL AVP

The Max-Requested-Bandwidth-DL AVP (AVP code 515) is of type Unsigned32, and 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.

9.3.25 Max-Requested-Bandwidth-UL AVP

The Max- Requested-Bandwidth-UL AVP (AVP code 516) is of type Unsigned32, and 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.

9.3.26 Media-Component-Description AVP

The Media-Component-Description AVP (AVP code 517) is of type Grouped, and contains service information for a single media component within an SCE session. The content may be based on the SDI exchanged between the SCE and the SCE client in the UE. The information may be used by the server to determine authorized QoS and IP flow classifiers for bearer authorization and charging rule selection.

Within one Diameter message, a single IP flow shall not be described by more than one Media-Component-Description AVP.

Bandwidth information and Flow-Status information provided within the Media-Component-Description AVP applies to all those IP flows within the media component, for which no corresponding information is being provided within Media-Sub-Component AVP(s). If bandwidth is explicitly allocated for RTCP flows associated with the component, it shall always be done at the component rather than the sub-component level, through the use of the RS-bandwidth and RR-bandwidth AVPs.

In stateless operation, the Media-Component-Description shall be present in every AA-Request sent by the SCE until it wishes to terminate the session. With this qualification, if a Media-Component-Description AVP is not supplied, or if optional AVP(s) within a Media-Component-Description AVP are omitted, but corresponding information has been provided in previous Diameter messages, the previous information for the corresponding IP flow(s) remains valid.

All IP flows within a Media-Component-Description AVP are permanently disabled by supplying a Flow Status AVP with the value "REMOVED". The server may delete the corresponding filters and state information.

AVP format:

```
Media-Component-Description ::= < AVP Header: 517 >
          { Media-Component-Number } ; Ordinal number of the media comp.
          *[ Media-Sub-Component ]        ; Set of flows for one flow identifier
           [ AF-Application-Identifier ]
           [ Media-Type ]
           [ Max-Requested-Bandwidth-UL ]
           [ Max-Requested-Bandwidth-DL ]
           [ Flow-Status ]
           [ RS-Bandwidth ]
           [ RR-Bandwidth ]
           [ Reservation-Class]
           [ Reservation-Priority]
           [ QoS-Downgradable ]
           [ Transport-Class ]
```

9.3.27 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.

9.3.28 Media-Sub-Component AVP

The Media-Sub-Component AVP (AVP code 519) is of type Grouped, and contains the requested QoS and filters for the set of IP flows identified by their common flow number within a given media component.

If Flow-Status information is provided within the Media-Sub-Component AVP, it takes precedence over information within the encapsulating Media-Component-Description AVP. If bandwidth information is provided, it indicates an allocation for this specific sub-component beyond the overall allocation declared at the component level. That is, the maximum bandwidth values declared at the component level apply only to the aggregation of sub-components for which no explicit declaration is made at the sub-component level.

The Flow-Status AVP shall not be supplied in the Media-Sub-Component AVP for RTCP flows.

If a Media-Sub-Component-AVP is not supplied, or if optional AVP(s) within a Media-Sub-Component AVP are omitted, but corresponding information has been provided in previous Diameter messages, the previous information for the corresponding IP flow(s) remains valid, unless new information is provided within the encapsulating Media-Component-Description AVP. If

Flow-Description AVP(s) are supplied, they replace all previous Flow-Description AVP(s), even if a new Flow-Description AVP has the opposite direction as the previous Flow-Description AVP.

All IP flows within a Media-Sub-Component AVP are permanently disabled by supplying a Flow Status AVP with the value "REMOVED". The server may delete the corresponding filters and state information.

AVP format:

```
Media-Sub-Component ::= < AVP Header: 519 >
                { Flow-Number }        ; Ordinal number of the IP flow
              0*2[ Flow-Description ]   ; UL and/or DL

                [ Flow-Status ]
                [ Flow-Usage ]
                [ Max-Requested-Bandwidth-UL ]
                [ Max-Requested-Bandwidth-DL ]
```

9.3.29 Media-Type AVP

The Media-Type AVP (AVP code 520) is of type Enumerated, and it determines the media type of a session component. The media types indicate the type of media. The following values are defined:

AUDIO (0)

VIDEO (1)

DATA (2)

APPLICATION (3)

CONTROL (4)

TEXT (5)

MESSAGE (6)

OTHER (0xFFFFFFFF)

9.3.30 Port-Number AVP

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

9.3.31 QoS-Downgradable AVP

The QoS-Downgradable AVP (ITU-T AVP code 1001) is of type Enumerated, and 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 traditional IP QoS and no need to reject the session.

NORMAL is the default value.

9.3.32 Reservation-Class AVP

The Reservation-Class AVP (AVP code 456) is of type Unsigned32 and contains an integer used as an index that identifies a set of traffic characteristics of the flow, thereby pointing to the type of transport service class to be applied (e.g., burstiness and packet size). As one example, this index may point to a configuration of ITU-T Y.1541 parameter values.

9.3.33 Reservation-Priority AVP

The Reservation-Priority AVP (AVP code 458) is of type Enumerated. The following values are specified:

DEFAULT (0): This is the lowest level of priority. If no Reservation-Priority AVP is specified in the AA-Request, this is the priority associated with the reservation.

PRIORITY-ONE (1)

PRIORITY-TWO (2)

PRIORITY-THREE (3)

PRIORITY-FOUR (4)

PRIORITY-FIVE (5)

PRIORITY-SIX (6)

PRIORITY-SEVEN (7)

PRIORITY-EIGHT (8)

PRIORITY-NINE (9)

PRIORITY-TEN (10)

PRIORITY-ELEVEN (11)

PRIORITY-TWELVE (12)

PRIORITY-THIRTEEN (13)

PRIORITY-FOURTEEN (14)

PRIORITY-FIFTEEN (15)

9.3.34 Resource-Reservation-Mode AVP

The Resource-Reservation-Mode AVP (ITU-T AVP code 1003) is of type Enumerated and indicates the desired operation for a resource request.

The following values are defined for the Resource-Reservation-Mode AVP, based on the definitions provided in clause 6.1.1 of [ITU-T Y.2111]:

AUTHORIZATION_ONLY_PULL (0)

This value shall be sent for the cases of:

– pull mode two-phase scheme;
– pull mode three-phase scheme.

AUTHORIZATION_RESERVATION_PUSH (1)

This value shall be sent for the cases of:

– the first phase of the push mode path-decoupled two-phase scheme;
– the first phase of the push mode path-coupled two-phase scheme.

AUTHORIZATION_RESERVATION_COMMITMENT_PUSH (2)

– This value shall be sent for the case of push mode path-decoupled single-phase scheme.

RESOURCE_RELEASE (3)

– This value shall be used when AAR is used as a resource release request in the case of stateless PD-PE.

9.3.35 RR-Bandwidth AVP

The RR-Bandwidth AVP (AVP code 521) is of type Unsigned32, and it indicates the maximum required bandwidth in bits per second for RTCP receiver reports within the session component, as specified in [IETF RFC 3556]. The bandwidth contains all the overhead coming from the IP-layer and the layers above, i.e., IP, UDP and RTCP.

9.3.36 RS-Bandwidth AVP

The RS-Bandwidth AVP (AVP code 522) is of type Unsigned32, and indicates the maximum required bandwidth in bits per second for RTCP sender reports within the session component, as specified in [IETF RFC 3556]. The bandwidth contains all the overhead coming from the IP-layer and the layers above, i.e., IP, UDP and RTCP.

9.3.37 Service-Class AVP

The Service-Class AVP (AVP code 459) is of type UTF8String, and it contains the service class requested by the SCE. The service class is to be checked against local policies in the PD-PE.

9.3.38 SIP-Forking-Indication AVP

The SIP-Forking-Indication AVP (AVP code 523) is of type Enumerated, and describes if several SIP dialogues are related to one Diameter session. The following values are defined:

SINGLE_DIALOGUE (0)

– This value is used to indicate that the Diameter session relates to a single SIP dialogue. This is also the default value applicable if the AVP is omitted.

SEVERAL_DIALOGUES (1)

– This value is used to indicate that the Diameter session relates to several SIP dialogues.

9.3.39 Specific-Action AVP

The Specific-Action AVP (AVP code 513) is of type Enumerated.

Within a PD-PE initiated Re-Authorization Request, the Specific-Action AVP determines the type of the action.

Within an initial AA request, the SCE may use the Specific-Action AVP to request specific actions from the server at the bearer events and to limit the contact to such bearer events where specific action is required. If the Specific-Action AVP is omitted within the initial AA request, the PD-PE shall not generate a notification of any of the events defined below.

The following values are defined. Values 0 through 5 are defined by [ETSI TS 129 209] (vendor ID is 10415, 3GPP). Values 6 and 7 are defined in [ETSI ES 283 026] (vendor ID 13019, ETSI).

SERVICE_INFORMATION_REQUEST (0)

– Within a RAR or PNR, this value shall be used when the server requests the service information from the SCE for the bearer event. In the AAR, this value indicates that the SCE requests the server to demand service information at each bearer authorization.

CHARGING_CORRELATION_EXCHANGE (1)

– Within a RAR or PNR, this value shall be used when the server reports the access network charging identifier to the SCE. The Access-Network-Charging-Identifier AVP shall be included within the request. In the AAR, this value indicates that the SCE requests the server to provide an access network charging identifier to the SCE at each bearer establishment/modification, when a new access network charging identifier becomes available.

INDICATION_OF_LOSS_OF_BEARER (2)

– Within a RAR or PNR, this value shall be used when the server reports a loss of a bearer (e.g., in the case of GPRS, PDP context bandwidth modification to 0 kbit) to the SCE. In the AAR, this value indicates that the SCE requests the server to provide a notification at the loss of a bearer.

INDICATION_OF_RECOVERY_OF_BEARER (3)

– Within a RAR or PNR, this value shall be used when the server reports a recovery of a bearer (e.g., in the case of GPRS, PDP context bandwidth modification from 0 kbit to another value) to the SCE. In the AAR, this value indicates that the SCE requests the server to provide a notification at the recovery of a bearer.

INDICATION_OF_RELEASE_OF_BEARER (4)

– Within a RAR or PNR, this value shall be used when the server reports the release of a bearer (e.g., PDP context removal for GPRS) to the SCE. In the AAR, this value indicates that the SCE requests the server to provide a notification at the removal of a bearer.

INDICATION_OF_ESTABLISHMENT_OF_BEARER (5)

– Within a RAR or PNR, this value shall be used when the server reports the establishment of a bearer (e.g., PDP context activation for GPRS) to the SCE. In the AAR, this value indicates that the SCE requests the server to provide a notification at the establishment of a bearer.

INDICATION_OF_SUBSCRIBER_DETACHMENT (6)

– In the AAR, this value indicates that the SCE requests the PD-PE to provide a notification at the detachment of a subscriber. In a RAR or PNR message, the PD-PE indicates to the SCE that the subscriber has been detached.

INDICATION_OF_RESERVATION_EXPIRATION (7)

– In the AAR, this value indicates that the SCE requests the PD-PE to provide a notification when the reservation expires. In a RAR or PNR message, the PD-PE indicates to the SCE that the reservation has expired.

INDICATION_OF_CONNECTION_STATUS (8)

– Within a RAR or PNR, this value shall be used to indicate that the PD-PE requests the SCE to check the connection status of the session.

9.3.40 Transport-Class AVP

The Transport-Class AVP (AVP code 311) is of type Unsigned32, and it contains an integer used as an index pointing to a class of transport services to be applied (e.g., forwarding behaviour).

9.3.41 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 }                ;
```

9.3.42 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 }                ;
```

9.3.43 SDP-Direction AVP

The SDP-Direction AVP (AVP code 1005) is of type Unsigned32, and provides the signalling direction to the PD-PE with respect to NAT control in NGN. Within the AA-Request, the SCE provides the SDP direction to the PE-PE through the PD-PE to indicate whether to allocate the NAT address in the access network/local core network or in the core network/peer core network. After successful address allocation, the PE-PE returns the NAT related information to the PD-PE which then forwards it to the SCE to facilitate SIP negotiation with other UEs in another domain. In this AVP, the following values are defined:

INNER_TO_OUTER (0)

– This value is used to indicate an uplink flow which is directed from the access network/local core network towards the core network/peer core network.

OUTER_TO_INNER (1)

– This value is used to indicate a downlink flow which originated from the core network/peer core network towards the access network/local core network.

9.3.44 Operation-Indication AVP

The Operation-Indication AVP (AVP code 1006) is of type Unsigned32, and indicates the type of operation (i.e., QoS resource reservation and/or NAT control) in the AAR message sent by the SCE to the PD-PE. The following values are defined:

NAT (0)

– This value is used to indicate that the PD-PE shall implement NAT control only.

QoS (1)

– This value is used to indicate that the PD-PE shall implement QoS resource reservation only.

NAT_and_QoS (2)

– This value is used to indicate that the PD-PE shall implement NAT control and QoS resource reservation simultaneously.

When the Operation-Indication AVP is omitted in the AAR message, the PD-PE may implement NAT control and QoS resource reservation simultaneously by default.

9.3.45 TLM-PE-Identifier AVP

The TLM-PE-Identifier AVP (AVP code 1007) is of type DiameterIdentity, and indicates the identifier of the TLM-PE the PD-PE needs to query the user information. Before the SCE requests an authorization for the session from the PD-PE, the identifier of the TLM-PE (e.g., IP address or domain name, etc.) is already acquired by SCE through static configuration or an information query procedure. When there is no explicit user information in the local PD-PE for normal session initiation, the TLM-PE-Identifier taken in the AAR message can be used by the PD-PE to determine the right TLM-PE for the user information query.

9.3.46 Acceptable-Service-Info AVP

The Acceptable-Service-Info AVP (AVP code 526) is of type Grouped, and contains the maximum bandwidth for an SCE session and/or for specific media components that will be authorized by the PD-PE. The Max-Requested-Bandwidth-DL AVP and Max-Requested-Bandwidth-UL AVP directly within the Acceptable-Service-Info AVP indicate the acceptable bandwidth for the entire SCE session. The Max-Requested-Bandwidth-DL AVP and Max-Requested-Bandwidth-UL AVP within a Media-Component-Description AVP included in the Acceptable-Service-Info AVP indicate the acceptable bandwidth for the corresponding media component.

If the acceptable bandwidth applies to one or more media components, only the Media-Component-Description AVP will be provided. If the acceptable bandwidth applies to the whole SCE session, only the Max-Requested-Bandwidth-DL AVP and Max-Requested-Bandwidth-UL AVP will be included.

```
Acceptable-Service-Info::= < AVP Header: x >
                            *[ Media-Component-Description]
                             [ Max-Requested-Bandwidth-DL ]
                             [ Max-Requested-Bandwidth-UL ]
                            *[ AVP ]
```

9.4 Use of namespaces

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

9.4.1 AVP codes

This Recommendation uses AVP values from the AVP Code namespace managed by ETSI for its Diameter vendor-specific applications. In addition, this Recommendation assigns AVP code values within the Diameter AVP Code namespace managed by ITU-T. See clause 9.3, Tables 3-5 and Tables 7 and 8, and Appendix II.

9.4.2 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 9.2.

9.4.3 Command code values

This Recommendation does not assign command code values but uses existing commands defined by the IETF, including those requested by 3GPP.

9.4.4 Application-ID value

This Recommendation defines the Rs Diameter application with application ID 16777235. The vendor identifier assigned by IANA to ITU-T (http://www.iana.org/assignments/enterprise-numbers) is 11502.

10 Security considerations

The primary objective of an attacker at the Rs interface will either be theft of service or denial of service. It is also possible that the attacker may attempt to achieve breach of confidentiality (e.g., to perform traffic analysis against the target or to determine parameters needed to intercept the user session).

Theft of service can be achieved by impersonating a SCE in order to achieve authorization of the attacker's requests. Alternatively, the attacker can modify the resource control protocol messages en route in order to enable QoS for the attacker's sessions rather than, or in addition to, those of the real user. Another possibility is that a user captures and replays the messages that set up an earlier

session, thereby impersonating the SCE. These threats imply the need for: a requirement for the authentication of the SCE; a requirement for message integrity; and a requirement for the prevention of replay of messages.

Clause 8.1 recommends the use of [ETSI TS 133 210] (3GPP TS 33.210) to ensure secure transport of Diameter messages. This reference is essentially a profile of IPSec and its accompanying key management. As such, it provides a level of authentication, integrity protection, and protection against replay. However, this protection is on a link-by-link basis, so if an attacker is able to get control of an intermediate node, the Diameter session remains vulnerable to man-in-the-middle attacks. Operators relying only on IPSec protection are therefore advised to be cautious in the use of agents to proxy or relay Diameter messages between the SCE and the Diameter server. Further considerations along this line are provided in the security considerations section of [IETF RFC 3588], which operators are advised to consult.

Confidentiality protection is optional when using IPSec. To meet the threat of disclosure identified above, operators are advised to enable confidentiality protection within their deployments.

Denial of service attacks can proceed using various means. One possibility is that the attacker creates overload conditions by causing a large number of UE requests for service over a sustained period. These might be designed to impose load on the PD-PE while avoiding charges to the subscribers whose equipment is being used by aborting the sessions before they become billable. A more dangerous case could be that of a rogue SCE. It may be desirable for the PD-PE implementation to provide means for identifying patterns of overload-generating traffic so that overload controls can be applied to the SCEs originating that traffic without affecting service provided to other SCEs.

In stateless operation, the PD-PE passes state information essential to its proper operation to other entities, some at least of which are under different ownership. The possibility exists that this information may be modified either deliberately or accidentally before being passed back to the PD-PE. Thus, integrity protection for this off-loaded state must be applied at the application level. Since this state may include information about the PD-PE operator's network that the operator may not wish to share with others, confidentiality protection in the form of encryption should also be applied to the state information.

Annex A

Support for SIP forking

(This annex forms an integral part of this Recommendation)

A.1 Support for SIP forking

A.1.1 Authorization of resources for early media for forked responses

When a SIP session has been originated by a connected UE, the SCE may receive multiple provisional responses due to forking before the first final answer is received. The SCE shall apply the same authorization token to all the forked responses and the corresponding early dialogues.

The UE and the SCE will become aware of the forking only when the second provisional response arrives. For this, and any subsequent provisional response, the SCE shall use an AA request within the existing Diameter session containing the SIP-Forking-Indication AVP with value SEVERAL_DIALOGUES and include the service information derived from the latest provisional response.

When receiving an AA request containing the SIP-Forking-Indication AVP with value SEVERAL_DIALOGUES, the PD-PE shall identify the existing authorization information for that Diameter session. The PD-PE shall authorize any additional media components and any increased QoS requirements for the previously authorized media components, as requested within the service information. The PD-PE shall authorize the maximum bandwidth required by any of the dialogues, but not the sum of the bandwidths required by all dialogues. Thus, the QoS authorized for a media component is equal to the highest QoS requested for that media component by any of the forked responses. The PD-PE shall also send additional packet classifiers as required by the Flow Description AVPs within the session information to the PE-PE.

A.1.2 Updating the authorization information at the final answer

The SCE shall store the SDP information for each early dialogue separately till the first final SIP answer is received. Then the related early dialogue is progressed to an established dialogue to establish the final SIP session. All the other early dialogues are terminated. The authorization information for the SIP session is updated to match the requirements of the remaining early dialogue only.

When receiving the first final SIP response, the SCE shall send an AA request without the SIP-Forking-Indication AVP and include the service information derived from the SDP corresponding to the dialogue of the final response.

When receiving an AA request with no SIP-Forking-Indication AVP or with a SIP-Forking-Indication AVP with value SINGLE_DIALOGUE, the PD-PE shall update the authorization information and packet classifiers to match only the requirements of the service information within this AA request.

Annex B

QoS parameter mapping for SDP

(This annex forms an integral part of this Recommendation)

This annex describes the rules for mapping SDP information to Rs parameters when the SDP Offer/Answer model described in [IETF RFC 3264] is supported by the SCE.

B.1 SDP to service information mapping in SCE

The mapping described in this clause is mandatory when the SCE behaves as a P-CSCF and should also be applied by other SCEs when SDP is used as the session description syntax.

When a session is initiated or modified, the SCE shall use the mapping rules in Table B.1 for each SDP media component to derive a Media-Component-Description AVP from the SDP Parameters. The derivation of sub-components is shown in Table B.2. Furthermore, the SCE shall map information about the grouping of media lines into resource reservation flows into the Flow-Grouping AVP as specified in Table B.3.

Table B.1 – Rules for derivation of service information within Media-Component-Description AVP from SDP media component

Service information per Media-Component-Description AVP (Notes 1 and 7)	Derivation from SDP parameters (Note 2)
Media-Component-Number	Ordinal number of the position of the "m=" line in the SDP
AF-Application-Identifier	The AF-Application-Identifier AVP may be supplied or omitted, depending on the application. When the SCE behaves as a P-CSCF, if the AF-Application-Identifier AVP is supplied, its value should not demand application-specific bandwidth or QoS class handling. However, if an SCE is capable of handling a QoS downgrading, the AF-Application-Identifier AVP may be used to demand application-specific bandwidth or QoS class handling.
Media-Type	The Media Type AVP shall be included with the same value as supplied for the media type in the "m=" line.

Flow-Status	IF port in m-line = 0 THEN
	  Flow-Status:= REMOVED;
	ELSE
	  IF a=recvonly THEN
	  IF <SDP direction> = UE originated THEN
	  Flow-Status := ENABLED_DOWNLINK; (NOTE 4)
	  ELSE /* UE terminated */
	  Flow-Status := ENABLED_UPLINK; (NOTE 4)
	  ENDIF;
	  ELSE
	  IF a=sendonly THEN
	  IF <SDP direction> = UE originated THEN
	  Flow-Status := ENABLED_UPLINK; (NOTE 4)
	  ELSE /* UE terminated */
	  Flow-Status := ENABLED_DOWNLINK; (NOTE 4)
	  ENDIF;
	  ELSE

Table B.1 – Rules for derivation of service information within Media-Component-Description AVP from SDP media component

Service information per Media-Component-Description AVP (Notes 1 and 7)	Derivation from SDP parameters (Note 2)

	IF a=inactive THEN
	Flow-Status :=DISABLED;
	ELSE /* a=sendrecv or no direction attribute */
	Flow-Status := ENABLED (NOTE 4)
	ENDIF;
	ENDIF;
	ENDIF;
	ENDIF;
	(Note 5)

Max-Requested-Bandwidth-UL	IF <SDP direction> = UE terminated THEN
	IF b=AS:<bandwidth> is present THEN
	Max-Requested-Bandwidth-UL:= <bandwidth> * 1000; /* Unit is bit/s
	ELSE
	Max-Requested-Bandwidth-UL:= <Operator specific setting>,
	or AVP not supplied;
	ENDIF;
	ELSE
	Consider SDP in opposite direction
	ENDIF

Max-Requested-Bandwidth-DL	IF <SDP direction> = UE originated THEN
	IF b=AS:<bandwidth> is present THEN
	Max-Requested-Bandwidth-DL:= <bandwidth> * 1000; /* Unit is bit/s
	ELSE
	Max-Requested-Bandwidth-DL:= <Operator specific setting>,
	or AVP not supplied;
	ENDIF;
	ELSE
	Consider SDP in opposite direction
	ENDIF

RR-Bandwidth	IF b=RR:<bandwidth> is present THEN
	RR-Bandwidth:= <bandwidth>;
	ELSE
	AVP not supplied
	ENDIF;
	(Note 3; Note 6)

RS-Bandwidth	IF b=RS:<bandwidth> is present THEN
	RS-Bandwidth:= <bandwidth>;
	ELSE
	AVP not supplied
	ENDIF;
	(Note 3, Note 6)

Media-Sub-Component	Supply one AVP for each Flow Number within the media component. The Flow Numbers are derived according to Annex C. The encoding of the AVP is described in Table B.2

Table B.1 – Rules for derivation of service information within Media-Component-Description AVP from SDP media component

Service information per Media-Component-Description AVP (Notes 1 and 7)	Derivation from SDP parameters (Note 2)
NOTE 1 – The encoding of the service information is defined in this Recommendation. NOTE 2 – The SDP parameters are described in [IETF RFC 4566]. NOTE 3 – The 'b=RS:' and 'b=RR:' SDP bandwidth modifiers are defined in [IETF RFC 3556]. NOTE 4 – As an operator policy to disable forward and/or backward early media, the Flow-Status may be downgraded before a SIP dialogue is established, i.e., until a 200 OK INVITE is received. The Value "DISABLED" may be used instead of the Values "ENABLED_UPLINK" or "ENABLED_DOWNLINK". The Values "DISABLED", "ENABLED_UPLINK" or "ENABLED_DOWNLINK" may be used instead of the Value "ENABLED". NOTE 5 – If the SDP answer is available when the session information is derived, the direction attributes and port number from the SDP answer shall be used to derive the flow status. However, to enable interoperability with SIP clients that do not understand the inactive SDP attribute, if a=inactive was supplied in the SDP offer, this shall be used to derive the flow status. If the SDP answer is not available when the session information is derived, the direction attributes from the SDP offer shall be used. NOTE 6 – Information from the SDP answer is applicable, if available. NOTE 7 – The AVPs may be omitted if they have been supplied in previous service information and have not changed.	

Table B.2 – Rules for derivation of Media-Sub-Component AVP from SDP media component

Rs service information per Media-Sub-Component AVP (Notes 1 and 5)	Derivation from SDP parameters (Note 2)
Flow-Number	Derived according to Annex C.
Flow-Status	AVP not supplied for RTCP flows.
Max-Requested-Bandwidth-UL	AVP not supplied for RTCP flows.
Max-Requested-Bandwidth-DL	AVP not supplied for RTCP flows.

Flow-Description	For uplink and downlink direction, a Flow-Description AVP shall be provided unless no IP Flows in this direction are described within the media component.
	The SDP direction attribute (Note 4) indicates the direction of the media IP flows within the media component as follows:
	`IF a=recvonly THEN (NOTE 3)`
	`  IF <SDP direction> = UE originated THEN`
	`  Provide only downlink Flow-Description AVP`
	`  ELSE /* UE terminated */`
	`  Provide only uplink Flow-Description AVP`
	`  ENDIF;`
	`ELSE`
	`  IF a=sendonly THEN (NOTE 3)`
	`  IF <SDP direction> = UE originated THEN`
	`  Provide only uplink Flow-Description AVP`
	`  ELSE /* UE terminated */`
	`  Provide only downlink Flow-Description`

Table B.2 – Rules for derivation of Media-Sub-Component AVP from SDP media component

Rs service information per Media-Sub-Component AVP (Notes 1 and 5)	Derivation from SDP parameters (Note 2)
	AVP ENDIF; ELSE /* a=sendrecv or a=inactive or no direction attribute */ Provide uplink and downlink Flow-Description AVPs ENDIF; ENDIF; For RTCP IP flows, uplink and downlink Flow-Description AVPs shall be provided irrespective of the SDP direction attribute. The uplink destination address shall be copied from the "c=" line of downlink SDP. (Note 6) The uplink destination port shall be derived from the "m=" line of downlink SDP. (Note 6) The downlink destination address shall be copied from the "c=" line of uplink SDP. (Note 6) The downlink destination port shall be derived from the "m=" line of uplink SDP. (Note 6) Uplink and downlink source addresses shall either be derived from the prefix of the destination address or be wildcarded by setting to "any", as specified in this Recommendation. Source ports shall not be supplied. Proto shall be derived from the transport of the "m=" line. For "RTP/AVP", proto is 17 (UDP).
Flow-Usage	The Flow-Usage AVP shall be supplied with value "RTCP" if the IP flow(s) described in the Media-Sub-Component AVP are used to transport RTCP. Otherwise, the Flow-Usage AVP shall not be supplied. [IETF RFC 4566] specifies how RTCP flows are described within SDP.

NOTE 1 – The encoding of the service information is defined in this Recommendation.

NOTE 2 – The SDP parameters are described in [IETF RFC 4566].

NOTE 3 – If the SDP direction attribute for the media component negotiated in a previous offer-answer exchange was sendrecv, or if no direction attribute was provided, and the new SDP direction attribute sendonly or recvonly is negotiated in a subsequent SDP offer-answer exchange, uplink and downlink Flow-Description AVPs shall be supplied.

NOTE 4 – If the SDP answer is available when the session information is derived, the direction attributes from the SDP answer shall be used to derive the flow description. However, to enable interoperability with SIP clients that do not understand the inactive SDP attribute, if a=inactive was supplied in the SDP offer, this shall be used. If the SDP answer is not available when the session information is derived, the direction attributes from the SDP offer shall be used.

NOTE 5 – The AVPs may be omitted if they have been supplied in previous service information and have not changed, as detailed in this Recommendation.

NOTE 6 – If the session information is derived from an SDP offer, the required SDP may not yet be available. The corresponding Flow Description AVP shall nevertheless be included and the unavailable fields (possibly all) shall be wildcarded.

Table B.3 – Rules for mapping SDP information about the grouping of media lines into resource reservation flows into the Flow Grouping AVP

Flow-Grouping AVP (Note 1)	Derivation from SDP parameters (Note 2)
Flow Grouping	For each SDP "a=group:SRF" SDP line, a Flow Grouping AVP shall be generated. (Note 3)
Flows	For each identification tag within "a=group:SRF" SDP line, a Flows AVP containing a Media-Component-Number AVP identifying the corresponding m-line shall be generated. (Note 3) No Flow-Number AVP shall be supplied within the Flows AVP.
NOTE 1 – The encoding of the service information is defined in this Recommendation. NOTE 2 – The SDP parameters are described in [IETF RFC 4566]. NOTE 3 – The SDP "group" attribute is defined in [IETF RFC 3388]. The "SRF" semantics attribute within this grouping framework is defined in [IETF RFC 3524].	

Annex C

Derivation of flow numbers

(This annex forms an integral part of this Recommendation)

C.1 Purpose and scope

This annex describes how to distinguish media components, the IP flows associated with each media component, and the sub-components within which these IP flows are grouped. It describes the numbering of media components and sub-components for the purpose of identifying them within the protocol.

C.2 Conceptual framework

C.2.1 Media components

A media component is a set of IP flows as defined in clause 3.4, which are described and managed as a group and can be thought of as conveying a single medium within the total user session. In the simplest case, a media component is described at the session level by a single "m=" line within an SDP session description. A more complex case is a media component that is described by a set of "m=" lines which are presented as alternatives within the session description. It is also possible that the user flows are not described by SDP but are somehow known to the UE and SCE by other means, perhaps from a subscriber profile or from an application-dependent algorithm.

Media components within a session shall be numbered consecutively starting from 1. Where an SDP session description is provided, the media components shall be numbered according to their order in the session description. Where no SDP description is provided, the media components shall be numbered in the order defined by the profile or algorithm that identifies them.

C.2.2 Media sub-components

A media sub-component is a single IP flow with its counterpart in the opposite direction, if any. The counterpart to an IP flow at the conceptual level is a flow carrying the same type of content over the same protocol. In the simple case of unicast flows described by a single SDP "m=" line, the media component so described consists of two sub-components. The first comprises the IP flow or flows carrying the primary content, the second, the RTCP flows in both directions.

The media sub-components within a given media component shall be given flow numbers running consecutively starting from 1. The ordering of media sub-components shall be by increasing value of port number of the downlink IP flow within that sub-component. Sub-components lacking a downlink flow shall follow after those with downlink flows and shall be ordered by increasing value of port number of the uplink flow.

C.2.3 No SDP and no common algorithm

If the UE and SCE do not share an algorithm for a given application, which guarantees that UE and SCE assign the same ordinal number to each media component, the ordinal number of the media component shall be set to zero and the ordinal number of the IP flows shall be assigned according to the following rules:

1) If ordinal numbers for several IP flows are assigned at the same time, all uplink IP flows shall be assigned lower ordinal number than all downlink IP flows.

2) If ordinal numbers for several IP flows are assigned at the same time, all uplink and all downlink IP flows shall separately be assigned ordinal numbers according to the increasing Internet protocol number assigned by IANA (e.g., 8 for TCP and 17 for UDP).

3) If ordinal numbers for several IP flows are assigned at the same time, for each Internet protocol with a port concept, all uplink and all downlink IP flows of this Internet protocol shall separately be assigned ordinal numbers according to increasing port numbers.

4) If IP flows are added to an existing session, the previously assigned binding info shall remain unmodified and the new IP flows shall be assigned ordinal numbers following the rules 1) to 3).

C.2.4 Persistence of numbering

Once media components and sub-components have been assigned numbers, these numbers shall not change or be reassigned for the duration of the session, even when IP flows are removed and others are added.

C.3 Examples

C.3.1 Example 1

A UE, as the offerer, sends a SDP session description, as shown in Table C.1, to an application server (only relevant SDP parameters are shown):

Table C.1 – Values of the SDP parameters sent by the UE in example 1

v=0
o=ecsreid 3262464865 3262464868 IN IP6 2001:0646:00F1:0045:02D0:59FF:FE14:F33A
s=MM01
i=One unidirectional audio flow and one unidirectional video flow and one bidirectional application flow
t=3262377600 3262809600
m=video 50230 RTP/AVP 31
c=IN IP6 2001:0646:00F1:0045:02D0:59FF:FE14:F33A
a=recvonly
m=audio 50330 RTP/AVP 0
c=IN IP6 2001:0646:00F1:0045:02D0:59FF:FE14:F33A
a=sendonly
m=application 50430 udp wb
c=IN IP6 2001:0646:00F1:0045:02D0:59FF:FE14:F33A
a=sendrecv

and receives the SDP parameters, as shown in Table C.2, from the application server:

Table C.2 – Values of the SDP parameters sent by the application server in example 1

v=0
o=ecsreid 3262464865 3262464868 IN IP6 2001:0646:00F1:0045:02D0:59FF:FE14:F33A
s=MM01
i=One unidirectional audio flow and one unidirectional video flow and one bidirectional application flow
t=3262377600 3262809600
m=video 51372 RTP/AVP 31
c=IN IP6 2001:0646:000A:03A7:02D0:59FF:FE40:2014
a=sendonly
m=audio 49170 RTP/AVP 0
c=IN IP6 2001:0646:000A:03A7:02D0:59FF:FE40:2014
a=recvonly
m=application 32416 udp wb
c=IN IP6 2001:0646:000A:03A7:0250:DAFF:FE0E:C6F2
a=sendrecv

From this offer-answer exchange of SDP parameters, the UE and the PD-PE each creates a list of component and flow numbers comprising the IP flows, as shown in Table C.3:

Table C.3 – Component and flow numbers in example 1

Order of 'm='-line	Type of IP flows	Destination IP address/Port number of the IP flows	Comp. No.	Flow No.
1	RTP (Video) DL	2001:0646:00F1:0045:02D0:59FF:FE14:F33A/ 50230	1	1
1	RTCP DL	2001:0646:00F1:0045:02D0:59FF:FE14:F33A/ 50231	1	2
1	RTCP UL	2001:0646:000A:03A7:02D0:59FF:FE40:2014/ 51373	1	2
2	RTP (Audio) UL	2001:0646:000A:03A7:02D0:59FF:FE40:2014/ 49170	2	1
2	RTCP DL	2001:0646:00F1:0045:02D0:59FF:FE14:F33A/ 50331	2	2
2	RTCP UL	2001:0646:000A:03A7:02D0:59FF:FE40:2014/ 49171	2	2
3	UDP (application) DL	2001:0646:00F1:0045:02D0:59FF:FE14:F33A/ 50430	3	1
3	UDP (application) UL	2001:0646:000A:03A7:0250:DAFF:FE0E:C6F2/ 32416	3	1

C.3.2 Example 2

In the general case, multiple ports may be specified with a "number of ports" qualifier as follows, [IETF RFC 4566]:

```
m=<media> <port>/<number of ports> <transport> <fmt list>
```

A UE, as the offerer, sends a SDP session description, as shown in Table C.4, to an application server (only relevant SDP parameters are shown):

Table C.4 – Values of the SDP parameters sent by the UE in example 2

v=0
o=ecsreid 3262464321 3262464325 IN IP6 2001:0646:00F1:0045:02D0:59FF:FE14:F33A
s=MM02
i=One unidirectional audio media consisting of two media IP flows described by one media component
t=3262377600 3262809600
m=audio 50330/2 RTP/AVP 0
c=IN IP6 2001:0646:00F1:0045:02D0:59FF:FE14:F33A
a=recvonly

and receives the SDP parameters, as shown in Table C.5, from the application server:

Table C.5 – Values of the SDP parameters sent by the application server in example 2

v=0
o=ecsreid 3262464321 3262464325 IN IP6 2001:0646:00F1:0045:02D0:59FF:FE14:F33A
s=MM02
i=One unidirectional audio media consisting of two media IP flows described by one media component
t=3262377600 3262809600
m=audio 49170/2 RTP/AVP 0
c=IN IP6 2001:0646:000A:03A7:02D0:59FF:FE40:2014
a=sendonly

From this offer-answer exchange of SDP parameters, the UE and the PD-PE each creates a list of flow identifiers comprising the IP flows, as shown in Table C.6:

Table C.6 – Component and flow numbers in example 2

Order of 'm='-line	Type of IP flows	Destination IP address/Port number of the IP flows	Comp. No.	Flow No.
1	RTP (audio) DL	2001:0646:00F1:0045:02D0:59FF:FE14:F33A/ 50330	1	1
1	RTCP DL	2001:0646:00F1:0045:02D0:59FF:FE14:F33A/ 50331	1	2
1	RTCP UL	2001:0646:000A:03A7:02D0:59FF:FE40:2014/ 49171	1	2
1	RTP (audio) DL	2001:0646:00F1:0045:02D0:59FF:FE14:F33A/ 50332	1	3
1	RTCP DL	2001:0646:00F1:0045:02D0:59FF:FE14:F33A/ 50333	1	4
1	RTCP UL	2001:0646:000A:03A7:02D0:59FF:FE40:2014/ 49173	1	4

C.3.3 Example 3: no SDP and no common algorithm

The UE and AF do not exchange SDP for an application and do not share an algorithm, which guarantees that the UE and AF assign the same ordinal number to each media component.

At the AF session initiation, the UE and AF agree to set up the following IP flows:

– Uplink UDP flow with destination port 100.
– Downlink UDP flow with destination port 100.
– Downlink TCP flow with destination port 100.
– Uplink TCP flow with destination port 100.
– Uplink UDP flow with destination port 200.

The following binding info is assigned to these IP flows:

– Uplink UDP flow with destination port 100: component 0, flow number 2.
– Downlink UDP flow with destination port 100: component 0, flow number 5.
– Downlink TCP flow with destination port 100: component 0, flow number 4.
– Uplink TCP flow with destination port 100: component 0, flow number 1.
– Uplink UDP flow with destination port 200: component 0, flow number 3.

At a later stage in the session, the TCP IP flows are removed and the following IP flows are added:

– Uplink UDP flow with destination port 150.
– Downlink UDP flow with destination port 50.

The following binding info is assigned to the IP flows existing at this stage:

– Uplink UDP flow with destination port 100: component 0, flow number 2.
– Downlink UDP flow with destination port 100: component 0, flow number 5.
– Uplink UDP flow with destination port 200: component 0, flow number 3.
– Uplink UDP flow with destination port 150: component 0, flow number 6.
– Downlink UDP flow with destination port 50: component 0, flow number 7.

C.3.4 Example 4

In this example, the SDP "a=rtcp" attribute, defined in [b-IETF RFC 3605], is used.

An UE, as the offerer, sends a SDP session description, as shown in Table C.7, to an application server (only relevant SDP parameters are shown):

Table C.7 – Values of the SDP parameters sent by the UE in example 1

v=0
o=ecsreid 3262464865 3262464868 IN IP6 2001:0646:00F1:0045:02D0:59FF:FE14:F33A
s=MM01
i=One unidirectional video media
t=3262377600 3262809600
m=video 50230 RTP/AVP 31
c=IN IP6 2001:0646:00F1:0045:02D0:59FF:FE14:F33A
a=recvonly
a=rtcp: 49320

and receives the SDP parameters, as shown in Table C.8, from the application server:

Table C.8 – Values of the SDP parameters sent by the application server in example 1

v=0
o=ecsreid 3262464865 3262464868 IN IP6 2001:0646:00F1:0045:02D0:59FF:FE14:F33A
s=MM01
i=One unidirectional video media
t=3262377600 3262809600
m=video 51372 RTP/AVP 31
c=IN IP6 2001:0646:000A:03A7:02D0:59FF:FE40:2014
a=sendonly
a=rtcp:53020

From this offer-answer exchange of SDP parameters, the UE and the PD-PE each creates a list of flow identifiers comprising the IP flows, as shown in Table C.9:

Table C.9 – Flow identifiers in example 4

Order of 'm='-line	Type of IP flows	Destination IP address/Port number of the IP flows	Comp. No.	Flow No.
1	RTP (Video) DL	2001:0646:00F1:0045:02D0:59FF:FE14:F33A/ 50230	1	2
1	RTCP DL	2001:0646:00F1:0045:02D0:59FF:FE14:F33A/ 49320	1	1
1	RTCP UL	2001:0646:000A:03A7:02D0:59FF:FE40:2014/ 53020	1	1

Appendix I

Mapping of Rs information components

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

This appendix describes the mapping of Stage 2 messages and information components from the Rs reference point (as defined in clause 8.1 of [ITU-T Y.2111]) to DIAMETER commands and AVPs as defined in this Recommendation.

Table I.1 – Mapping of Rs messages to DIAMETER commands

Rs message	Source	Destination	Command name	Abbreviation
Resource Initiation Request	SCE	PD-PE	AA-Request	AAR
Resource Initiation Response	PD-PE	SCE	AA-Answer	AAA
Resource Modification Request	SCE	PD-PE	AA-Request	AAR
Resource Modification Response	PD-PE	SCE	AA-Answer	AAA
Resource Action Request	PD-PE	SCE	Re-Auth-Request (PD-PE stateful case)	RAR
Resource Action Request	PD-PE	SCE	Push-Notification-Request (PD-PE stateless case)	PNR
Resource Action Response	SCE	PD-PE	Re-Auth-Answer (PD-PE stateful case)	RAA
Resource Action Response	SCE	PD-PE	Push-Notification-Answer (PD-PE stateless case)	PNA
Resource Notification	PD-PE	SCE	Re-Auth-Request	RAR
Resource Release Request	SCE	PD-PE	Session-Termination-Request (PD-PE stateful case)	STR (PD-PE stateful case)
Resource Release Request	SCE	PD-PE	AA-Request (PD-PE stateless case)	AAR (PD-PE stateless case)
Resource Release Response	PD-PE	SCE	Session-Termination-Answer (PD-PE stateful case)	STA (PD-PE stateful case)
Resource Release Response	PD-PE	SCE	AA-Answer (PD-PE stateless case)	AAA (PD-PE stateless case)
Abort Resource Request	PD-PE	SCE	Abort-Session-Request (PD-PE stateful case)	ASR

Table I.1 – Mapping of Rs messages to DIAMETER commands

Rs message	Source	Destination	Command name	Abbreviation
Abort Resource Request	PD-PE	SCE	Push-Notification-Request (PD-PE stateless case)	PNR
Abort Resource Response	SCE	PD-PE	Abort-Session-Answer (PD-PE stateful case)	ASA
Abort Resource Response	SCE	PD-PE	Push-Notification-Answer (PD-PE stateless case)	PNA

Table I.2 – Mapping of Rs message parameters to DIAMETER AVPs

Rs message parameter	DIAMETER AVP name
SCF Identifier	AF-Application-Identifier or Origin-Host
Resource Control Session Identifier	Session-Id
Globally Unique Address Information	Globally-Unique-Address
Unique IP Address	Framed-IP-Address/Framed-IPv6-Prefix
Address Realm	Address-Realm
Transport Subscriber Identifier	User-Name
Resource Requestor Identifier	Origin-Host, Origin-Realm or AF-Application-Identifier
Resource Request Priority	Reservation-Priority
Reservation Holding Time	Authorization-Lifetime, Auth-Grace-Period
Resource Control Session Information	Auth-Session-State, Class
Dynamic Firewall Working Mode	Dynamic-Firewall-Working-Mode
Authorization Token	Authorization-Token
Charging Correlation Information	AF-Charging-Identifier, Access-Network-Charging-Identifier
Media Profile	Media-Component-Description Reservation-Class
Media Number	Media-Component-Number
Type of Service	AF-Application-Identifier QoS-Downgradeable
Application Class of Service	Service-Class, Transport-Class, QoS-Downgradeable
Media Priority	Reservation-Priority
Media Flow Description	Media-Sub-Component
Flow Direction	Flow-Description (Direction – dir)
Flow Number	Flow-Number

Table I.2 – Mapping of Rs message parameters to DIAMETER AVPs

Rs message parameter	DIAMETER AVP name
Flow Status	Flow-Status
Protocol Version	Flow-Description (Source and Destination IP Address)
IP Addresses	Flow-Description (Source and Destination IP Address)
Ports	Flow-Description (Source and Destination Ports)
Protocol Number	Flow-Description (Protocol – proto)
Bandwidth	Max-Requested-Bandwidth-UL, Max-Requested-Bandwidth-DL
Resource Reservation Mode	Resource-Reservation-Mode
Event Notification Indication	Specific-Action
Resource Information Indicator	Specific-Action (SERVICE_INFORMATION_REQUEST)
Transport Loss Indicator	Specific-Action (INDICATION_OF_LOSS_OF_BEARER)
Transport Recovery Indicator	Specific-Action (INDICATION_OF_RECOVERY_OF_BEARER)
Transport Release Indicator	Specific-Action (INDICATION_OF_RELEASE_OF_BEARER)
NAPT Control and NAT Traversal	Binding-Information Latching-Indication
Address Binding Information Request	Binding-Input-List
Resource Request Result	Result-Code, Experimental-Result, Error-Message
Address Translation Command	Binding-Output-List
Address Binding Information Response	Binding-Output-List
Timestamp	Event-Timestamp
Reason	Abort-Cause
Signalling direction	SDP-Direction
Type of operation	Operation-Indication
Identifier of the TLM-PE	TLM-PE-Identifier

Appendix II

ITU-T registry for ITU-T defined Diameter attribute-value pairs (AVPs)

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

ITU-T maintains the list of ITU-T defined Diameter AVPs with the following information:

– AVP code;

– AVP name;

– defining ITU-T Recommendation Number;

– Approval date of the Recommendation.

User applications must include the ITU-T vendor-ID value 11502 in the associated Diameter AVP header for these AVPs.

Complete path to ITU-T vendor ID is {iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) itu(11502)}.

An OID repository (as defined in ITU-T X.660-series of Recommendations) is available at http://www.oid-info.com, where ITU-T vendor ID was registered here.

An AVP corresponds to an Information Element in a Diameter message, of the Diameter Base Protocol defined in [IETF RFC 3588].

TSB will assign a unique AVP code for each new AVP used in an ITU-T Recommendation. A request from an ITU-T Study Group (SG) should be made to TSB to obtain and use a code in an ITU-T Recommendation. The code shall be used in ITU-T Recommendations only after assignment by TSB.

Recommendation ITU-T Q.3321.1 uses AVP codes 1001 to 1007 in the ITU-T registry for ITU-T defined Diameter AVPs.

The list of assigned codes is published on the ITU website with free public access. http://www.itu.int/ITU-T/avp/index.html.

Bibliography

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

[b-IETF RFC 3605] IETF RFC 3605 (2003), *Real Time Control Protocol (RTCP) attribute in Session Description Protocol (SDP)*.

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, 2010