

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.3301.1

(08/2013)

SERIES Q: SWITCHING AND SIGNALLING

Signalling requirements and protocols for the NGN –
Resource control protocols

Resource control protocol No. 1, version 3 – Protocol at the Rs interface between service control entities and the policy decision physical entity

Recommendation ITU-T Q.3301.1



International
Telecommunication
Union
Documents

Document Sharing Hub

ITU-T Q-SERIES RECOMMENDATIONS
SWITCHING AND SIGNALLING

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

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

Recommendation ITU-T Q.3301.1

Resource control protocol No. 1, version 3 – Protocol at the Rs interface between service control entities and the policy decision physical entity

Summary

Recommendation ITU-T Q.3301.1 v3 (formerly 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.3301.1 v3 supersedes Recommendation ITU-T Q.3301.1 v2 (06/2010).

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T Q.3301.1	2007-03-09	11
2.0	ITU-T Q.3321.1	2010-06-13	11
2.0	ITU-T Q.3301.1 v2	2010-06-13	11
3.0	ITU-T Q.3301.1 v3	2013-08-13	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/>.

© ITU 2014

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

Table of Contents

	Page
1 Scope	1
2 References.....	1
3 Definitions	3
4 Abbreviations and acronyms	3
5 Rs interface	5
5.1 Overview	5
5.2 Rs reference model	5
5.3 Functional elements and capabilities	5
6 SCE session-specific procedures	6
6.1 Procedures at the PD-PE	6
6.2 Procedures at the SCE	8
6.3 IMS-related SCE procedures	11
7 Protocol specification	12
8 Use of the Diameter base protocol.....	13
8.1 Securing Diameter messages	13
8.2 Accounting functionality	13
8.3 Use of sessions	13
8.4 Transport protocol	13
8.5 Routing considerations	13
8.6 Advertising application support	14
9 Message specification.....	14
9.1 Commands.....	14
9.2 Experimental-Result-Code AVP values	22
9.3 AVPs.....	23
9.4 Use of namespaces	38
10 Security considerations	39
Annex A – Support for SIP forking	41
A.1 Support for SIP forking	41
Annex B – QoS parameter mapping for SDP	42
B.1 SDP to service information mapping in SCE	42
Annex C – Derivation of flow numbers.....	47
C.1 Purpose and scope	47
C.2 Conceptual framework	47
C.3 Examples	48
Annex D – Support for ETS.....	53
D.1 Handling of ETS session	53
Appendix I – Mapping of Rs information components	54



	Page
Appendix II – ITU-T registry for ITU-T defined Diameter attribute-value pairs	57
Bibliography.....	58

Copyright © 2013 ITU-T. All rights reserved.

Recommendation ITU-T Q.3301.1

Resource control protocol No. 1, version 3 – 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 priority information to the PD-PE to facilitate appropriate priority handling (e.g., emergency telecommunications service (ETS) priority information);
- 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 (2011), *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 V10.9.0 (2013), <i>Universal Mobile Telecommunications System (UMTS); LTE; Policy and charging control over Rx reference point (3GPP TS 29.214 version 10.9.0 Release 10).</i>
[ETSI TS 129 329]	ETSI TS 129 329 V6.7.0 (2006), <i>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).</i>
[ETSI TS 133 210]	ETSI TS 133 210 V6.6.0 (2006), <i>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).</i>
[ETSI TS 183 017]	ETSI TS 183 017 V3.2.1 (2010), <i>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.</i>
[ETSI ES 283 026]	ETSI ES 283 026 V1.1.1 (2006), <i>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.</i>
[ETSI ES 283 034]	ETSI ES 283 034 V1.1.1 (2006), <i>Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Network Attachment Sub-System (NASS); e4 interface based on the DIAMETER protocol.</i>
[IETF RFC 3261]	IETF RFC 3261 (2002), <i>SIP: Session Initiation Protocol.</i>
[IETF RFC 3264]	IETF RFC 3264 (2002), <i>An Offer/Answer Model with Session Description Protocol (SDP).</i>
[IETF RFC 3520]	IETF RFC 3520 (2003), <i>Session Authorization Policy Element.</i>
[IETF RFC 3524]	IETF RFC 3524 (2003), <i>Mapping of Media Streams to Resource Reservation Flows.</i>
[IETF RFC 3550]	IETF RFC 3550 (2003), <i>RTP: A Transport Protocol for Real-Time Applications.</i>
[IETF RFC 3556]	IETF RFC 3556 (2003), <i>Session Description Protocol (SDP) Bandwidth Modifiers for RTP Control Protocol (RTCP) Bandwidth.</i>
[IETF RFC 4005]	IETF RFC 4005 (2005), <i>Diameter Network Access Server Application.</i>
[IETF RFC 4412]	IETF RFC 4412 (2006), <i>Communications Resource Priority for the Session Initiation Protocol (SIP).</i>
[IETF RFC 4566]	IETF RFC 4566 (2006), <i>SDP: Session Description Protocol.</i>
[IETF RFC 4960]	IETF RFC 4960 (2007), <i>Stream Control Transmission Protocol.</i>

[IETF RFC 5888]	IETF RFC 5888 (2002), <i>Grouping of Media Lines in the Session Description Protocol (SDP)</i> .
[IETF RFC 6733]	IETF RFC 6733 (2012), <i>Diameter Base Protocol</i> .

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following term defined elsewhere:

None.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

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

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

3.2.3 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.

3.2.4 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).

3.2.5 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.

3.2.6 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.

3.2.7 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.

3.2.8 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
CEA	Capabilities-Exchange-Answer



Documents

Document Sharing Hub

Rec. ITU-T Q.3301.1 (08/2013)

3

CER	Capabilities-Exchange-Request
CGPD-PE	CPN Gateway Policy Decision – Physical Entity
CGPE-PE	CPN Gateway Policy Enforcement – Physical Entity
CPN	Customer Premises Network
ETS	Emergency Telecommunications Service
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
MPS	Multimedia Priority Service
NAPT	Network Address and Port Translation
NASREQ	Network Access Server Requirement
NAT	Network Address Translation
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
RTP	Real-Time Transport Protocol
SCE	Service Control Entity
SDI	Session Description Information
SDP	Session Description Protocol
SIP	Session Initiation Protocol
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 policy decision physical entity (PD-PE) and the service control entity (SCE), e.g., the proxy-call session control function 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.

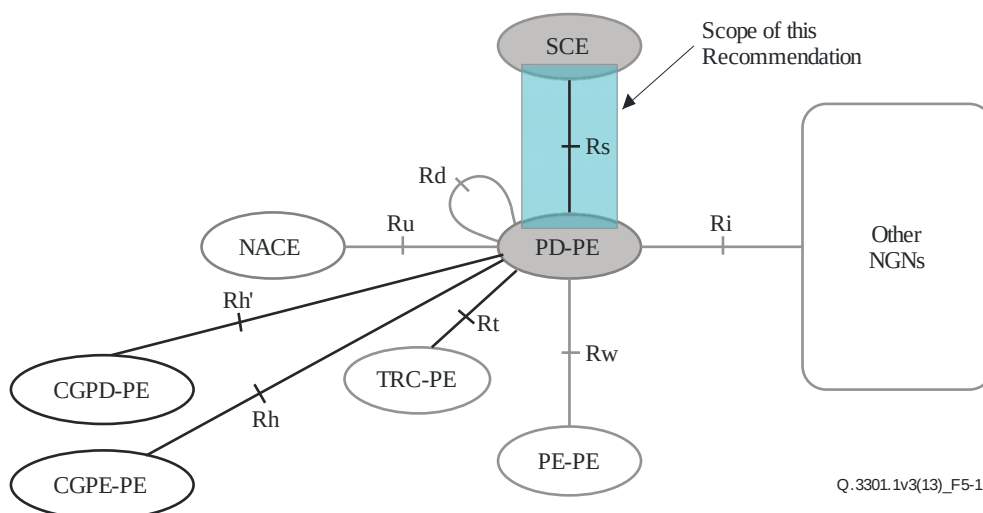


Figure 5-1 – Rs reference model

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 attribute-value pair (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 6733]. 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 policy enforcement physical entity (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 network address and port translation (NAPT) control and network address translation (NAT) traversal function control at the PE-PE based on the information indicated by the Binding-Information AVP and session description protocol (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-connectivity access network (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.

If the AA-Request contains the Restoration-Indication AVP indicating that the QoS of the request can be restored, the PD-PE is recommended to check the resources availability. If there are sufficient resources, the QoS of this session will be restored.

If the AA-Request contains the Downgraded-Indication AVP indicating that the QoS of the request has been downgraded and if there are sufficient resources in the network, the PD-PE is recommended to retrieve the original QoS of the session, rather than the current downgraded QoS.

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.

If the AA-Request contains the Restoration-Indication AVP indicating that the QoS of the request can be restored, the PD-PE is recommended to check resource availability. If there are sufficient resources, the QoS of this session will be restored.

If the AA-Request contains the Downgraded-Indication AVP indicating that the QoS of the request has been downgraded and if there are sufficient resources in the network, the PD-PE is recommended to retrieve the original QoS of the session, rather than the current downgraded QoS.

6.1.3 Session termination

Session termination is signalled by receipt of a Session-Termination-Request (STR) 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 Re-Auth-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 6733], the Session-Id is globally unique and is meant to uniquely identify a user session without reference to any other information. The Session-Id begins with the sender's identity encoded in the 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 session description information (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 IP multimedia subsystem (IMS), the P-CSCF receives an SDP offer sent by the served user equipment (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 6733]. The Globally-Unique-Address AVP is defined in the Diameter Network Access Server specification, [IETF RFC 4005].

The SCE may include the multimedia priority service (MPS)-Identifier AVP in order to indicate that the new SCE session relates to an ETS session. If the PD-PE receives the MPS-Identifier AVP indicating an ETS session, the PD-PE takes specific actions on the corresponding IP-CAN to ensure that the ETS session is prioritized. For ETS session handling, see Annex D.

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-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.

The SCE may include the MPS-Identifier AVP in order to indicate that the modified SCE session relates to an ETS session. If the PD-PE receives the MPS-Identifier AVP, it takes specific actions

on the corresponding IP-CAN to ensure that the ETS session is prioritized. For ETS session handling, see Annex D.

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 STR 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).

If the SCE session being terminated corresponds to an ETS session, the PD-PE may revoke the actions related to the prioritization of the ETS session in the corresponding IP-CAN. For ETS handling, see Annex D.

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 session initiation protocol (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 real-time transport control protocol (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, real-time transport protocol (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 6733] is used to support information transfer on the Rs interface. [IETF RFC 6733] shall apply except as modified by the additional methods, commands, AVPs, and result and event codes specified in this Recommendation. Unless otherwise indicated, the procedures of [IETF RFC 6733] (including error handling and unrecognized information handling) are unmodified.

In addition to the AVPs from the Diameter base application [IETF RFC 6733], 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. Vendor identifiers are assigned by Internet Assigned Numbers Authority (IANA) [b-IANA]; the vendor identifier assigned to ITU-T 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 6733] 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 (i.e., 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 6733]. The 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 4960] and shall utilize the new SCTP checksum method specified in [IETF RFC 4960].

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 Capabilities-Exchange-Request (CER)/Capabilities-Exchange-Answer (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 6733]. 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 6733].

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 6733].

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) (see [b-IANA]) 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 6733], 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.