International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.3305.1

(05/2008)

SERIES Q: SWITCHING AND SIGNALLING

Signalling requirements and protocols for the NGN –
Resource control protocols

**Resource control protocol No. 5 (rcp5) –
Protocol at the interface between a transport
resource control physical entity (TRC-PE) and a
policy decision physical entity (PD-PE)
(Rt interface): Diameter-based**

Recommendation ITU-T Q.3305.1

ITU-T Q-SERIES RECOMMENDATIONS

SWITCHING AND SIGNALLING

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

Recommendation ITU-T Q.3305.1

Resource control protocol No. 5 (rcp5) –
Protocol at the interface between a transport resource control physical entity (TRC-PE) and a policy decision physical entity (PD-PE) (Rt interface): Diameter-based

Summary

Recommendation ITU-T Q.3305.1 specifies a protocol to be used between the physical implementation of the transport resource control functional entity (TRC-FE) and the policy decision physical entity (PD-PE) of a transport network, defined as the Rt reference point in Recommendation ITU-T Y.2111. It is used to control network transport resources required to convey the media flow in an access or a core network.

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.3305.1

Resource control protocol No. 5 (rcp5) –
Protocol at the interface between a transport resource control physical entity (TRC-PE) and a policy decision physical entity (PD-PE) (Rt interface): Diameter-based

1 Scope

This Recommendation provides the stage 3 specification of the Rt interface. The localization of the Rt interface in the overall resource and admission control function (RACF) architecture is visualized in Figure 1. The functional requirements corresponding to this interface are contained in clause 8.5 of [ITU-T Y.2111] and in [b-ITU-T Q-Sup.51].
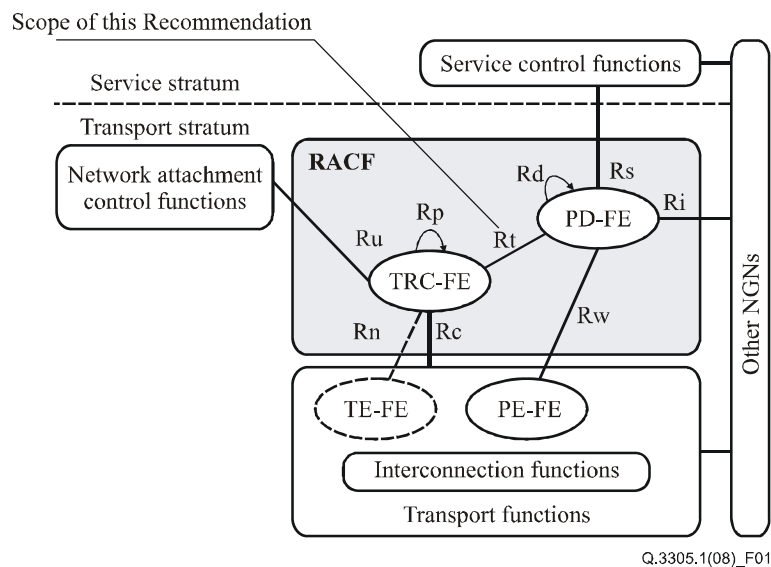
Figure 1 – Localization of the Rt reference point in the generic resource and admission control functional architecture of NGN

The Rt interface protocol operates between the policy decision and the transport control physical elements (Figure 2) of the resource and admission control function (RACF) and is used to control network transport resources required to convey the media flow.

NOTE – Protocols operate between physical entities which are instantiations of corresponding functional entities defined by functional architectures.
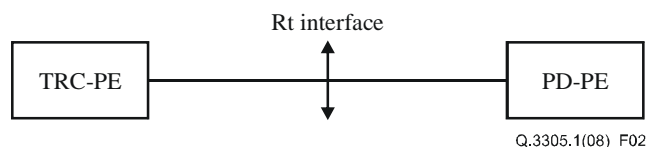
Figure 2 – Field of application of the Rt interface protocol in the NGN RACF

2 References

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

[ITU-T Q.3301.1]   Recommendation ITU-T Q.3301.1 (2007), *Resource control protocol No. 1 – Protocol at the Rs interface between service control entities and the policy decision physical entity.*

[ITU-T Y.2012]   Recommendation ITU-T Y.2012 (2006), *Functional requirements and architecture of the NGN release 1.*

[ITU-T Y.2111]   Recommendation ITU-T Y.2111 (2006), *Resource and admission control in Next Generation Networks.*

[ETSI ES 283 026]   ETSI ES 283 026 V1.4.0 (2007-09), *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.*
<http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=25093http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=25093>

[ETSI ES 283 034]   ETSI ES 283 034 V1.1.1 (2006-06), *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Network Attachment Sub-System (NASS); e4 interface based on the DIAMETER protocol; Release 1.*
<http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=23522>

[ETSI TS 129 209]   ETSI TS 129 209 V6.7.0 (2007-06), *Universal Mobile Telecommunications System (UMTS); Policy control over Gq interface (3GPP TS 29.209 version 6.7.0 Release 6).*
<http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=26703>

[ETSI TS 183 017]   ETSI TS 183 017 V1.4.0 (2007-08), *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; Release 2.* <http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=24757>

[IETF RFC 2960]   IETF RFC 2960 (2000), *Stream Control Transmission Protocol.*
<http://www.ietf.org/rfc/rfc2960.txt?number=2960>

[IETF RFC 3309]   IETF RFC 3309 (2002), *Stream Control Transmission Protocol (SCTP) Checksum Change.* <http://www.ietf.org/rfc/rfc3309.txt?number=3309>

[IETF RFC 3588]   IETF RFC 3588 (2003), *Diameter Base Protocol.*
<http://www.ietf.org/rfc/rfc3588.txt?number=3588>

[IETF RFC 4005]   IETF RFC 4005 (2005), *Diameter Network Access Server Application.*
<http://www.ietf.org/rfc/rfc4005.txt?number=4005>

[IETF RFC 4301]   IETF RFC 4301 (2005), *Security Architecture for the Internet Protocol.*
<http://www.ietf.org/rfc/rfc4301.txt?number=4301>

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1   attribute-value pair (AVP) [IETF RFC 3588]: The Diameter protocol consists of a header followed by one or more Attribute-Value-Pairs (AVPs). An AVP includes a header and is used to encapsulate protocol-specific data (e.g., routing information) as well as authentication, authorization or accounting information.

3.1.2   flow identifier [b-ETSI TS 129 207]: Used for the identification of the IP flows, described within a media component associated with an AF session.

NOTE – A Flow identifier consists of two parts: 1) the ordinal number of the position of the media component description in the session description information and 2) the ordinal number of the IP flow(s) within the media component description assigned in the order of increasing port numbers.

3.2   Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1   hard-state reservation: A type of reservation whereby the requested resources are reserved without time-limit. Hard-state reservations are terminated when the DIAMETER session is terminated.

3.2.2   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.

3.2.3   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.

3.2.4   soft-state reservation: A type of reservation whereby the requested resources are reserved for a finite amount of time. Soft-state reservations are terminated if the DIAMETER session is terminated.

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

GCID   GPRS Charging ID

GPRS   General Packet Radio Service

IMS   IP Multimedia Subsystem

IP-CAN   IP-Connectivity Access Network

NAAF   Network Authentication and Authorization Functional Element

NAPT   Network Address and Port Translation

NASREQ   Network Access Server Application

P-CSCF   Proxy-Call Session Control Function

PDF   Policy Decision Function

PEF   Policy Enforcement Function

PD-PE	Policy Decision Physical Entity
RAA	Re-Auth-Answer
RACF	Resource and Admission Control Function
RACS	Resource and Admission Control Subsystem
RAR	Re-Auth-Request
RCEF	Resource Control Enforcement Function
SBLP	Service Based Local Policy
SCE	Service Control Entity
SDI	Session Description Information
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SPDF	Service Policy Decision Function
STA	Session-Termination-Answer
STR	Session-Termination-Request
TRC-PE	Transport Resource Control-Physical Entity

5 Rt interface

5.1 Overview

The Rt interface is a RACF internal interface.

5.2 Functional elements and capabilities

Policy Decision Physical Entity (PD-PE) and transport control physical entity (TRC-PE) are the entities which interact across the Rt interface within the RACF. They may be implemented within a single network element or may pertain to physically separate network elements.

The detailed information about PD-PE and TRC-PE can be found in clauses 3.1 and 3.2 of [b-ITU-T Q.3300].

5.3 Rt interface protocol

Diameter [IETF RFC 3588] is the base protocol used for the resource control at the Rt interface.

6 Resource control procedures

NOTE – This clause is based on clause 5 of [ETSI ES 283 026], with appropriate changes made to comply with Rt interface functional requirements. In particular, it should be noted that the distribution of functions across the Rt (PD-FE – TRC-FE) interface differs from the distribution of functions across the [ETSI ES 283 026] Rq interface (SPDF – A-RACF) as the [ETSI ES 283 026] A-RACF entity encompasses part of the functionality of a PD-FE.

The resource control procedures are defined in seven interaction procedures:

1)   Reservation;

2)   Commit;

3)   Reservation and commit;

4)   Refresh;

5)   Modification;

6)   Release;

7)   Event notification.

The Flow-Status AVP (clause 7.5.11) is used to define the action to be taken for each AA-Request made by the PD-PE to the TRC-PE. The rules for interpreting the Flow-Status AVP are the following:

•   Reservation: New Media-Description-Component AVP(s) and Media-Sub-Component AVP(s). Optional Flow-Status AVP(s) set to DISABLED (3).

•   Modification: Updated Media-Description-Component AVP(s) and/or Media-Sub-Component AVP(s). Flow-Status AVP not modified, unless the state needs to be modified (e.g., for committing a resource reservation, or for releasing a resource reservation).

•   Commit: Media-Description-Component AVP(s) and optionally Media-Sub-Component AVP(s) of existing reservations with Flow-Status AVP(s) set to ENABLED-UPLINK (0), ENABLED-DOWNLINK (1) or ENABLED (2).

•   ReservationAndCommit: New Media-Component-Description AVP(s) and Media-Sub-Component AVP(s). Flow-Status AVP(s) set to ENABLED-UPLINK (0), ENABLED-DOWNLINK (1) or ENABLED (2).

•   Release: Media-Description-Component AVP(s) and optionally Media-Sub-Component AVP(s) of existing reservations with Flow-Status AVP(s) set to REMOVED (4).

•   Refresh: Existing reservation unchanged (Media-Component-Description AVP(s) not specified or unchanged), Flow-Status AVP unchanged.

7   Rt protocol

This clause defines the Rt protocol, based on Diameter [IETF RFC 3588].

NOTE – This clause is based on, and compatible with, clause 6 of [ETSI ES 283 026], with appropriate changes made to comply with Rt interface functional requirements defined in [ITU-T Y.2111].

7.1   Protocol support

The Diameter Base Protocol as specified in [IETF RFC 3588] is used to support information transfer on the Rt 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 specified, the procedures of [IETF RFC 3588] (including error handling and unrecognized information handling) are unmodified. In addition to the AVPs defined in clause 7.5, the Diameter AVPs from the Diameter base application [IETF RFC 3588] are reused within the Diameter messages sent over the Rt interface.

This Recommendation defines the Rt Diameter application with application ID 16777235 (Vendor-Specific application IDs assigned by IANA).

The vendor identifier assigned by IANA to ITU-T is 11502, the vendor identifier assigned by IANA to ETSI is 13019 and the vendor identifier assigned by IANA to 3GPP is 10415.

The Vendor-Id header for AVPs defined in this Recommendation shall be set to ITU-T (11502).

The Vendor-Id header for AVPs imported from [ETSI TS 129 209] shall be set to 3GPP (10415).

The Vendor-Id header for AVPs imported from [ETSI TS 183 017], [ETSI ES 283 034] and [ETSI ES 283 026] shall set to ETSI (13019).

With regard to the Diameter protocol defined over the Rt interface, the TRC-PE acts as a Diameter server, in the sense that it is the network element that handles authorization requests for a particular realm. The PD-PE 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 TRC-PE and the PD-PE is optional, where the Rt is intra-operator, i.e., TRC-PE and PD-PE are all in the same domain.

7.2 Use of the Diameter base protocol

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

7.2.1 Securing Diameter messages

For secure transport of Diameter messages at the network layer use IPSec per [IETF RFC 4301]. In trusted environments, IPSec without encryption enabled may be used.

7.2.2 Accounting functionality

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

7.2.3 Transport protocol

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

7.2.4 Routing considerations

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

The PD-PE obtains the contact address of the TRC-PE for a given flow 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.

7.2.5 Advertising application support

The Capabilities-Exchange-Request (CER) and Capabilities-Exchange-Answer (CEA) 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 PD-PE and TRC-PE shall advertise the support of the Rt specific application by including the value 16777258 of the application identifier in the Auth-Application-Id AVP within the Vendor-Specific-Application-Id grouped AVP of the Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands.

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

7.3 Rt messages

Existing Diameter command codes from the Diameter base protocol [IETF RFC 3588] and the NASREQ Diameter application [IETF RFC 4005] are used at the Rt interface. The Application-ID of 16777222 is used together with the command code to identify the Rt messages.

7.3.1 AA-Request (AAR) command

The AA-Request command (AAR), indicated by the Command-Code field set to 265 and the "R" bit set in the Command Flags field, is sent by the PD-PE to the TRC-PE for reserve, commit, modify, release and refresh operations.

Message Format:

```
<AA-Request> ::= < Diameter Header: 265, REQ, PXY >
                 < Session-Id >
                 { Auth-Application-ID }
                 { Origin-Host }
                 { Origin-Realm }
                 { Destination-Realm }
                *[ Specific-Action ]
                 [ AF-Charging-Identifier ]
                *[ Media-Component-Description ]
                *[ Flow-Grouping ]
                 [ Reservation-Priority ]
                 [ User-Name ]
                 [ Globally-Unique-Address ]
                 [ Address-Realm ]
                 [ Service-Class ]
                 [ Overbooking indicator]
                 [ Authorization-Lifetime ]
                *[ Proxy-Info ]
                *[ Route-Record ]
                *[ AVP ]
```

7.3.2 AA-Answer (AAA) command

The AA-Answer command (AAA), indicated by the Command-Code field set to 265 and the "R" bit cleared in the Command Flags field, is sent by the PD-PE in response to the AAR command. The TRC-PE may confirm the priority associated with the reservation by echoing the Reservation-Priority AVP (clause 7.5.23).

Message Format:

```
<AA-Answer> ::=  < Diameter Header: 265, PXY >
                 < Session-Id >
                 { Auth-Application-ID }
                 { Origin-Host }
                 { Origin-Realm }
                 [ Result-Code ]
                 [ Experimental-Result ]
                 [ Error-Message ]
                 [ Error-Reporting-Host ]
                 [ Auth-Grace-Period ]
                *[ Session-Bundle-Id ]
                 [ Reservation-Priority ]
                 [ Authorization-Lifetime ]
                *[ Failed-AVP ]
                *[ Proxy-Info ]
                *[ AVP ]
```

7.3.3 Re-Auth-Request (RAR) command

The RAR command, indicated by the Command-Code field set to 258 and the "R" bit set in the Command Flags field, is sent by the TRC-PE to the PD-PE in order to indicate a specific action.

The values INDICATION_OF_RELEASE_OF_BEARER,
INDICATION_OF_SUBSCRIBER_DETACHMENT, and
INDICATION_OF_RESERVATION_EXPIRATION of the Specific-Action AVP shall not be combined with each other in a Re-Auth-Request.

Message Format:

```
<RA-Request> ::= < Diameter Header: 258, REQ, PXY >
                 < Session-Id >
                 { Origin-Host }
                 { Origin-Realm }
                 { Destination-Realm }
                 { Destination-Host }
                 { Auth-Application-Id }
                *{ Specific-Action }
                *[ Flows ]
                 [ Abort-Cause ]
                 [ Origin-State-Id ]
                *[ Proxy-Info ]
                *[ Route-Record ]
                *[ AVP ]
```

7.3.4   Re-Auth-Answer (RAA) command

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

Message Format:

```
<RA-Answer> ::= < Diameter Header: 258, PXY >
                < Session-Id >
                { Origin-Host }
                { Origin-Realm }
                [ Result-Code ]
                [ Experimental-Result ]
               *[ Media-Component-Description ]
               *[ Flow-Grouping ]
                [ Origin-State-Id ]
                [ Error-Message ]
                [ Error-Reporting-Host ]
               *[ Failed-AVP ]
               *[ Proxy-Info ]
               *[ AVP ]
```

7.3.5   Session-Termination-Request (STR) command

The STR command, indicated by the Command-Code field set to 275 and the "R" bit set in the Command Flags field, is sent by the PD-PE to inform the TRC-PE that an authorized session shall be terminated.

Message Format:

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

7.3.6 Session-Termination-Answer (STA) command

The STA command, indicated by the Command-Code field set to 275 and the "R" bit cleared in the Command Flags field, is sent by the TRC-PE to the PD-PE in response to the STR command.

Message Format:

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

7.3.7 Abort-Session-Request (ASR) command

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

Message Format:

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

7.3.8 Abort-Session-Answer (ASA) command

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

Message Format:

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

7.4 Experimental-Result-Code AVP values

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

This Recommendation reuses existing Experimental-Result-Code AVP values defined in [ETSI TS 129 209]. This clause defines the specific values of the Experimental-Result-Code AVP:

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 7.5.7 are not observed.

7.4.2 Experimental-Result-Code AVP values defined in this Recommendation

This clause defines the specific values of the Experimental-Result-Code AVP (vendor-id is ITU-T):

INSUFFICIENT_RESOURCES (4041).

> The TRC-PE indicates insufficient resources to perform the requested action.

MODIFICATION_FAILURE (5041).

> The TRC-PE indicates that the resources reservation could not be modified. This is a permanent failure.

COMMIT_FAILURE (4043).

> The TRC-PE indicates that the resources reservation could not be committed.

REFRESH_FAILURE (4044).

> The TRC-PE indicates that the lifetime of a reservation could not be extended.

QOS_PROFILE_FAILURE (4045).

> The TRC-PE indicates that the request did not match the QoS profile.

ACCESS_PROFILE_FAILURE (4046).

> The TRC-PE indicates that the request did not match any access profile.

PRIORITY_NOT_GRANTED (4047).

> The TRC-PE indicates that the priority level of the request is not accepted.

7.5 AVPs

This clause summarizes the AVPs used in this Recommendation, beyond those defined in the Diameter Base Protocol.

7.5.1 AVPs imported from [ETSI ES 283 026]

Table 1 describes the Diameter AVPs which were defined for the Gq' interface protocol in [ETSI ES 283 026] and which are used in this Recommendation; their AVP Code values; types; possible flag values; and whether the AVP may be encrypted. Flag values are described in the context of this Recommendation rather than in the context of the application where they were defined. The Vendor-Id header for these AVPs shall be set to ETSI (13019).

Table 1 – Diameter AVPs imported from [ETSI ES 283 026]

Attribute name	AVP code	Clause defined	Value type (Note 2)	AVP flag rules (Note 1)				May Encr.
				Must	May	Should not	Must not	
Session-Bundle-Id	400	7.5.24	Unsigned32	M, V	P			Y
NOTE 1 – The AVP header bit denoted as "M" indicates whether support of the AVP is required. The AVP header bit denoted as "V" indicates whether the optional Vendor-ID field is present in the AVP header. For further details, see [IETF RFC 3588]. NOTE 2 – The value types are defined in [IETF RFC 3588].								

7.5.2 AVPs imported from [ETSI TS 129 209]

Table 2 describes the Diameter AVPs which were defined for the Gq interface protocol and which are used in this Recommendation; their AVP Code values; types; possible flag values; and whether the AVP may be encrypted. Flag values are described in the context of this Recommendation rather than in the context of the application where they were defined. The Vendor-Id header for these AVPs shall be set to 3GPP (10415). AVPs which are defined in [ETSI TS 129 209] and not listed in Table 2 should not be sent by Diameter implementations conforming to this Recommendation and, in the case where they are sent, they shall be ignored by the receiving entities.

Table 2 – Diameter AVPs imported from [ETSI TS 129 209]

Attribute name	AVP code	Clause defined	Value type (Note 2)	AVP flag rules (Note 1)				May Encr.
				Must	May	Should not	Must not	
Abort-Cause	500	7.5.5	Enumerated	M, V	P			Y
AF-Application-Identifier	504	7.5.6	OctetString	M, V	P			Y
AF-Charging-Identifier	505	7.5.25	OctetString	M, V	P			Y
Flow-Description	507	7.5.7	IPFilterRule	M, V	P			Y
Flow-Grouping	508	7.5.8	Grouped	M, V	P			Y
Flow-Number	509	7.5.9	Unsigned32	M, V	P			Y
Flows	510	7.5.10	Grouped	M, V	P			Y
Flow-Status	511	7.5.11	Enumerated	M, V	P			Y
Flow-Usage	512	7.5.12	Enumerated	M, V	P			Y
Specific-Action	513	7.5.13	Enumerated	M, V	P			Y
Max-Requested-Bandwidth-DL	515	7.5.14	Unsigned32	M, V	P			Y
Max-Requested-Bandwidth-UL	516	7.5.15	Unsigned32	M, V	P			Y
Media-Component-Description	517	7.5.16	Grouped	M, V	P			Y
Media-Component-Number	518	7.5.17	Unsigned32	M, V	P			Y
Media-Sub-Component AVP	519	7.5.18	Grouped	M, V	P			Y
Media-Type	520	7.5.19	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 – The value types are defined in [IETF RFC 3588].								

7.5.3 AVPs imported from [ETSI TS 183 017]

Table 3 describes the Diameter AVPs which were defined for the Gq' interface protocol in [ETSI TS 183 017] and which are used in this Recommendation; their AVP Code values; types; possible flag values; and whether the AVP may be encrypted. Flag values are described in the context of this Recommendation rather than in the context of the application where they were defined. The Vendor-Id header for these AVPs shall be set to ETSI (13019). AVPs which are defined in [ETSI TS 183 017] and not listed in Table 3 should not be sent by Diameter implementations conforming to this Recommendation and, in the case where they are sent, shall be ignored by the receiving entities.

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

| Attribute name | AVP code | Clause defined | Value type (Note 2) | AVP flag rules (Note 1) | | | | May Encr. |
				Must	May	Should not	Must not	
Reservation-Class	456	7.5.20	Unsigned32	M, V	P			Y
Reservation-Priority	458	7.5.23	Enumerated					
Service-Class	459	7.5.26	UTF8String	V			M	Y
Overbooking-Indicator	460	7.5.28	Enumerated	V			M	Y
NOTE 1 – The AVP header bit denoted as "M" indicates whether support of the AVP is required. The AVP header bit denoted as "V" indicates whether the optional Vendor-ID field is present in the AVP header. For further details, see [IETF RFC 3588]. NOTE 2 – The value types are defined in [IETF RFC 3588].								

7.5.4   AVPs imported from [ETSI ES 283 034]

Table 4 describes the Diameter AVPs which were defined for the e4 interface protocol in [ETSI ES 283 034] and which are used in this Recommendation, their AVP Code values, types, possible flag values and whether the AVP may be encrypted. Flag values are described in the context of this Recommendation rather than in the context of the application where they were defined. The Vendor-Id header for these AVPs shall be set to ETSI (13019). AVPs which are defined in [ETSI ES 283 034] and not listed in Table 4 should not be sent by Diameter implementations conforming to this Recommendation and, in the case they are sent, shall be ignored by the receiving entities.

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

| Attribute name | AVP code | Clause defined | Value type (Note 2) | AVP flag rules (Note 1) | | | | May Encr. |
				Must	May	Should not	Must not	
Globally-Unique-Address	300	7.5.21	Grouped	M, V				Y
Address-Realm	301	7.5.22	OctetString	M, V				Y
Transport-Class	311	7.5.27	Unsigned32	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].								

7.5.5   Abort-Cause AVP

The Abort-Cause AVP (AVP code 500) is of type Enumerated, and it determines the cause of an ASR. The following values defined in [ETSI TS 129 209] are used:

BEARER_RELEASED (0)

> This value is used when the bearer has been deactivated as a result from normal signalling handling. For xDSL, the bearer may refer to an ATM VC.

INSUFFICIENT_SERVER_RESOURCES (1)

> This value is used to indicate that the TRC-PE 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., TRE-PE for xDSL).

7.5.6   AF-Application-Identifier AVP

The AF-Application-Identifier AVP (AVP code 504) is of type OctetString, and contains information that identifies the RACF client requesting the resources (e.g., name of an ASP or group of ASPs).

7.5.7 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.

7.5.8 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.

If Flow-Grouping AVP(s) have been provided in earlier service information, and 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]
```

7.5.9 Flow-Number AVP

The Flow-Number AVP (AVP code 509) is of type Unsigned32, and it contains the ordinal number of the IP flow(s), assigned according to the rules in Annex C of [ITU-T Q.3301.1].

7.5.10 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]
```

7.5.11 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 Flow-Status AVP may be present in the Media-Description-Component AVP and/or in the Media-Sub-Component AVP. The following values are defined:

ENABLED-UPLINK (0)

This value shall be used to commit the corresponding resource reservation in the uplink direction.

ENABLED-DOWNLINK (1)

This value shall be used to commit the corresponding resource reservation in the downlink direction.

ENABLED (2)

This value shall be used to commit a resource reservation in both directions.

DISABLED (3)

This value shall be used to indicate that the corresponding resource reservation is reserved only and not (yet) committed.

REMOVED (4)

This value shall be used to release all resources associated with the corresponding resource reservation.

7.5.12 Flow-Usage AVP

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

NO_INFORMATION (0)

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

RTCP (1)

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

NO_INFORMATION is the default value.

NOTE: A PD-PE may choose not to identify RTCP flows, e.g., in order to avoid that RTCP flows are always enabled by the TRC-PE.

7.5.13 Specific-Action AVP

The Specific-Action AVP (AVP code 513) is of type Enumerated. Within an initial AA-Request, the PD-PE may use the Specific-Action AVP to request from the TRC-PE notification of specific actions. If the Specific-Action AVP is omitted within the initial AA-Request, no notification of any of the events defined below is requested.

The following event from [ETSI TS 129 209] is supported:

INDICATION_OF_RELEASE_OF_BEARER (4)

Within a RAR, this value shall be used when the TRC-PE reports to the PD-PE the release of a bearer (e.g., TRE-PE policies being removed). In the AAR, this value indicates that the PD-PE requests the TRC-PE to provide a notification at the removal of a bearer.

In addition, this Recommendation defines two new events:

INDICATION_OF_SUBSCRIBER_DETACHMENT (6)

Within a RAR, this value shall be used when the TRC-PE reports to the PD-PE that a subscriber has been detached. In the AAR, this value indicates that the PD-PE requests the TRC-PE to provide a notification at the detachment of a subscriber.

INDICATION_OF_RESERVATION_EXPIRATION (7)

Within a RAR, this value shall be used when the TRC-PE reports to the PD-PE that a reservation is about to expire. In the AAR, this value indicates that the PD-PE requests the TRC-PE to provide a notification when a reservation expires.

Events other than the ones listed above, including those defined by [ETSI TS 129 209] and not used in this Recommendation, are not considered relevant at the Rt interface and thus are not to be supported. If events other than the ones listed above are specified by the PD-PE, these values are to be ignored by the TRC-PE.

7.5.14 Max-Requested-Bandwidth-DL AVP

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

7.5.15 Max-Requested-Bandwidth-UL AVP

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

7.5.16 Media-Component-Description AVP

The Media-Component-Description AVP (AVP code 517) is of type Grouped, and it contains service information for a single media component within a session. It may be based on the SDI exchanged between the SCE and the SCE client in the UE. The information shall be used by the TRC-PE to determine the QoS requirements.

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

The Media-Component-Description AVP may contain the Flow-Status AVP, which indicates the particular reservation operation to be performed on the media.

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

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-Priority ]
                          [ Reservation-Class ]
                          [ Transport-Class ]
```

7.5.17 Media-Component-Number AVP

The Media-Component-Number AVP (AVP code 518) is of type Unsigned32, and it contains the ordinal number of the media component, assigned according to the rules in Annex C of [ITU-T Q.3301.1].

7.5.18 Media-Sub-Component AVP

The Media-Sub-Component AVP (AVP code 519) is of type Grouped, and it contains the requested QoS and filters for the set of IP flows identified by their common Flow-Identifier. The Media-Sub-Component AVP may contain the Flow-Status AVP, which indicates the particular reservation operation to be performed on the flow.

Possible Bandwidth information provided within the Media-Sub-Component AVP takes precedence over information within the encapsulating Media-Component-Description AVP. If a Media-Sub-Component AVP is not supplied, or if optional AVP(s) within a Media-Sub-Component AVP are omitted, and if 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.

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

7.5.19 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 following values are defined:

- AUDIO (0)
- VIDEO (1)
- DATA (2)
- APPLICATION (3)
- CONTROL (4)
- TEXT (5)
- MESSAGE (6)
- OTHER (0xFFFFFFFF)

7.5.20 Reservation-Class AVP

The Reservation-Class AVP (AVP code 456) is of type Unsigned32, and it contains an integer used as an index pointing to the traffic characteristics of the flow (e.g., burstiness and packet size).

7.5.21 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 >
                             [Frame-IP-Address]
                             [Frame-IPv6-Prefix]
                             [Address-Realm]
```

7.5.22 Address-Realm AVP

The Address-Realm AVP (AVP code 301) is of type OctetString.

7.5.23 Reservation-Priority AVP

The Reservation-Priority AVP (AVP code 458) is of type Enumerated. It may be specified in an AA-Request as a main AVP in order to associate a priority with a resource reservation or modification request. It may also be specified as part of a Media-Component AVP in order to associate a priority with resource reservations requested for the media flows identified by the Media-Sub-Component AVP(s) in a Media-Component AVP. The following values of this AVP are specified:

> DEFAULT (0): This is the lowest level of priority. If no Reservation-Priority AVP is specified as a main AVP in the AA-Request, this is the priority associated with a resource reservation or modification request. If no Reservation-Priority AVP is specified in a Media-Component-Description AVP, this is the priority associated with resource reservations requested for the media flows identified by the Media-Sub-Component AVP(s) in a Media-Component-Description AVP.
>
> PRIORITY-ONE (1).
>
> PRIORITY-TWO (2).
>
> PRIORITY-THREE (3).
>
> PRIORITY-FOUR (4).
>
> PRIORITY-FIVE (5).
>
> PRIORITY-SIX (6).
>
> PRIORITY-SEVEN (7).

7.5.24 Session-Bundle-Id AVP

The Session-Bundle-Id (AVP code 400) is of type Unsigned32. It may be specified by the TRC-PE in the AA-Answer, when the initial reservation is granted, in order to identify the group of sessions to which the session of the AA-Answer belongs. The value of the Session-Bundle-Id AVP is meaningful for the TRC-PE only. It may be included by the TRC-PE in subsequent Abort-Session-Request (ASR) messages sent to the PD-PE.

7.5.25 AF-Charging-Identifier AVP

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

7.5.26 Service-Class AVP

The Service-Class AVP (AVP code 459) is of type UTF8String, and it contains the service class requested by the PD-PE.

7.5.27 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).

7.5.28 Overbooking-Indicator AVP

The Overbooking indicator AVP (AVP code 460) is of type Enumerated, indicating that the PD-PE should require processing the resource request in overbooking mode. The following values are specified:

- NO-OVERBOOKING (0)

  Means that no overbooking mode is required

- OVERBOOKING (1)

  Means that overbooking mode is required

If this AVP is not included, it is assumed that no overbooking is required.

Appendix I

Resource reservation flow states maintained by RACF

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

NOTE – This appendix is based on, and compatible with, Annex A of [ETSI ES 283 026] with appropriate changes made to comply with Rt interface functional requirements.

Table I.1 below defines the resource reservation flow states maintained by TRC-PE and the corresponding transition conditions.

Table I.1 – Flow state transitions

State	Event	Action	Next state
Idle	Received Reservation Request	Verify availability of resource. Wait for the Resource Availability event.	Idle
Idle	Received Reservation & Commit Request	Verify availability of resource and perform Resource Reservation Commit. Wait for the Successful Enforcement event.	Idle
Idle	Resource Availability	Send AAA with the Result-Code AVP set to DIAMETER_SUCCESS. Initialize Authorization-Lifetime and Auth-Grace-Period timers (in case of soft-state).	Reserved
Idle	Resource not available	Send AAA with the Experimental-Result-Code AVP set to INSUFFICIENT_RESOURCES.	Idle
Idle	Successful Resource Reservation Enforcement	Send AAA with the Result-Code AVP set to DIAMETER_SUCCESS. Initialize Authorization-Lifetime and Auth-Grace-Period timers (in case of soft-state).	Committed
Idle	Unsuccessful Resource Reservation Enforcement	Send AAA with the Experimental-Result-Code AVP set to COMMIT_FAILURE.	Idle
Reserved	Received Commit Request	Enforce Resource Reservation in network elements (i.e., RCEF).	Reserved
Reserved	Successful Resource Reservation Enforcement	Send AAA with the Result-Code AVP set to DIAMETER_SUCCESS.	Committed
Reserved	Unsuccessful Resource Reservation Enforcement	Send AAA with the Experimental-Result-Code AVP to COMMIT_FAILURE.	Idle
Reserved	Received STR	Send STA, clean-up.	Idle

Table I.1 – Flow state transitions

State	Event	Action	Next state
Reserved	Expiration of Authorization-Lifetime timer	The A-RACF shall send an unsolicited RAR message to the SPDF with the Specific-Action AVP set to INDICATION_OF_RESERVATION_EXPIR ATION.	Reserved
Reserved	Expiration of Auth-Grace-Period timer	Clean-up.	Idle
Reserved	Received Resource Reservation Refresh	Send AAA with the Result-Code AVP set to DIAMETER_SUCCESS. Re-initialize Authorization-Lifetime and Auth-Grace-Period timers.	Reserved
Reserved	Received Modification Request	Perform Resource Reservation Modification.	Reserved
Reserved	Successful Resource Reservation Modification	Send AAA with the Result-Code AVP set to DIAMETER_SUCCESS. Re-initialize Authorization-Lifetime and Auth-Grace-Period timers (in case of soft-state).	Reserved
Reserved	Unsuccessful Resource Reservation Modification	Send AAA with the Experimental-Result-Code AVP set to MODIFICATION_FAILURE.	Reserved
Committed	Received Modification Request	Perform Resource Reservation Modification.	Committed
Committed	Successful Resource Reservation Modification	Send AAA with the Result-Code AVP set to DIAMETER_SUCCESS. Re-initialize Authorization-Lifetime and Auth-Grace-Period timers (in case of soft-state).	Committed
Committed	Unsuccessful Resource Reservation Modification	Send AAA with the Experimental-Result-Code AVP set to MODIFICATION_FAILURE.	Committed
Committed	Expiration of Authorization-Lifetime timer	TRC-PE shall send an unsolicited RAR message to the PD-PE with the Specific-Action AVP set to INDICATION_OF_RESERVATION_EXPIR ATION.	Committed
Committed	Received Resource Reservation Refresh	Send AAA with the Result-Code AVP set to DIAMETER_SUCCESS. Re-initialize Authorization-Lifetime and Auth-Grace-Period timers (in case of soft-state)	Committed

Table I.1 – Flow state transitions

State	Event	Action	Next state
Committed	Expiration of Auth-Grace-Period timer	Clean-up.	Idle
Committed	Received STR	Release resources, clean-up.	Idle
All	Critical Event Detected	Send ASR with appropriate Abort-Cause AVP, cleanup.	Idle
All	Non-Critical Event Detected	Send RAR with appropriate Specific-Action AVP.	Unchanged

Bibliography

[b-ITU-T Q.3300]   Recommendation ITU-T Q.3300 (2008), *Architectural framework for the Q.33xx series of Recommendations.*

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

[b-ETSI TS 129 207] ETSI TS 129 207 V6.5.0 (2005-09), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Policy control over Go interface (3GPP TS 29.207 version 6.5.0 Release 6).* <http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=23774>

[b-ETSI TS 129 208] ETSI TS 129 208 V6.7.0 (2007-06), *Digital cellular telecommunications system (Phase 2+);Universal Mobile Telecommunications System (UMTS); End-to-end Quality of Service (QoS) signalling flows (3GPP TS 29.208 version 6.7.0 Release 6).* <http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=26702>

[b-ETSI TS 133 210] ETSI TS 133 210 V6.6.0 (2006-09), *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).* <http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=25254>

[b-IETF RFC 3556]   IETF RFC 3556 (2003), *Session Description Protocol (SDP) Bandwidth Modifiers for RTP Control Protocol (RTCP) Bandwidth.* <http://www.ietf.org/rfc/rfc3556.txt?number=3556>

SERIES OF ITU-T RECOMMENDATIONS

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