International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.3306.1

(10/2009)

SERIES Q: SWITCHING AND SIGNALLING

Signalling requirements and protocols for the NGN – Resource control protocols

---

Resource control protocol no. 6 (rcp6) – Protocol at the interface between intra-domain policy decision physical entities (PD-PE) (Rd interface)

Recommendation ITU-T Q.3306.1

ITU-T Q-SERIES RECOMMENDATIONS

SWITCHING AND SIGNALLING

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

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

Recommendation ITU-T Q.3306.1

Resource control protocol no. 6 (rcp6) – Protocol at the interface between intra-domain policy decision physical entities (PD-PE) (Rd interface)

Summary

Recommendation ITU-T Q.3306.1 specifies the rcp6 protocol used between intra-domain policy decision physical entities (PD-PEs) in the resource and admission control functional block. This interface operates across the Rd reference point as defined in Recommendation ITU-T Y.2111. It is used for inter-communication between PD-PEs that can optionally be deployed in larger domains for scalability reasons.

Source

Recommendation ITU-T Q.3306.1 was approved on 29 October 2009 by ITU-T Study Group 11 (2009-2012) under Recommendation ITU-T A.8 procedures.

Keywords

Diameter, RACF, Rd interface, Resource control.

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.3306.1

Resource control protocol no. 6 (rcp6) – Protocol at the interface between intra-domain policy decision physical entities (PD-PE) (Rd interface)

1 Scope

This Recommendation specifies the protocol used between intra-domain policy decision physical entities (PD-PEs) in the resource and admission control functional block. The functional requirements of the Rd interface are contained in clause 8.8 of [ITU-T Y.2111]. The Rd interface is the interface between intra-domain PD-PEs.

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

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

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

[ETSI TS 129 329] ETSI TS 129 329 V8.3.0 (2009), *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 8.3.0 Release 8)*.

[ETSI TS 183 017] ETSI TS 183 017 V2.3.1 (2008), *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control: DIAMETER protocol for session-based policy set-up information exchange between the Application Function (AF) and the Service Policy Decision Function (SPDF); Protocol specification*.

[ETSI ES 283 026] ETSI ES 283 026 V2.4.1 (2008), *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN);Resource and Admission Control; Protocol for QoS reservation information exchange between the Service Policy Decision Function (SPDF) and the Access-Resource and Admission Control Function (A-RACF) in the Resource and Protocol specification*.

[ETSI ES 283 034]	ETSI ES 283 034 V2.2.0 (2008), *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Network Attachment Sub-System (NASS); e4 interface based on the DIAMETER protocol*.
[IETF RFC 3588]	IETF RFC 3588 (2003), *Diameter Base Protocol*.
[IETF RFC 4005]	IETF RFC 4005 (2005), *Diameter Network Access Server Application*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following term defined elsewhere:

3.1.1 policy decision physical entity (PD-PE) [ITU-T Q.3300]: A device that implements the policy decision functional entity (PD-FE) as defined in clause 7.2.3.2 of [ITU-T Y.2111].

3.2 Terms defined in this Recommendation

This Recommendation does not define any terms.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AAA	AA-Answer
AAR	AA-Request
AVP	Attribute-Value Pair
CPN	Customer Premises Network
NAPT	Network Address and Port Translation
NAT	Network Address Translation
PD-PE	Policy Decision Physical Entity
PE-PE	Policy Enforcement Physical Entity
RAA	Re-Auth-Answer
RAC-PE	Resource and Admission Control Physical Entity
RAR	Re-Auth-Request
SCE	Service Control Entity
SDI	Session Description Information
STA	Session Termination Answer
STR	Session Termination Request
TRC-PE	Transport Resource Control Physical Entity
TRE-PE	Transport Resource Enforcement Physical Entity

5 Conventions

There are no specific conventions in this Recommendation.

6 Rd interface

6.1 Overview

The Rd interface is defined in [ITU-T Y.2111] and is used between intra-domain PD-PEs in the resource and admission control physical entity (RAC-PE). It is used for inter-communication between PD-PEs that can optionally be deployed in larger domains for scalability reasons.

The Rd interface is shown in Figure 6-1, which depicts the generic resource and admission control functional architecture in NGN. It is based on Figure 5 of [ITU-T Y.2111], with the following modifications:

- "Service control functions" is replaced by "Service control entity",
- "Network attachment control functions" is replaced by "Network attachment control entity",
- CGPE-FE is replaced by CGPE-PE,
- PD-FE is replaced by PD-PE,
- TRC-FE is replaced by TRC-PE,
- TRE-FE is replaced by TRE-PE,
- PE-FE is replaced by PE-PE,
- RACF is replaced by RAC-PE.

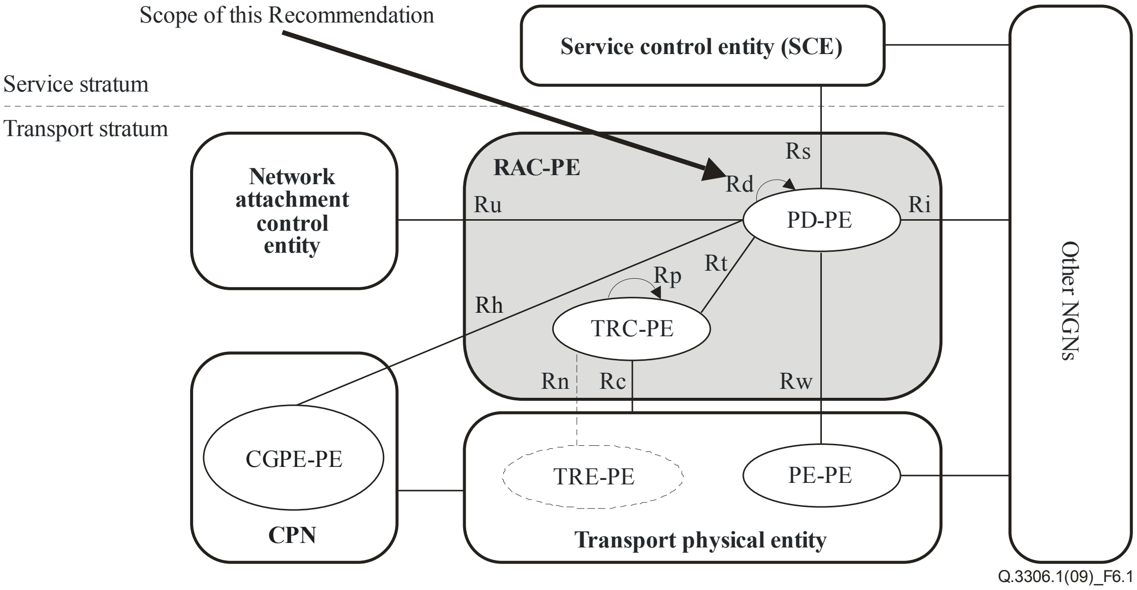

Figure 6-1 – Generic resource and admission control functional architecture in NGN

6.2 Functional elements and capabilities

The PD-PE communicates with the service control entity (SCE) over the Rs interface and interacts across the Rd interface with other PD-PEs within the same network domain. In the case where multiple PD-PEs are deployed, each one can handle a subset of the PE-PEs. If the PD-PE which receives a request over the Rs interface (i.e., the originating PD-PE) is not able to directly reach the targeted PE-PE, because of the network configuration, the originating PD-PE needs to communicate internally over Rd with an intra-domain peer PD-PE to reach the requested PE-PE.

Detailed information about the PD-PE implementation can be found in clause 6.3 of [ITU-T Q.3300]. An example configuration of multiple PD-PEs is shown in Figure 2 of [ITU-T Q.3300].

6.3 Rd interface protocol

Diameter [IETF RFC 3588] is the base protocol used for the PD-PE's interconnection via the Rd interface.

7 Procedures

7.1 Initial reservation for a session

7.1.1 Procedures at the originating PD-PE

The originating PD-PE performs the admission control based on requirements from the SCE. The originating PD-PE requests an authorization for the session from the intra-domain peer PD-PE by sending the AA-Request (AAR) message. It is required that this AAR message contain a new Session-Id.

The AAR message can optionally contain an Authorization-Lifetime attribute-value pair (AVP) to indicate the maximum lifetime that it is requesting.

The AAR message can optionally include an Auth-Session-State AVP to indicate the originating PD-PE's preference for stateful or stateless operation.

The originating PD-PE can optionally include the Operation-Indication AVP to indicate the following operations after receiving the AAR message:

- the peer PD-PE must perform NAPT control and NAT traversal functions, or
- QoS resource reservation, or
- both.

The originating PD-PE is required to include the corresponding Media-Component-Description AVP(s) into the AAR message, if the session description information (SDI) is already available. The originating PD-PE can optionally include the Flow-Grouping AVP(s) to request a particular grouping for the IP flows described within the SDI.

When providing a given Media-Component-Description AVP in the initial AAR message, the originating PD-PE can optionally request the intra-domain peer PD-PE to commit the requested resources by setting the Flow-Status AVP to the value ENABLED, ENABLED-UPLINK or ENABLED-DOWNLINK. Alternatively, the originating PD-PE can optionally perform resource allocation in two phases using separate reserve and commit operations. If commitment is done in two phases, the Flow-Status AVP value of the initial AAR message is required to be set to DISABLED.

If, based on local configuration data, the originating PD-PE determines that address translation needs to occur on the user plane (e.g., the PE-PE implements NAT, or NAPT, or the hosted NAPT procedure), the following action is performed:

- after the originating PD-PE receives an SDI that is associated with the end-point served by it, the originating PD-PE is required to include the Binding-Information AVP with the Input-List AVP.

The originating PD-PE optionally includes the SDP-Direction AVP along with the Binding-Information AVP. These indicate whether the address set in the Output-list AVP is expected to be received in the AAA message in either of the following:

- the originating core network, or
- the peer core network.

If required (e.g., in cases where the served end-point is behind a hosted-NAPT), the originating PD-PE can optionally include the Latching-Indication AVP set to 0.

Based on local configuration data, the originating PD-PE can optionally include the TLM-PE-Identifier AVP in the AAR message to indicate the identifier of TLM-PE (e.g., IP address or domain name, etc.) related to the user.

For the purpose of QoS profile correlation in an intra-domain peer PD-PE lying within an access network, the originating PD-PE is required to include, within the AAR message, a correlation identifier in the form of:

- User-Name AVP, or
- Globally-Unique-IP-Address AVP.

The User-Name AVP is defined in [IETF RFC 3588]. The Globally-Unique-IP-Address AVP is defined in [IETF RFC 4005].

The originating PD-PE can optionally specify the Reservation-Priority AVP in the AAR message or within a Media-Component-Description AVP in the AAR message, or both.

The originating PD-PE can optionally specify the events it wants to be informed about in the Specific-Action AVP of the AAR message.

The originating PD-PE is required to examine the content of any Auth-Session-State AVP it receives in the AAA message. If such an AVP is present and indicates stateful operation, the originating PD-PE is required to include the same Session-Id value as it placed in the initial AAR message in subsequent messages relating to this session.

If a received Auth-Session-State AVP indicates stateless operation, the originating PD-PE is required to store the value of the Class AVP(s) also present in the AAA message. In the stateless operation, the originating PD-PE is required to include the stored Class AVP(s) in any message it sends to the intra-domain peer PD-PE relating to the same session.

The originating PD-PE is required to store the contents of the Binding-Output-List AVP received within the Binding-Information AVP contained in the AAA message for future usage.

The action of the originating PD-PE is a matter of policy when it does not receive the AAA message, when the AAA message arrives after the internal timer has expired, or when the AAA message arrives with an indication different from DIAMETER_SUCCESS.

7.1.2 Procedures at the intra-domain peer PD-PE

The intra-domain peer PD-PE can optionally honour the preference indicated in the Auth-Session-State AVP, or can optionally 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 is present in the initial AAR message or if the intra-domain peer PD-PE chooses stateless operation for the current session, the intra-domain peer PD-PE is required to return an Auth-Session-State AVP in the AAA message to indicate its decision.

In stateful operation, the intra-domain peer PD-PE stores the Session-Id value received in the AAR message. The same Session-Id value will be present in subsequent commands relating to this session, as described in [IETF RFC 3588]. The intra-domain peer PD-PE can use the received Session-Id values to locate the session related information in order to act on the commands.

In stateless operation, the intra-domain peer PD-PE does not store the received Session-Id. Instead, it generates one or more Class AVPs based on local policy data which can be extracted possibly from the contents of the AAR message or from the messages received over other interfaces. The one or more Class AVPs will contain the information needed for the PD-PE to reconstruct its state when it receives additional messages relating to the same user session. This information can optionally include:

- a unique string identifying the session corresponding to the initial AAR message;

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

The Class AVP(s) is required to be returned to the originating PD-PE in the AAA message. The intra-domain peer PD-PE also forwards equivalent state-preserving tokens to the TRC-PE(s) and PE-PE when it communicates with them. Then the intra-domain peer PD-PE receives those tokens back again in messages from TRC-PE(s) and PE-PE.

If the Resource-Reservation-Mode AVP is present, the intra-domain peer PD-PE is required to use it to determine whether the initial AAR message 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 AAR message. If the Resource-Reservation-Mode AVP is not consistent with the Flow-Status AVP, the request is recommended to be rejected.

A request for authorization only (pull mode) cannot be indicated in the absence of the Resource-Reservation-Mode AVP. However, the intra-domain peer PD-PE can infer a request for authorization from the AAR message. This is done without involvement of the originating PD-PE if the Flow-Status AVP for a given media component or sub-component is set to DISABLED (3). Intra-domain peer PD-PE can infer a request for authorization if the Flow-Status AVP is set to any variant of ENABLED, (0), (1), or (2).

The intra-domain peer PD-PE is required to use the contents of the AAR message to enforce any functions needed over the Rt and Rw interfaces. The intra-domain peer PD-PE recognizes policy enforcement functions requested on the transport plane based on the contents of an AAR message, and possibly on configuration data.

If the AAR message contains the Media-Component-Description AVP(s), the intra-domain peer PD-PE is required to trigger the resource reservation procedure towards the TRC-PE. If the AAR message contains Flow-Grouping AVP(s), the intra-domain peer PD-PE is required to only authorize the QoS whenever the IP flows are distributed to the forwarding plane in a way that is allowed by the Flow-Grouping AVP(s).

Additionally, based on the contents of the AAR message (e.g., the AAR message can optionally contain AVPs such as Service-Class) and on local policies, the intra-domain peer PD-PE can optionally request opening or closing of a gate.

The intra-domain peer PD-PE is required to wait for the result of the above interaction(s) (i.e., the interactions described in this clause and up to this point in the text) before returning, in a single AAA message, the result of those interactions to the originating PD-PE. The AAA message is required to be sent only after all actions taken upon the Rt or Rw or both interfaces are achieved. The contents of the AAA message are required to be derived as follows:

- If the resource reservation procedure succeeds and if the requested binding information was received via the Rw interface, the AAA message sent by the intra-domain peer PD-PE to the originating PD-PE is required to contain the allocated token in the Authorization-Token AVP (in pull mode).
- If the resource reservation procedure fails (i.e., the intra-domain peer PD-PE receives a reservation failure notification via the Rt interface), the intra-domain peer PD-PE is required to return the Experimental-Result-Code AVP with the value INSUFFICIENT_RESOURCES in the AAA message.

- If the Resource Reservation procedure succeeds but the peer PD-PE did not succeed in getting a binding via the Rw interface, the peer PD-PE is required to return the Experimental-Result-Code AVP with the value BINDING_FAILURE in the AAA message. Additionally, the peer PD-PE is required to release any associated requested resources through the Rt interface.

7.2 Session modification

7.2.1 Procedures at the originating PD-PE

During the session modification, the originating PD-PE is required to send an updated SDI to the intra-domain peer PD-PE. The updated SDI is based on exchanges within the SCE session signalling. The originating PD-PE does this by sending the AAR message, with an existing Session-Id, containing the Media-Component-Description AVP(s) which contains the updated service information. The originating PD-PE can optionally include the Flow-Grouping AVP(s) to request a particular grouping for the IP flows described within the service description. This is distributed to the forwarding plane.

The originating PD-PE can optionally 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 commitment status: change the Flow-Status AVP of the corresponding Media-Component-Description AVP and optionally Media-Sub-Component AVP 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 AAR message as a hint of the maximum lifetime that it is requesting.

The originating PD-PE can optionally request the intra-domain peer PD-PE to revoke the commitment of requested resources by setting the Flow-Status AVP to the value DISABLED.

The Reservation-Priority AVP associated with a reservation request or a media component is not to be modified, if present.

If updated SDI pointing towards the end-point served by the originating PD-PE is available, and if the SDI pointing determines that address translation needs to occur on the user plane (e.g., the PE-PE implements NAT or NAPT or hosted NAPT procedures), the originating PD-PE is required to 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 end-point is behind a hosted-NAPT), the originating PD-PE can optionally include the Latching-Indication AVP set to "RELATCH".

The originating PD-PE is required to store for future use the contents of the Binding-Output-List AVP received within the Binding-Information AVP contained in the AAA message.

Originating PD-PE's actions are matter of local policies for the following conditions: when the originating PD-PE does not receive the AAA message, or when it arrives after the originating PD-PE timer has expired, or when it arrives with an indication different from DIAMETER_SUCCESS.

7.2.2 Procedures at the intra-domain peer PD-PE

The intra-domain peer PD-PE can optionally receive the AAR message from the originating PD-PE with modified service information. Based on the contents of the AAR message, the intra-domain peer PD-PE is required to coordinate any required modifications to the existing resource reservation over the Rt interface, to existing enabled policy enforcement settings, or to both.

The intra-domain peer PD-PE is required to acknowledge the session modification by issuing an AAA message back to the originating PD-PE only after all actions taken upon the Rt, the Rw, or both interfaces are completed.

Depending on the value of the Flow-Status AVP received from the originating PD-PE, the intra-domain peer PD-PE is required to interpret the session modification as a commitment of requested resources or as a removal of the commitment of requested resources.

Once the intra-domain peer PD-PE recognizes, based on the contents of an AAR message and possibly on configuration data, that policy enforcement functions are requested on the transport plane, the intra-domain peer PD-PE is required to use the contents of the AAR message in order to enforce any functions needed over the Rw interface.

7.3 Session termination

7.3.1 Procedures at the originating PD-PE

When the session is terminated, in stateful operation the originating PD-PE is required to terminate the Diameter session. It terminates the Diameter session by sending a Session-Termination-Request (STR) message with the associated Session-Id AVP to the intra-domain peer PD-PE. In stateless operation, it is required to request session termination by sending an AAR message containing the associated Class AVP and the Resource-Reservation-Mode AVP with a value of RESOURCE_RELEASE (3).

7.3.2 Procedures at the intra-domain peer PD-PE

Session termination is signalled by receipt of an STR message from the originating PD-PE in stateful operation, or receipt of an AAR 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 intra-domain peer PD-PE is required to trigger the session termination procedure over the Rt interface and revoke any transport plane actions associated with the session.

7.4 PD-PE notifications

On a request basis, the Rd interface supports indication of relevant events such as revocation of established resource reservations. The intra-domain peer PD-PE sends unsolicited RAR messages to the originating PD-PE to notify such events. These messages are implicitly requested through policies established in the intra-domain peer PD-PE via the Specific-Action AVP of the initial AAR message.

The originating PD-PE can optionally specify, in the Specific-Action AVP of the initial AAR message, the events it wants to be informed of.

If one of the events supported at the Rd interface occurs, the intra-domain peer PD-PE is required to send an unsolicited RAR message to the originating PD-PE containing:

- the value of the Specific-Action AVP, indicating the event that occurred; and
- optionally, the appropriate Abort-Cause AVP value.

8 Protocol specifications

The Diameter Base Protocol as specified in [IETF RFC 3588] is used to support information transfer at the Rd interface. Procedures and protocols in [IETF RFC 3588] or its future revisions by IETF are required to be applied.

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

This Recommendation defines the Rd Diameter application ITU-T Rd with application ID 16777274. The vendor identifier assigned by IANA to ITU-T is 11502.

9 Messages specifications

9.1 Commands

Existing Diameter command codes from the Diameter Base Protocol, [IETF RFC 3588]; the network access server diameter application, [IETF RFC 4005]; and the Sh application described in [ETSI TS 129 329], are used. Support for these commands is required as indicated in Tables 9-1 and 9-2.

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

Table 9-1 – Required commands for stateful operation

Command	Abbreviation	Defining reference	Command code
AA-Request	AAR	[IETF RFC 4005]	265
AA-Answer	AAA	[IETF RFC 4005]	265
Re-Auth-Request	RAR	[IETF RFC 3588]	258
Re-Auth-Answer	RAA	[IETF RFC 3588]	258
Session-Termination-Request	STR	[IETF RFC 3588]	275
Session-Termination-Answer	STA	[IETF RFC 3588]	275

Table 9-2 – Required commands for stateless operation

Command	Abbreviation	Defining reference	Command code
AA-Request	AAR	[IETF RFC 4005]	265
AA-Answer	AAA	[IETF RFC 4005]	265

9.2 Experimental-Result-Code AVP values

This clause defines specific values of the Experimental-Result-Code AVP used in this Recommendation. It is imported from ETSI specification, as indicated in clause 9.2.1.

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

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

INSUFFICIENT_RESOURCES (4041)

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

9.3 Attribute-value pairs (AVPs)

Tables 9-3 to 9-5 summarize the AVPs used in this Recommendation, beyond those defined in [IETF RFC 3588].

Table 9-3 describes the Diameter AVPs used within this Recommendation that have been defined by [ETSI TS 183 017], providing their AVP codes and value types. The Vendor-Id header of all AVPs identified in Table 9-3 is required to be set to ETSI (13019). These AVPs are described in this Recommendation for information, however the normative details for these AVPs are contained in [ETSI TS 183 017].

The mandatory flag (M) is optionally set for the Transport-Class AVP and is required to be cleared for all other AVPs in Table 9-3. The vendor flag (V) is required to be set for all AVPs in Table 9-3. ETSI vendor id (13019) is required to appear in the AVP header. All AVPs in Table 9-3 can optionally be encrypted.

Table 9-3 – Diameter AVPs imported from [ETSI TS 183 017]

Attribute name	AVP code	Value type
Transport-Class	311	Unsigned32
Binding-Information	450	Grouped
Binding-Input-List	451	Grouped
Binding-Output-List	452	Grouped
V6-Transport-Address	453	Grouped
V4-Transport-Address	454	Grouped
Port-Number	455	Unsigned32
Reservation-class	456	Unsigned32
Latching-Indication	457	Enumerated
Reservation-Priority	458	Enumerated
Service-Class	459	UTF8String

Table 9-4 describes the Diameter AVPs imported from [ETSI ES 283 034]. The Vendor-Id header of all AVPs defined in Table 9-4 is required to be set to ETSI (13019).

The mandatory flag (M) is required to be cleared for the AVPs listed in Table 9-4. The vendor flag (V) is required to be set for all AVPs in Table 9-4 and ETSI vendor id (13019) is required to appear in the AVP header. The AVPs in Table 9-4 are required to be sent unencrypted.

Table 9-4 – Diameter AVPs imported from [ETSI ES 283 034]

Attribute name	AVP code	Value type
Globally-Unique-IP-Address	300	Grouped
Address-Realm	301	OctetString

Table 9-5 describes the Diameter AVPs defined in [ETSI TS 129 209] and used within this Recommendation. These AVPs are described in this Recommendation for information. The Vendor-Id header of all AVPs defined in Table 9-5 is required to be set to 3GPP (10415).

[ITU-T Q.3301.1] modifies the syntax of certain Grouped AVPs defined in [ETSI TS 129 209] by adding one or more optional AVP(s) to the syntax specified in [ETSI TS 129 209]. AVPs defined in [ETSI TS 129 209] but not listed in the following table are not recommended to be sent by Diameter conforming to this Recommendation and are required to be ignored by receiving entities.

The mandatory flag (M) is required to be set for the AVPs in Table 9-5. The vendor flag (V) is required to be set for all AVPs in Table 9-5 and 3GPP vendor id (10415) is required to appear in the AVP header. The AVPs in Table 9-5 can optionally be sent encrypted.

Table 9-5 – Diameter AVPs imported from [ETSI TS 129 209]

Attribute name	AVP code	Value type
Abort-Cause	500	Enumerated
Access-Network-Charging-Address	501	Address
Access-Network-Charging-Identifier	502	Grouped
Access-Network-Charging-Identifier-Value	503	OctetString
AF-Application-Identifier	504	OctetString
AF-Charging-Identifier	505	OctetString
Authorization-Token	506	OctetString
Flow-Description	507	IPFilterRule
Flow-Grouping	508	Grouped
Flow-Number	509	Unsigned32
Flows	510	Grouped
Flow-Status	511	Enumerated
Flow-Usage	512	Enumerated
Specific-Action	513	Enumerated
Max-Requested-Bandwidth-DL	515	Unsigned32
Max-Requested-Bandwidth-UL	516	Unsigned32
Media-Component-Description	517	Grouped
Media-Component-Number	518	Unsigned32
Media-Sub-Component AVP	519	Grouped
Media-Type	520	Enumerated
RR-Bandwidth	521	Unsigned32
RS-Bandwidth	522	Unsigned32
SIP-Forking-Indication	523	Enumerated

10 Security considerations

The security aspects are not applicable to intra-domain operations.

SERIES OF ITU-T RECOMMENDATIONS

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

Printed in Switzerland
Geneva, 2010