International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.3307.1

(06/2009)

SERIES Q: SWITCHING AND SIGNALLING

Signalling requirements and protocols for the NGN – Resource control protocols

Resource control protocol No. 7 – Protocol at the interface between inter-domain policy decision physical entities (Ri interface)

Recommendation ITU-T Q.3307.1

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.3307.1

Resource control protocol No. 7 – Protocol at the interface between inter-domain policy decision physical entities (Ri interface)

Summary

Recommendation ITU-T Q.3307.1 provides stage 3 specification of the Ri interface between policy decision physical entities (PD-PE) in different domains using the Diameter protocol. The functional requirements and the stage 2 specification for the Ri interface are defined in Recommendation ITU-T Y.2111. This Recommendation as well as Recommendation ITU-T Y.2111 supports nomadism.

Source

Recommendation ITU-T Q.3307.1 was approved on 29 June 2009 by ITU-T Study Group 11 (2009-2012) under Recommendation ITU-T A.8 procedures.

Keywords

Diameter, resource control, Ri application.

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.3307.1

Resource control protocol No. 7 – Protocol at the interface between inter-domain policy decision physical entities (Ri interface)

1 Scope

The protocol specified in this Recommendation is used to support inter-domain PD-PE communication when the service control entity (SCE) is not capable of interacting with the PD-PE in each domain crossed by the media flow.

The Ri interface is used to control session-based policy. Using the protocol specified in this Recommendation, the original PD-PE can:

– provide information to the peer PD-PE to identify media flows and their required QoS resource characteristics (e.g., QoS class, bandwidth, priority);

– provide service priority information to the peer PD-PE to facilitate appropriate priority handling;

– request resource usage information through the peer PD-PE for charging;

– indicate if the media is recommended to be enabled (i.e., gate opened) when resources are reserved;

– indicate if the media is recommended not to be enabled as soon as the resources are reserved, i.e., the original PD-PE can optionally request that the media gate be opened later;

– if a network address and port translation (NAPT) function is required, request address mapping information so it can do any modifications that may be required for application signalling (e.g., SDP); and

– if a path-coupled resource reservation mechanism is used, indicate to the peer PD-PE whether it wishes to be notified when reservations are obtained and released.

When an authorization token mechanism is used, the peer PD-PE may supply the original PD-PE with one or more authorization tokens which the SCE is required to include in the application signalling messages to the customer premises equipment (CPE).

This Recommendation only discusses per session reservation. The functional requirements and the stage 2 specification for this interface are defined in [ITU-T Y.2111]. As indicated in [ITU-T Y.2111], this Recommendation only supports nomadism; other use cases are for further study.

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 Q.3303.1] Recommendation ITU-T Q.3303.1 (2007), *Resource control protocol No. 3 – Protocol at the interface between a Policy Decision Physical Entity (PD-PE) and Policy Enforcement Physical Entity (PE-PE): COPS alternative*.

[ITU-T Y.110] Recommendation ITU-T Y.110 (1998), *Global Information Infrastructure principles and framework architecture*.

[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); LTE; Sh interface based on the Diameter protocol*.

[ETSI TS 133 210] ETSI TS 133 210 V8.2.0 (2009), *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 8.2.0 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 2960] IETF RFC 2960 (2000), *Stream Control Transmission Protocol*.

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

[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 terms defined elsewhere:

3.1.1 gate [ITU-T Y.2111]: A construct used to enable or disable the forwarding of IP packets based on the policy decision. A gate is identified by the classifier (e.g., IPv4 5-tuple) and direction of a media flow or a group of media flows that are in conformance to the same set of policy decisions.

3.1.2 policy decision physical entity (PD-PE) [ITU-T Q.3303.1]: The PD-PE is an implemented instance of the policy decision functional entity (PD-FE) as defined in [ITU-T Y.2111].

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 attribute-value pair (AVP): An attribute-value pair corresponds to an information element in a Diameter message (see [IETF RFC 3588]).

3.2.2 domain: A collection of physical or functional entities which are owned and operated by a player and can include entities from more than one role. The extent of a domain is defined by a useful context and one player can have more than one domain.

3.2.3 originating policy decision physical entity (PD-PE): A PD-PE in an originating domain which triggers QoS resource requests to a peer PD-PE.

NOTE – "The originating PD-PE" is an implemented instance of the "original PD-FE" described in [ITU-T Y.2111].

3.2.4 peer policy decision physical entity (PD-PE): A PD-PE in the interconnected domain which receives QoS resource requests from an originating PD-PE.

3.2.5 stateful operation: An operation in which a peer PD-PE stores a Session-Id value received in an AA-Request message.

3.2.6 stateless operation: An operation in which a peer PD-PE does not store a Session-Id received in an AA-Request message.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AAA	AA-Answer
AAR	AA-Request
AVP	Attribute-Value Pair
CEA	Capability Exchange Answer
CER	Capability Exchange Request
CGPE-PE	Customer premises network Gateway Policy Enforcement Physical Entity
CPE	Customer Premises Equipment
CPN	Customer Premises Network
GPRS	General Packet Radio Service
IP-CAN	Internet Protocol Connectivity Access Network
IPSec	Internet Protocol Security
NACE	Network Attachment Control Entity
NACF	Network Attachment Control Function
NAPT	Network Address and Port Translation
NAT	Network Address Translation
PD-PE	Policy Decision Physical Entity
PE-PE	Policy Enforcement Physical Entity
QoS	Quality of Service

RACF	Resource and Admission Control Functions
RAC-PE	Resource and Admission Control Physical Entity
RAR	Re-Auth-Request
SCE	Service Control Entity
SDI	Session Description Information
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SLA	Service Level Agreement
TRC-PE	Transport Resource Control Physical Entity
TRE-PE	Transport Resource Enforcement Physical Entity
UE	User Equipment

5 Conventions

There are no specific conventions within this Recommendation.

6 Ri interface

6.1 Overview

The RI reference point interface is defined in [ITU-T Y.2111] and is used for service-based policy set-up information between the originating and peer PD-PEs for inter-domain communication. Through the Ri, an originating PD-PE triggers admission control in the interconnected domain by forwarding originating PD-PE requests. Also through the Ri, the interconnected domain communicates its admission control results back to the originating domain. Requests and results are per-session reservation or per-aggregate reservation.

Figure 6-1, which shows the generic resource and admission control functional architecture in NGN, is a replica of Figure 5 of [ITU-T Y.2111] with:

– "service control functions" being replaced by "service control entity" (SCE);
– "network attachment control functions" being replaced by "network attachment control entity (NACE)";
– "CGPE-FE" being replaced by "CGPE-PE";
– "PD-FE" being replaced by "PD-PE";
– "TRC-FE" being replaced by "TRC-PE";
– "TRE-FE" being replaced by "TRE-PE";
– "PE-FE" being replaced by "PE-PE"; and
– "RACF" being replaced by "RAC-PE".

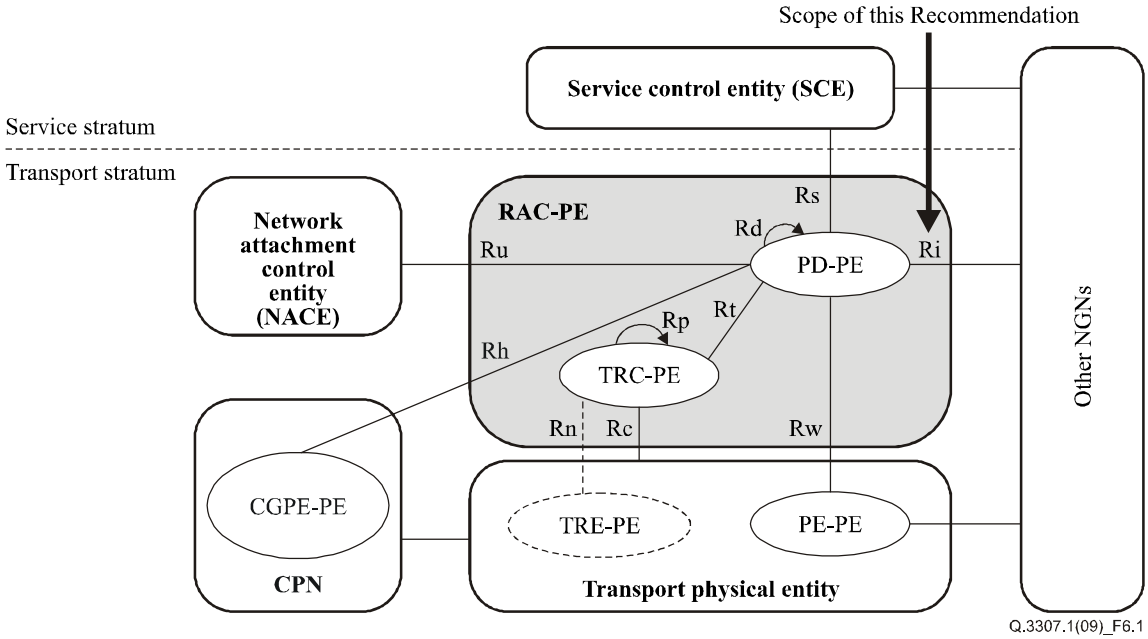

Figure 6-1 – Generic resource and admission control functional architecture in NGN

6.2 Functional elements and capabilities

6.2.1 Policy decision physical entity (PD-PE)

PD-PE is a functional element that coordinates the resource reservation requests. The peer PD-PE makes the final decision regarding network resource and admission control based on network policies or forwarded reservation requests from originating PD-PE, service level agreements (SLAs), service information provided by the SCE, transport subscription information provided by the network attachment control function (NACF) in access networks, and resource-based admission decision results provided by the TRC-PE. The PD-PE controls the gates in the PE-PEs at a per-flow level.

6.2.2 Per-session reservation

The Dynamic-Firewall-Working-Mode AVP defined in clause 9.3.13 of [ITU-T Q.3301.1] is not supported at the Ri interface. It is also recommended that charging information between operators not be passed through the Ri interface. A list of AVPs which are not supported at the Ri interface are provided in clause 10.3.

7 Procedures

7.1 Procedures for a per-session reservation

The originating PD-PE triggers a QoS resource request to the peer PD-PE via the Ri interface, indicating the desired QoS requirements. In return, the originating PD-PE receives a response. The peer PD-PE informs the originating PD-PE when a request has been denied and can optionally provide information on an acceptable level of QoS. The peer PD-PE sends a request to the PE-PE to implement the final admission decisions. In some scenarios (e.g., the resource information of the bearer network changes, or overtime of the connection timer), the peer PD-PE can optionally send the resource information to the originating PD-PE in the adjacent bearer network. The originating PD-PE in the adjacent bearer network can optionally update local resource information according to the received resource information.

7.2 Initial reservation for a session

7.2.1 Procedures at the originating PD-PE

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

The AAR may contain an Authorization-Lifetime AVP as an indication of the maximum lifetime that it is requesting.

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

The originating PD-PE may include the Operation-Indication AVP to indicate whether the peer PD-PE must perform NAPT control and network address translation (NAT) traversal functions, or QoS resource reservation, or both, after receiving the AAR.

The originating PD-PE is required to include the corresponding Media-Component-Description AVP(s) in the 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 IP flows described within the service description. This is distributed to the forwarding plane.

When providing a given Media-Component-Description AVP in the initial AAR, the originating PD-PE can optionally request the 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 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 AAR 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 the NAT, or NAPT, or hosted NAPT procedure), the following action is performed. After the originating PD-PE receives an SDI that is associated with the endpoint served by it, the originating PD-PE is required to include the Binding-Information AVP with the Input-List AVP.

The originating PD-PE can optionally include the SDP-Direction AVP along with the Binding-Information AVP to indicate whether the address set in the Output-list AVP is expected to be received in the AA-Answer (AAA) in either of the following:

– originating core network; or

– peer core network.

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

Based on local configuration data, the originating PD-PE can optionally include the TLM-PE-Identifier AVP in AAR to indicate the TLM-PE related to the user.

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

– the User-Name AVP; or

– the Globally-Unique-Address AVP.

The User-Name AVP is defined in [IETF RFC 3588]. The Globally-Unique-Address AVP is defined in [ETSI ES 283 034].

The originating PD-PE can optionally specify the Reservation-Priority AVP in the AAR and/or within a Media-Component-Description AVP of the AAR.

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

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 in subsequent messages relating to this session as it is placed in the initial AAR.

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) which are present in the AAA message. The originating PD-PE is required to include the stored Class AVP(s) in any message it sends to the peer PD-PE related 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 use.

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

7.2.2 Procedures at the peer PD-PE

The 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 was present in the initial AAR or if the peer PD-PE chooses stateless operation for the current session, the peer PD-PE is required to return an Auth-Session-State AVP in the AAA to indicate its decision.

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

In stateless operation, the peer PD-PE does not store the received Session-Id. Instead, it generates one or more Class AVPs based on local policy data (possibly the contents of the AAR and of messages received over other interfaces). The one or more Class AVPs will contain the information needed for the peer 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;
– 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 peer PD-PE also forwards equivalent state-preserving tokens to the TRC-PE(s) and PE-PE when it communicates with them. Then the peer PD-PE receives those tokens back again in messages from TRC-PE(s) and PE-PE.

The peer PD-PE can optionally acquire user profile information from the TLM-FE in the NACE according to the TLM-PE-Identifier AVP, if present.

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

– NAT control only:

  In NAT control only, the peer PD-PE is required to exercise NAPT control and NAT traversal function control at the PE-PE based on the information indicated by the Binding-Information AVP and optionally the SDP-Direction AVP.

– QoS resource reservation only:

  In QoS resource reservation only, the peer PD-PE is required to perform QoS resource reservation based on the information indicated by the Resource-Reservation-Mode AVP and media information.

– QoS resource reservation and NAT control:

  In QoS resource reservation and NAT control, peer PD-PE shall perform both of the actions requested.

If the Resource-Reservation-Mode AVP is present, the peer PD-PE is required to use it to determine whether the initial AAR is for:

– authorization only (pull mode);

– authorization and reservation (push mode, first phase of two phase operation); 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 for individual components and sub-components, 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 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). The peer PD-PE can also infer a request for authorization if the Flow-Status AVP is set to any variant of ENABLED (0), (1) or (2).

The peer PD-PE is required to use the contents of the AAR in order to enforce any functions needed over the Rt and Rw interfaces whenever it recognizes that policy enforcement functions are requested on the transport plane and based on the contents of an AAR and possibly on configuration data.

If the AAR contains the Media-Component-Description AVP(s), the peer PD-PE is required to trigger the resource reservation procedure towards the TRC-PE. If the AAR contains Flow-Grouping AVP(s), the 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 (e.g., the AAR may contain AVPs such as Service-Class) and the local policies, the peer PD-PE can optionally request opening or closing of a gate.

The peer PD-PE is required to wait for the result of the above interaction(s) (i.e., interactions described in this clause 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 and/or Rw 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 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 peer PD-PE receives a reservation failure notification via the Rt interface), the 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.

7.3 Session modification

7.3.1 Procedures at the originating PD-PE

During the session modification, the originating PD-PE is required to send an updated SDI to the peer PD-PE. The updated SDI is created 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 IP flows described within the service description. This is distributed to the forwarding plane.

The originating PD-PE 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 commitment status: change the Flow-Status AVP of the corresponding Media-Component-Description AVP and/or 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 as an indication of the maximum lifetime that it is requesting.

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

It is required that the Reservation-Priority AVP associated with a reservation request or a media component is not modified if present.

If an updated SDI pointing towards the endpoint served by the originating PD-PE is available, and if it 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 endpoint 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.

The behaviour 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, is a matter of local policies.

7.3.2 Procedures at the peer PD-PE

The peer PD-PE may receive the AAR message from the originating PD-PE with modified service information. Based on the contents of the AAR message, the peer PD-PE is required to coordinate any required modifications to the existing resource reservation over the Rt interface and/or to existing enabled policy enforcement settings. The 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 through Rt and/or Rw interfaces are completed.

Depending on the value of the Flow-Status AVP received from the originating PD-PE, the 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 peer PD-PE recognizes, based on the contents of the AAR and possibly on configuration data, that policy enforcement functions are requested on the transport plane, the peer PD-PE is required to use the contents of the AAR message in order to enforce any functions needed over the Rw interface.

7.4 Session termination

7.4.1 Procedures at the originating PD-PE

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

7.4.2 Procedures at the peer PD-PE

Session termination is signalled by receipt of a Session-Termination-Request 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 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.

7.5 PD-PE notifications

On a request basis, the Ri interface supports the indication of relevant events such as revocation of established resource reservations. The 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 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 command, which events it wants to be informed about.

If one of the events supported at the Ri interface occurs, the 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 specification

The Diameter base protocol is specified in [IETF RFC 3588] and is used to support information transfer at the Ri interface. Conformance to [IETF RFC 3588] is required in this Recommendation except as otherwise indicated.

In addition to the AVPs from [IETF RFC 3588], the Diameter messages sent over the Ri interface use other AVPs as indicated in clause 10.4.

This Recommendation defines the Ri Diameter application with application ID 16777271. The vendor identifier assigned by IANA to ITU-T is 11502.

This Recommendation reuses Diameter 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 (i.e., IETF and 3GPP). However, this Recommendation specifies default values and behaviours for the use of some of these attributes in the Ri application.

With regard to the Diameter protocol defined over the Ri interface, the peer 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 originating PD-PE acts as the Diameter client, in the sense that it is the network element requesting authorization to use bearer path network resources.

9 Use of the Diameter base protocol

9.1 Securing Diameter messages

The method defined in [ETSI TS 133 210] is required to be used for secure transport of Diameter messages.

9.2 Accounting functionality

Accounting functionality (accounting session state machine, related command codes and AVPs) is not used over the Ri interface.

9.3 Use of sessions

As described in clauses 6, operation for a given session can be stateful or stateless. Stateless operation is always indicated definitively by a value of NO_STATE_MAINTAINED in an Auth-Session-State AVP returned by the peer PD-PE in the AAA message responding to the initial AAR message. For stateful operation, the Session-Id AVP is required to be present in all messages passing between the PD-PEs, as described in [IETF RFC 3588]. The Session-Termination-Request (STR) and Session-Termination-Answer (STA) commands defined in [IETF RFC 3588] are required to be used to terminate the Diameter user sessions. For stateless operation, the Class AVP returned in the AAA message responding to the initial AAR message is required to be present in all messages passing between the PD-PEs. The Diameter user session is required to be terminated by sending an AAR message containing the Class AVP and the Resource-Reservation-Mode AVP with a value of RESOURCE_RELEASE (3).

9.4 Transport protocol

Diameter messages over the Ri interface are required to make use of SCTP [IETF RFC 2960] and the SCTP checksum method specified in [IETF RFC 3309].

9.5 Routing considerations

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

The originating PD-PE obtains the contact address of the peer 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 are required to be present in the request.

To ensure that messages are routed to the correct application at the destination host, the Diameter message header sent is required to contain the Ri application identifier (16777271) as agreed during CER/CEA negotiation.

9.6 Advertising application support

The Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands are specified in [IETF RFC 3588]. The Diameter base application identifier (0) is required to be used in header parts of Diameter messages.

The originating PD-PE and the peer PD-PE are required to advertise the support of the Ri application by including an instance of the Vendor-Specific-Application-Id grouped AVP within the Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands for the application supported, according to the following rules:

1) The originating PD-PE is required to advertise which type of operation the Ri application supports.
2) The peer PD-PE is required to respond by indicating the subset of applications it is prepared to support, out of those offered by the originating PD-PE. If this subset is empty, the peer PD-PE's response is required to be as described in clause 5.3 of [IETF RFC 3588].

If originating and peer PD-PEs indicate support of the Ri application, then the Ri application identifier (16777271) is required to be used in the Diameter message header of all subsequent messages exchanged within this association.

Support of the Ri application within the CER/CEA is indicated by supplying an instance of the Vendor-Specific-Application-Id grouped AVP containing a Vendor-Id AVP set to ITU-T (11502) and an Auth-Application-Id AVP set to Ri application ID (16777271).

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) is required to indicate the manufacturer of the Diameter node as per [IETF RFC 3588].

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

10 Message specification

10.1 Use of namespaces

This clause contains the namespaces that are either listed in Appendix II of [ITU-T Q.3301.1], or the values assigned to existing namespaces managed by IANA.

10.1.1 AVP codes

This Recommendation uses AVP values from the AVP code namespace managed by ETSI and ITU-T for their Diameter vendor-specific applications.

10.1.2 Application-ID value

This Recommendation defines the Ri Diameter application with application ID 16777271. The vendor identifier assigned by IANA to ITU-T is 11502.

10.2 Commands

Existing Diameter command codes from the Diameter base protocol [IETF RFC 3588] and the network access server diameter application [IETF RFC 4005] are used, as shown in Tables 10-1 and 10-2. Support for these commands is required as defined in [ITU-T Q.3301.1].

Table 10-1 – 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
Abort-Session-Request	ASR	[IETF RFC 3588]	274
Abort-Session-Answer	ASA	[IETF RFC 3588]	274

Table 10-2 – 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
Push-Notification-Request	PNR	[ETSI TS 129 329]	309
Push-Notifications-Answer	PNA	[ETSI TS 129 329]	309

10.3 AVPs that are not supported over the Ri interface

In the scenario of inter-operator communication, the following AVPs will not be used:

– Access-Network-Charging-Address AVP.

– Access-Network-Charging-Identifier AVP.

– Access-Network-Charging-Identifier-Value AVP.

10.4 Descriptions of specific AVPs

AVPs identified in Tables 10-3, 10-4 and 10-5, which are described in [ETSI TS 183 017], [ETSI ES 283 034] and [ETSI TS 129 209], are applicable for the Ri interface. Procedures specified in [ITU-T Q.3301.1] for use of some of these AVPs are modified in this Recommendation. Affected AVPs are described in clauses 10.4.1 to 10.4.11.

Table 10-3 describes the Diameter AVPs that are used within this Recommendation that have been defined by ETSI [ETSI TS 183 017].

The mandatory flag (M) is optionally set for the Transport-Class AVP and is required to be clear for all other AVPs in Table 10-3. The vendor flag (V) is required to be set for all AVPs in Table 10-3, and ETSI vendor ID (13019) is required to appear in the AVP header. All AVPs in Table 10-3 can optionally be encrypted.

Table 10-3 – 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 10-4 describes the Diameter AVPs imported from [ETSI ES 283 034]. The Vendor-Id header of all AVPs defined in Table 10-4 is required to be set to ETSI (13019).

The mandatory flag (M) is required to be cleared for the AVPs in Table 10-4. The vendor flag (V) is required to be set for all AVPs in Table 10-4, and ETSI vendor ID (13019) is required to appear in the AVP header. The AVPs in Table 10-4 are required to be sent unencrypted.

Table 10-4 – Diameter AVPs imported from [ETSI ES 283 034]

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

Table 10-5 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 10-5 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 Table 10-5, should not 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 10-5. The vendor flag (V) is required to be set for all AVPs in Table 10-5, and 3GPP vendor ID (10415) is required to appear in the AVP header. The AVPs in Table 10-5 can be optionally sent encrypted.

Table 10-5 – 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	519	Grouped
Media-Type	520	Enumerated
RR-Bandwidth	521	Unsigned32
RS-Bandwidth	522	Unsigned32
SIP-Forking-Indication	523	Enumerated

10.4.1 Service-Class AVP

The Service-Class AVP (AVP code 459) is of type UTF8String [IETF RFC 3588], and it contains the service class requested by the originating PD-PE. The service class is to be checked against local policies in the PD-PEs.

10.4.2 Acceptable-Service-Info AVP

The Acceptable-Service-Info AVP (AVP code 526) is of type Grouped [IETF RFC 3588], and contains the maximum bandwidth for a session and/or for specific media components that will be authorized by the peer PD-PE. The Max-Requested-Bandwidth-DL AVP and Max-Requested-Bandwidth-UL AVP directly within the Acceptable-Service-Info AVP indicate the acceptable bandwidth for the entire session. The Max-Requested-Bandwidth-DL AVP and Max-Requested-Bandwidth-UL AVP within a Media-Component-Description AVP included in the Acceptable-Service-Info AVP indicate the acceptable bandwidth for the corresponding media component.

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

AVP format:

```
Acceptable-Service-Info::= < AVP Header: 526 10415>
                            *[ Media-Component-Description]
                             [ Max-Requested-Bandwidth-DL ]
                             [ Max-Requested-Bandwidth-UL ]
                            *[ AVP ]
```

10.4.3 Flow-Description AVP

The Flow-Description AVP (AVP code 507) is of type IPFilterRule [IETF RFC 3588], and defines a packet filter for an IP flow with the following information:

– direction (in or out);

– source and destination IP address (possibly masked) or user identifier;

– protocol;

– source and destination port (list or ranges).

The IPFilterRule type [IETF RFC 3588] is required to be used with the following restrictions:

– The Action field is required to be "permit".

– "options" field is prohibited to be used.

– The invert modifier "!" for addresses is prohibited to be used.

– The keyword "assigned" is prohibited to be used.

If any of these restrictions is not observed by the originating PD-PE, the peer PD-PE is required to send an error message response to the originating PD-PE containing the Experimental-Result-Code AVP with value FILTER_RESTRICTIONS.

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

The direction "in" means an IP flow direction from the terminal with the correlation identifier specified in the initial AAR message to the other terminal, and the direction "out" means an IP flow opposite of the "in" direction. The correlation identifier is defined in clause 7.2.1. For the source and destination user identifier, a transport subscriber identifier may be used.

10.4.4 AF-Application-Identifier AVP

The AF-Application-Identifier AVP (AVP code 504) is of type OctetString [IETF RFC 3588], and it contains information that identifies the particular service that the originating PD-PE service session belongs to. This information can optionally be used by the PD-PE to differentiate QoS for different application services. For example, the AF-Application-Identifier can optionally be used as additional information together with the Media-Type AVP when the QoS class for the bearer authorization at the Ri interface is selected. The AF-Application-Identifier may be used also to complete the QoS authorization with application-specific default settings in the PD-PE if the originating PD-PE does not provide full Media-Component-Description information.

10.4.5 AF-Charging-Identifier AVP

The AF-Charging-Identifier AVP (AVP code 505) is of type OctetString [IETF RFC 3588], and contains the charging identifier that is sent by the originating PD-PE. This information can optionally be used for correlation of charging information obtained from the transport stratum.

10.4.6 Binding-Information AVP

The Binding-Information AVP (AVP code 450) is of type Grouped [IETF RFC 3588] and is sent between PD-PEs in order to convey binding information required for NAT, NAPT, NAT-PT and NAPT-PT control.

AVP format:

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

10.4.7 Binding-Input-List AVP

The Binding-Input-List AVP (AVP code 451) is of type Grouped [IETF RFC 3588] and contains a list of transport addresses for which a binding is requested. The originating PD-PE constructs the Binding-Input-List using session description information (SDI).

AVP format:

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

10.4.8 Connection-Status-Timer AVP

The Connection-Status-Timer AVP (ITU-T AVP code 1004) is of type Unsigned32 [IETF RFC 3588] and is in units of seconds. The AVP is used to specify the maximum time interval between Diameter messages sent or received for a particular session. The value of zero implies infinity.

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

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

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

If no communication activity is detected for a period significantly exceeding the timer period, the originating PD-PE will assume the session does not exist and release the session.

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

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

10.4.9 Flow-Usage AVP

The Flow-Usage AVP (AVP code 512) is of type Enumerated [IETF RFC 3588], and provides information about the usage of IP Flows. The following values are defined:

– NO_INFORMATION (0)

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

– RTCP (1)

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

NO_INFORMATION is the default value.

10.4.10 Media-Component-Description AVP

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

Within one Diameter message, a single IP flow is prohibited to be described by more than one Media-Component-Description AVP.

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

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

All IP flows within a Media-Component-Description AVP are permanently disabled by supplying a Flow-Status AVP with value "REMOVED". The peer PD-PE can optionally delete corresponding filters and state information.

AVP format:

```
Media-Component-Description ::= < AVP Header: 517 10415>
     { Media-Component-Number } ; Ordinal number of the media comp.
     *[ Media-Sub-Component ] ; Set of flows for one flow identifier
     [ AF-Application-Identifier ]
     [ Media-Type ]
     [ Max-Requested-Bandwidth-UL ]
     [ Max-Requested-Bandwidth-DL ]
     [ Flow-Status ]
     [ RS-Bandwidth ]
     [ RR-Bandwidth ]
     [ Reservation-Class]
     [ Reservation-Priority]
     [ QoS-Downgradable ]
     [ Transport-Class ]
```

10.4.11 Specific-Action AVP

The Specific-Action AVP (AVP code 513) is of type Enumerated [IETF RFC 3588].

Within re-authorization request messages initiated by a peer PD-PE, the Specific-Action AVP determines the type of action being performed in the forwarding plane.

Within an initial AAR message the originating PD-PE can optionally use the Specific-Action AVP to request specific actions from the peer PD-PE. For example, a specific requested action would be to limit reporting of actions being performed in the forwarding plane.

If the Specific-Action AVP is omitted within the initial AAR message, the peer PD-PE is prohibited from generating notifications of any of the events defined below.

The following values are defined:

– Values 0 through 5 are defined by [ETSI TS 129 209] (vendor ID is 10415, 3GPP).

– Values 6 and 7 are defined in [ETSI ES 283 026] (vendor ID 13019, ETSI).

SERVICE_INFORMATION_REQUEST (0)

Within a RAR message or PNR message, this value is required to be used when the peer PD-PE requests the service information from the originating PD-PE for the bearer event. In the AAR message, this value indicates that the originating PD-PE requests the peer PD-PE to demand service information for each bearer authorization.

INDICATION_OF_LOSS_OF_BEARER (2)

Within a RAR message or PNR message, this value is required to be used when the peer PD-PE reports a loss of a bearer (e.g., in the case of GPRS PDP context bandwidth modification to 0 kbit/s) to the originating PD-PE. In the AAR message, this value indicates that the originating PD-PE requests the peer PD-PE to provide a notification at the loss of a bearer.

INDICATION_OF_RECOVERY_OF_BEARER (3)

Within a RAR message or PNR message, this value is required to be used when the peer PD-PE reports a recovery of a bearer (e.g., in the case of GPRS, PDP context bandwidth modification from 0 kbit/s to another value) to the originating PD-PE. In the AAR message, this value indicates that the originating PD-PE requests the peer PD-PE to provide a notification at the recovery of a bearer.

INDICATION_OF_RELEASE_OF_BEARER (4)

Within a RAR message or PNR message, this value is required to be used when the peer PD-PE reports the release of a bearer (e.g., PDP context removal for GPRS) to the originating PD-PE. In the AAR, this value indicates that the originating PD-PE requests the peer PD-PE to provide a notification at the removal of a bearer.

INDICATION_OF_ESTABLISHMENT_OF_BEARER (5)

Within a RAR message or PNR message, this value is required to be used when the peer PD-PE reports the establishment of a bearer (e.g., PDP context activation for GPRS) to the originating PD-PE. In the AAR message, this value indicates that the originating PD-PE requests the peer PD-PE to provide a notification at the establishment of a bearer.

INDICATION_OF_SUBSCRIBER_DETACHMENT (6)

In the AAR message, this value indicates that the originating PD-PE requests the peer PD-PE to provide a notification that the subscriber has been released. In a RAR message or PNR message, the peer PD-PE indicates to the originating PD-PE that the subscriber has been released.

INDICATION_OF_RESERVATION_EXPIRATION (7)

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

INDICATION_OF_CONNECTION_STATUS (8)

Within a RAR message or PNR message, this value is required to be used to indicate that the peer PD-PE requests the originating PD-PE to check the connection status of the session.

NOTE – INDICATION_OF_CONNECTION_STATUS (8) is defined in [ITU-T Q.3301.1].

11 Security considerations

The Ri interface is used for passing service-based policy set-up information between originating and peer PD-PEs for inter-domain communication. This Recommendation considers security threats and potential attacks and defines security requirements. The primary objective of an attacker at the Ri interface is either theft of service or denial of service. It is also possible that the attacker may attempt to achieve breach of confidentiality (e.g., to perform traffic analysis against the target or to determine parameters needed to intercept the user session).

Theft of service can be achieved by impersonating a PD-PE to achieve authorization of the attacker's requests. Alternatively, the attacker can modify the messages in this Recommendation to enable QoS for the attacker's sessions rather than or in addition to those of the real user. Another possibility is that a user captures and replays the messages that set up an earlier session, thereby impersonating the originating PD-PE. These threats imply requirements for:

– authentication of the originating PD-PE;

– message integrity; and

– prevention of replay of messages.

PD-PEs located in different trust environments are required to authenticate each other during security association establishment. The peer PD-PE is required to ignore requests from unauthenticated sources.

This requires special treatment in support of redundancy (which may, in turn, be needed to ensure reliability, or performance, or both). If the peer PD-PE is replicated, an entity that communicates with any such replica is required to use the same authentication information. This introduces an additional requirement that an eavesdropper be unable to repeat a recorded authentication handshake with another replica.

Clause 9.1 recommends the use of [ETSI TS 133 210] to ensure secure transport of Diameter messages. This reference is essentially a profile of IPSec and its accompanying key management. As such, it provides a level of authentication, integrity protection and protection against replay. However, this protection is on a link-by-link basis, so if an attacker is able to get control of an intermediate node, the Diameter session remains vulnerable to man-in-the-middle attacks. Operators relying only on IPSec protection are therefore advised to be cautious in the use of agents to proxy or relay Diameter messages between the originating and peer PD-PEs. Further considerations along this line are provided in clause 13 (security considerations) of [IETF RFC 3588], which operators are advised to consult.

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

Denial of service attacks can proceed using various means. One possibility is that the attacker creates overload conditions by causing a large number of UE requests for service over a sustained period. These might be designed to impose load on the peer PD-PE while avoiding charges to the subscribers whose equipment is being used by causing the sessions to be aborted before they become billable. A more dangerous case could be that of an originating PD-PE that is under the control of an attacker.

It may be desirable for the peer PD-PE implementation to provide means for identifying patterns of overload-generating traffic. In this way, overload controls can be applied to the PD-PEs originating that traffic without affecting service provided to other originating PD-PEs.

In stateless operation, the originating PD-PE passes state information essential to a peer PD-PE in a different domain. The possibility exists that this information may be modified either deliberately or accidentally before being passed back to the originating PD-PE. Thus, integrity protection for this off-loaded state is required to be applied at the application level. Since this state may include information about the PD-PE operator's network that the operator may not wish to share with others, confidentiality protection in the form of encryption is also recommended to be applied to the state information.

Appendix I

Basic signalling procedures for Ri interface

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

Figure I.1 shows an example of inter-domain communication for the nomadism scenario defined in [ITU-T Y.2111]. In the nomadism scenario, the Ri interface is used for communicating end-to-end QoS signalling.

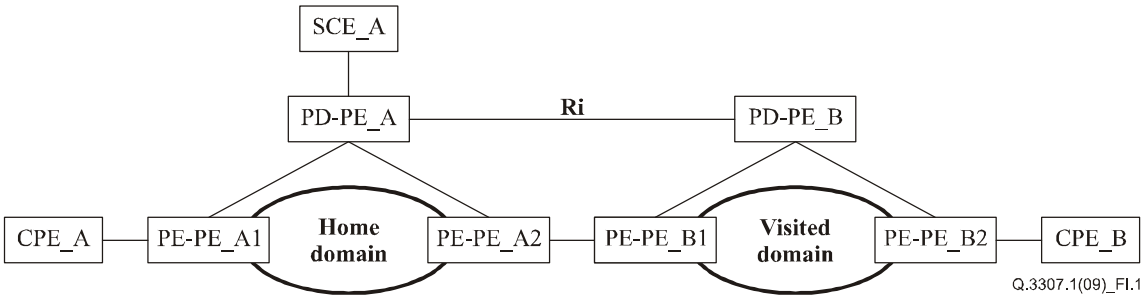

Figure I.1 – Inter-domain communication for nomadism

I.1 Resource reservation procedure

Figure I.2 shows the resource reservation procedure for nomadism. SCE_A is triggered to send a QoS resource reservation request to PD-PE_A. PD-PE_A coordinates the QoS resources at PE-PE_A1 and PE-PE_A2 (see Figure I.1). PD-PE_A sends a QoS resource reservation request (AAR) to PD-PE_B (i.e., AAR (Ri)) to coordinate QoS resources at PE-PE_B1 and PE-PE_B2. As a result of processing the QoS resource reservation request, PD-PE_B sends a response (AAA) message back to PD-PE_A (i.e., AAA (Ri)).

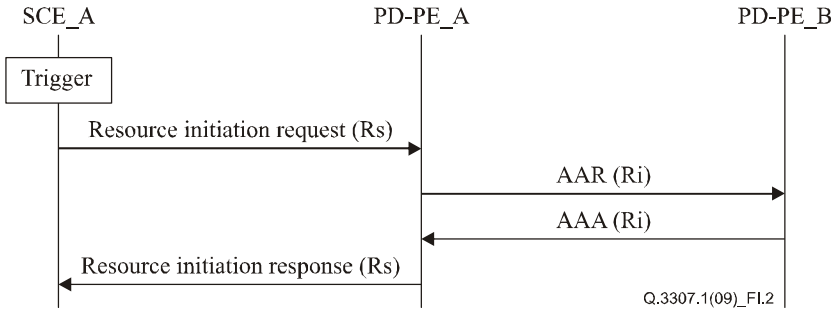

Figure I.2 – Inter-domain QoS resource reservation signalling procedure over Ri

I.2 Resource release procedure

Figure I.3 shows the resource release procedure for nomadism. SCE_A is triggered to send a session termination request to PD-PE_A. PD-PE_A releases the QoS resource at PE-PE_A1 and PE-PE_A2. PD-PE_A sends a QoS resource release request (STR) to PD-PE_B to release QoS resources at PE-PE_B1 and PE-PE_B2. As a result of processing the QoS resource release request, PD-PE_B sends a response (STA) message back to PD-PE_A.

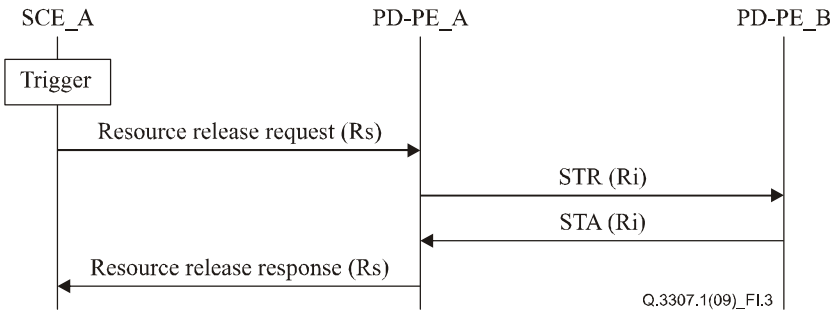

Figure I.3 – Inter-domain QoS resource release signalling procedure over Ri

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