International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.3223

(06/2009)

SERIES Q: SWITCHING AND SIGNALLING

Signalling requirements and protocols for the NGN – Signalling and control requirements and protocols to support attachment in NGN environments

Requirements and protocol for the interface between a transport location management physical entity and a policy decision physical entity (Ru Interface)

Recommendation ITU-T Q.3223

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.3223

Requirements and protocol for the interface between a transport location management physical entity and a policy decision physical entity (Ru Interface)

Summary

Recommendation ITU-T Q.3223 describes requirements and protocol for the Ru interface between a transport location management physical entity (TLM-PE) in a network attachment control entity (NACE) and a policy decision physical entity (PD-PE) in a resource and admission control entity (RACE) of ITU-T next generation network (NGN) release 1.

Source

Recommendation ITU-T Q.3223 was approved on 29 June 2009 by ITU-T Study Group 11 (2009-2012) under Recommendation ITU-T A.8 procedures.

Keywords

Network attachment, next generation network (NGN), Ru interface.

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.3223

Requirements and protocol for the interface between a transport location management physical entity and a policy decision physical entity (Ru Interface)

1 Scope

This Recommendation defines the requirements and protocol for the Ru interface (identical to the TC-TC1 interface defined in [ITU-T Y.2012]) between a transport location management physical entity (TLM-PE) in a network attachment control entity (NACE) and a policy decision physical entity (PD-PE) in a resource and admission control entity (RACE) of ITU-T NGN release 1 architecture.

Whenever applicable, this Recommendation specifies the requirements for the Ru interface referring to the Diameter base specifications. Whenever needed, extensions to Diameter-based specifications are provided in this Recommendation.

2 References

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

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

[ITU-T Y.2014] Recommendation ITU-T Y.2014 (2008), *Network attachment control functions in next generation networks*.

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

[ITU-T Y.2701] Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN release 1*.

[ETSI TS 129 229] ETSI TS 129 229 v8.6.0 (2009), *Digital cellular telecommunication system (Phase 2+); Universal Mobile Telecommunications system (UMTS); LTE; Cx and Dx interfaces based on the Diameter protocol*.

[ETSI TS 129 329] ETSI TS 129 329 (2006), *Digital cellular telecommunication system (Phase 2+); Universal Mobile Telecommunications system (UMTS); Sh interface based on the Diameter protocol; Protocol details*.

[ETSI TS 183 017] ETSI TS 183 017 (2007), *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 283 034] ETSI ES 283 034 v1.5.0 (2008), *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Network Attachment Sub-System (NASS); e4 interface based on the Diameter protocol*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 authentication [ITU-T Y.2014]: A property by which the correct identifier of an entity or party is established with a required assurance. The party being authenticated could be a user, subscriber, home environment or serving network.

3.1.2 authorization [b-ITU-T X.800]: The granting of permission based on authenticated identification.

NOTE – In some contexts, authorization may be granted without requiring authentication or identification, e.g., emergency call services.

3.1.3 customer premises equipment (CPE) [ITU-T Y.2014]: One or more devices allowing a user to access services delivered by NGN.

NOTE – This includes devices under user control commonly referred to as home gateway (HGW) or terminals (TE), etc., but not network-controlled entities such as access gateways.

3.1.4 attribute-value pair (AVP) [ETSI ES 283 034]: Corresponds to an information element in a Diameter message.

NOTE – See [b-IETF RFC 3588] for details.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ABNF	Augmented Backus-Naur Form
AM-PE	Access Management Physical Entity
AVP	Attribute-Value Pair
CPE	Customer Premises Equipment
HGWC-PE	Home Gateway Configuration Physical Entity
IMS	Internet Protocol Multimedia Subsystem
IPSec	Internet Protocol Security
NACE	Network Attachment Control Entity
NACF	Network Attachment Control Function
NAC-PE	Network Access Configuration Physical Entity
NAPT	Network Address and Port Translation
NAS	Network Access Server
NASS	Network Attachment Sub-System
P-CSCF	Proxy Call Session Control Function
PD-PE	Policy Decision Physical Entity
PE-PE	Policy Enforcement Physical Entity
QoS	Quality of Service
RACE	Resource and Admission Control Entity
RACF	Resource and Admission Control Function

RFC	Request For Comments
SCE	Service Control Entity
SCTP	Stream Control Transport Protocol
SDP	Session Description Protocol
SIP	Session Initiation Protocol
TAA-PE	Transport Authentication and Authorization Physical Entity
TLM-PE	Transport Location Management Physical Entity
TRC-PE	Transport Resource Control Physical Entity
TUP-PE	Transport User Profile Physical Entity

5 Ru interface

5.1 Overview

The network attachment control function (NACF) maintains information about IP-connectivity access sessions associated with user equipment connected to the NGN. This information is stored in the transport location management physical entity (TLM-PE) and it is pushed to or pulled from the PD-PE in the RACE when the initial attachment is established or the PD-PE needs the information to make a decision (see Figure 5-1):

5.2 Reference point

This clause describes the Ru reference point.

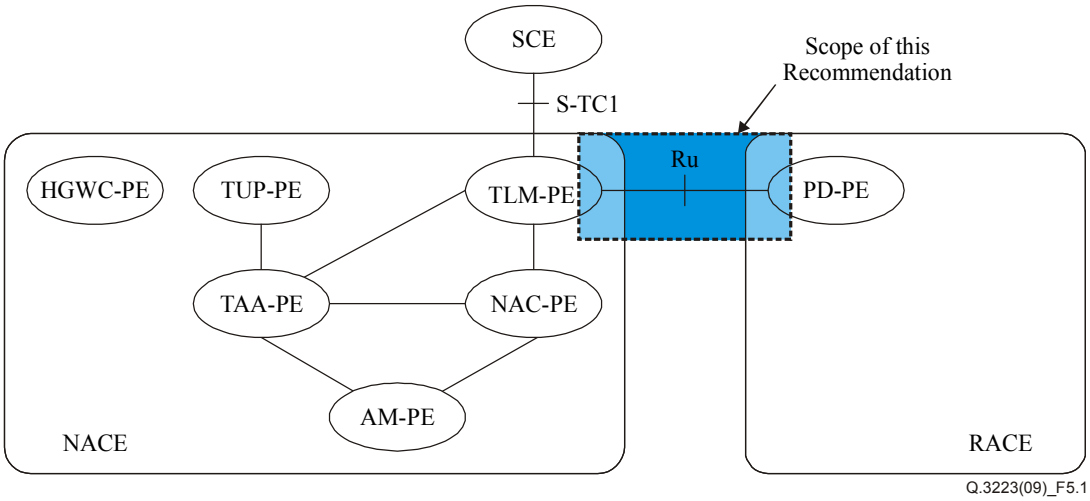

Figure 5-1 – Ru reference point

5.3 Physical entities

Table 5-1 indicates the mapping from the functional entities to the physical entities implementing them.

Table 5-1 – Mapping from functional to physical entities concerned with the Ru reference point

Functional entity	Abbrev.	Physical entity	Abbrev.
Service control functions	SCF	Service control entity (e.g., implementation of P-CSCF)	SCE
Network attachment control functions	NACF	Network attachment control entity	NACE
Resource and admission control functions	RACF	Resource and admission control entity	RACE
Policy decision functional entity	PD-FE	Policy decision physical entity	PD-PE
Transport location management functional entity	TLM-FE	Transport location management physical entity	TLM-PE

5.3.1 Transport location management physical entity (TLM-PE)

The transport location management physical entity (TLM-PE) is a physical entity that implements the functionalities of the transport location management functional entity (TLM-FE) defined in the NACF. The TLM-PE registers the association between the IP address allocated to the terminal and related network location information provided by the NAC-PE, for example, access transport equipment characteristics, line identifier (logical access ID), IP edge identity, etc. The TLM-PE registers the association between network location information received from the NAC-PE and geographical location information. The TLM-PE may also store the identity of a user or a terminal to which the IP address has been allocated (information received from the TAA-PE), as well as the user network QoS profile and user preferences regarding the privacy of location information. In case the TLM-PE does not store the identity/profile of the user/terminal, the TLM-PE shall be able to retrieve this information from the TAA-PE.

The TLM-PE responds to location queries from service control functions and applications. The actual information delivered by the TLM-PE may take various forms (e.g., network location, geographical coordinates, postal address, etc.), depending on agreements with the requestor and on user preferences regarding the privacy of its location. The TLM-PE interfaces with the NAC-PE to establish the association between the IP address, which is allocated by the NAC-FE to the end-user equipment, and the line ID.

The TLM-PE also registers user network profile information (received from the TAA-PE at authentication) to make this profile information available to the RACE during authentication of the terminal. The TLM-PE is able to correlate the information received from NAC-PE and TAA-PE based on the logical access ID.

5.3.2 Policy decision physical entity (PD-PE)

The PD-PE is a physical entity that implements the functionalities of the policy decision functional entity (PD-FE) defined in [ITU-T Y.2111], which coordinates the resource reservation requests received from the SCE. The functionality of the PD-PE is further detailed in clause 7.2.3.2 of [ITU-T Y.2111].

6 Signalling requirements

The Ru reference point should allow information exchange as follows:

– The profile information is pushed by the TLM-PE to the PD-PE.

– The profile information is pulled by the PD-PE from the TLM-PE.

The PD-PE and TLM-PE should use one of two selection mechanisms, either local static configuration or dynamic discovery, based on a globally unique IP address and/or transport subscriber ID to locate the respective communicating entities (i.e., PD-PE → TLM-PE, or TLM-PE → PD-PE).

The following information flows shall be used on the Ru interface:

– Transport resource information.

– Transport resource information indication.

– Transport resource release notification.

Figure 6-1 shows the information flows between the TLM-PE and the PD-PE via the Ru interface.

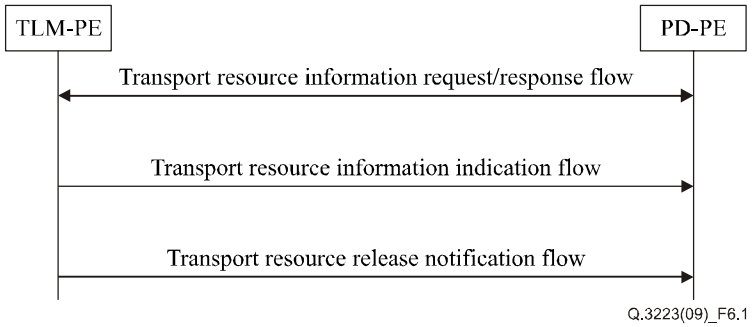

Figure 6-1 – Information flows over Ru interface

6.1 Transport resource information

The information flow of the transport resource information request is sent by the PD-PE to the TLM-PE to request the access transport network profile information. Globally unique IP address information and/or a transport subscriber identifier should be used to discover the NACE and identify the user profile using the static configuration or dynamic discovery approaches. There are two scenarios for this pull mode: one is the failure recovery of the PD-PE, the other is the synchronization of the data in the PD-PE with the user data in the TLM-PE to avoid inconsistency. It contains the following information components (see Table 6-1).

NOTE 1 – In the following tables, each information element is marked as (M) mandatory, (C) conditional or (O) optional.

NOTE 2 – In this Recommendation, '(C)' implies 'Conditional mandatory'. The case of 'conditional option' is not applicable for this Recommendation.

Table 6-1 – Transport resource information request

Information element name	Description
Globally unique IP address information (M)	This information element contains the IP address of the user equipment used by the subscriber and the addressing domain in which the IP address is significant.
Transport subscriber ID (O)	A globally unique identifier for the CPE requesting the transport resource. This identifier can be used for locating the transport subscription information for the CPE.
RACF ID (O)	The identity of the RACF function requesting access profile information.

The transport resource information response information flow is sent by the TLM-PE to the PD-PE to provide the access transport network profile information during either a new resource initiation request from the SCE or the network failure recovery procedure. It contains the following information components (see Table 6-2).

Table 6-2 – Transport resource information response

Information element name	Description
Globally unique IP address information (M)	This information element contains the IP address of the user equipment used by the subscriber and the addressing domain in which the IP address is significant.
Logical access ID (M)	The identity of the logical access to which the user equipment is connected.
Access network type (O)	The type of access network over which network attachment is provided to the user equipment.
Transport subscriber ID (C)	The user who is attached to the network. This element shall be included if available in the TLM-PE.
Physical access ID (O)	The identity of the physical access to which the user equipment is connected.
Default configuration (O)	See Table 6-3.
Transport resource subscription (O)	See Table 6-4.

The default configuration information can be included optionally in the transport resource information response. The involved information elements are shown in Table 6-3.

Table 6-3 – Default configuration information elements

Information element name	Description
Default access control list (O)	The list of destination IP addresses, ports, prefixes and port ranges allowed to cut through by default.
Default maximum uplink bandwidth (O)	The maximum bandwidth that can be used for the upstream connections by default.
Default maximum downlink bandwidth (O)	The maximum bandwidth that can be used for the downstream connections by default.

The transport resource subscription information can be included optionally in the transport resource information response. The involved information elements are shown in Table 6-4.

Table 6-4 – Transport resource subscription information elements

Information element name	Description
Network class of service (O)	The transport class applicable to the QoS profile information.
Subscribed uplink bandwidth (O)	The maximum amount of bandwidth subscribed to by the attached user in the uplink direction for a specific network class of service.
Subscribed downlink bandwidth (O)	The maximum amount of bandwidth subscribed to by the attached user in the downlink direction for a specific network class of service.
Level of priority (O)	The maximum priority allowed for any reservation request.

6.2 Transport resource information indication

The transport resource information indication information flow is sent by the TLM-PE to the PD-PE to push the access transport network profile information when an IP address assigned to a subscriber or the relevant profile is changed after the profile information has been sent to the PD-PE. It contains the following information components (see Table 6-5).

Table 6-5 – Access profile notification information elements

Information element name	Description
Globally unique IP address information (M)	This information element contains the IP address of the user equipment used by the subscriber and the addressing domain in which the IP address is significant.
Logical access ID (M)	The identity of the logical access to which the user equipment is connected.
Access network type (O)	The type of access network over which network attachment is provided to the user equipment.
Transport subscriber ID (C)	The user who is attached to the network. This element shall be included if available in TLM-PE.
Physical access ID (O)	The identity of the physical access to which the user equipment is connected.
Default configuration (O)	See Table 6-3.
Transport resource subscription (O)	See Table 6-4.

6.3 Transport resource release notification

The transport resource release notification information flow is sent by the TLM-PE to notify the PD-PE to remove the resource profile information from the local repository when the assigned IP address is released (e.g., DHCP leased timer expiry or a release of the access transport resources). It contains the following information components (see Table 6-6).

Table 6-6 – Transport resource release notification information elements

Information element name	Description
Globally unique IP address information (M)	This information element contains the IP address of the user equipment used by the subscriber and the addressing domain in which the IP address is significant.
Transport subscriber ID (O)	The user who is attached to the network.

7 Procedure descriptions

The following clauses describe the realization of the functional procedures defined in the NACF [ITU-T Y.2014] and RACF specifications [ITU-T Y.2111] using Diameter commands described in clause 9.

7.1 General

7.1.1 Mapping the information elements

This clause describes a mapping of the information elements defined in the NACF specification onto the Diameter AVPs.

In the tables that describe this mapping, each information element is marked as (M) mandatory or (O) optional:

– A mandatory information element (marked as (M) in the table) shall always be present in the command. If this information element is absent, an application error occurs at the receiver and an answer message shall be sent back to the originator of the request with the Result-Code set to DIAMETER_MISSING_AVP. This message shall also include a Failed-AVP AVP containing the missing information element, i.e., the corresponding Diameter AVP defined by the AVP code and the other fields set as expected for this information element.

– An optional information element (marked as (O) in the table) may be present or absent in the command, at the discretion of the application at the sending entity. Absence or presence of this information element shall not cause an application error and may be ignored by the receiver.

7.1.2 Subscriber profile

Subscriber profile information sent over the Ru interface is structured into two groups: the transport resource subscription information and the default configuration information.

Tables 7-1 and 7-2 detail the involved information elements as defined in the NACF specification [ITU-T Y.2014] and their mapping to Diameter AVPs.

Table 7-1 – Default configuration information

Information element name	Mapping to Diameter AVP	Category
Default access control list	NAS-Filter-Rule	O
Default upstream bandwidth	Maximum-Allowed-Bandwidth-UL	O
Default downstream bandwidth	Maximum-Allowed-Bandwidth-DL	O

Table 7-2 – Transport resource subscription information

Information element name	Mapping to Diameter AVP	Category
Network class of service	Transport-Class	O
Subscribed uplink bandwidth	Maximum-Allowed-Bandwidth-UL	O
Subscribed downlink bandwidth	Maximum-Allowed-Bandwidth-DL	O
Level of priority	Reservation-Priority	O

7.2 Procedures on the Ru interface

7.2.1 Transport resource information exchange

7.2.1.1 Overview

This procedure is used by the RACF to request the transport resource information from the TLM-PE. This procedure is mapped to the commands User-Data-Request/Answer in the Diameter application specified in clause 9. Tables 7-3 and 7-4 detail the involved information elements as defined in the NACF specification [ITU-T Y.2014] and their mapping to Diameter AVPs.

Table 7-3 – Transport resource information request

Information element name	Mapping to Diameter AVP	Category
Globally unique IP address	Globally-Unique-Address	O
Transport subscriber ID	User-Name	O
NOTE – One of these elements shall be present.		

Table 7-4 – Transport resource information response

Information element name	Mapping to Diameter AVP	Category
Globally unique IP address	Globally-Unique-Address	O
Transport subscriber identifier	User-Name	O
Physical connection identifier	Physical-Access-Id	O
Logical connection identifier	Logical-Access-Id	M
Type of access transport network	Access-Network-Type	O
Transport resource subscription	Transport-Resource-Subscription	O

7.2.1.2 Procedure at the RACF side

The RACF may use this procedure upon reception of the resource reservation request associated with an IP-Address for which no record is stored.

The RACF shall populate the transport resource information request as follows:

1) The User-Name AVP or the Globally-Unique-Address AVP shall be included. The Globally-Unique-Address AVP shall be included in configurations where more than one IP address may be assigned per subscriber identifier.

2) If present, the Globally-Unique-Address AVP shall contain a Frame-IP-Address or Frame-IPv6-Prefix AVP value, and an Address-Realm AVP. The Address-Realm AVP shall be included and set either using configuration data (in which case, all terminal equipment served by the RACF belong to the same addressing domain) or from the physical or logical interface over which was received the resource request that triggered the pull procedure.

7.2.1.3 Procedure at the TLM-PE side

Upon reception of the transport resource information request, the TLM-PE shall, in the following order:

1) If the Globally-Unique-Address AVP is present, use this information as a key to retrieve the requested session information.

2) If the Globally-Unique-Address AVP is absent but the User-Name AVP is present, use the latter information as a key to retrieve the requested session information.

3) If both the Globally-Unique-Address AVP and the User-Name AVP are absent, return a transport resource information response with Result-Code set to DIAMETER_MISSING_AVP.

4) If more than one record include the same subscriber identity matching the value of the User-Name AVP and no Globally-Unique-Address AVP is included, return a transport resource information response with Result-Code set to DIAMETER_UNABLE_TO_COMPLY.

5) If no session record is stored for the Globally-Unique-Address AVP or the User-Name AVP, return a transport resource information response with the Experimental-Result-Code AVP be set to DIAMETER_ERROR_USER_UNKNOWN.

If a unique subscriber record can be retrieved, the TLM-PE shall:

1) Check which session data can be returned to the RACF, based on local policy rules and per-subscriber privacy information stored in the TLM-PE.

2) Check whether the session data to be retrieved is currently being updated by another entity. If there is an update of the data in progress, the TLM-PE may delay the response message until the update has been completed and shall include in the response message the updated data requested. The TLM-PE shall ensure that the data returned is not corrupted by this conflict.

If the TLM-PE cannot fulfil the received request for reasons not stated in the above steps, e.g., due to database error, it shall stop processing the request and set Result-Code to DIAMETER_UNABLE_TO_COMPLY or an Experimental-Result-Code AVP set to DIAMETER_USER_DATA_NOT_AVAILABLE.

Otherwise, the requested operation shall take place and the TLM-PE shall return the Result-Code AVP set to DIAMETER_SUCCESS and the session data in the transport resource information response.

7.2.2 Transport resource information indication

7.2.2.1 Overview

This procedure is used to push session-related information from the TLM-PE to the RACF. This information flow occurs when an IP address has been allocated to a subscriber or in case a modification occurs on a profile that has already been pushed to the RACF.

The TLM-PE should push session-related information to the RACF as soon as it is available to the TLM-PE. This may require the TLM-PE to pull part of the information from other components of the NACF.

For the same subscriber, the TLM-PE may push several independent session records with different IP addresses, with or without the same logical access identifier.

This procedure is mapped to the commands Push-Notification-Request/Answer in the Diameter application specified in clause 9. Table 7-5 details the involved information elements as defined in the NACF specification [ITU-T Y.2014] and their mapping to Diameter AVPs.

Table 7-5 – Transport resource information indication

Information element name	Mapping to Diameter AVP	Category
Globally unique IP address	Globally-Unique-Address	O
Transport subscriber identifier	User-Name	O
Physical connection identifier	Physical-Access-Id	O
Logical connection identifier	Logical-Access-Id	M
Type of access transport network	Access-Network-Type	O
Transport resource subscription	Transport-Resource-Subscription	O
Default configuration	Initial-Gate-Setting	O

7.2.2.2 Procedure at the TLM-PE side

The TLM-PE knows the address of the RACF entity to which the information should be pushed, either from configuration data or from the user profile (i.e., received from the TAA-PE/TUP-PE).

The TLM-PE shall populate the transport resource information indication as follows:

– The Globally-Unique-Address AVP shall contain a Frame-IP-Address or Frame-IPv6-Prefix AVP value, and an Address-Realm AVP.

– The Logical-Access-Id AVP shall be present.

The presence of the other AVPs depends on the user profile and local policy rules.

7.2.2.3 Procedure at the RACF side

If the logical access ID is not included or is invalid, the RACF shall return a transport resource information indication with a Result-Code AVP value set to DIAMETER_INVALID_AVP_VALUE.

If the globally unique identifier contained in the Globally-Unique-Address AVP is not known, the RACF shall:

– Create an internal record to store the received information for future use (i.e., for processing resource reservation requests received from the SCE).

– Derive the following information from the logical access ID:

  • The identification and bandwidth capacity of the layer 2 resources over which the subscriber traffic is carried.

  • The address of the physical node(s) implementing the edge node FE and access node FE.

– If the received information contains an Initial-Gate-Setting AVP, perform any appropriate actions to enforce the policy information. This may involve interacting with the policy enforcement physical entity (PE-PE) through the Rw interface (defined in [ITU-T Y.2111]).

If the globally unique identifier contained in the Globally-Unique-Address AVP is already known, the RACF shall:

– Replace the entire content of the internal record with the received information for future use.

– If the received information contains a default configuration, perform any appropriate actions to enforce the new policy information. This may involve interacting with the PE-PE through the Rw interface.

Such an update shall not have any impact on ongoing application sessions for which an authorization has already been provided by the RACF.

If the contents of the request are invalid, the RACF shall return a transport resource information indication response with a Result-Code AVP value set to the appropriate value as described in clause 7.1.

If the creation or modification of the session record is successful but a failure occurs during the processing of the default configuration (e.g., due to a failure in the interaction with the PE-PE), the RACF shall return a transport resource information indication response with a Result-Code AVP value set to DIAMETER_LIMITED_SUCCESS.

If the RACF cannot fulfil the received request for reasons not stated in the above steps, e.g., due to database error, it shall stop processing the request and return a transport resource information indication response with a Result-Code AVP value set to DIAMETER_UNABLE_TO_COMPLY or an Experimental-Result-Code AVP set to DIAMETER_SYSTEM_UNAVAILABLE. In the latter case, the TLM-PE is expected to retry after a provisioned time period.

Otherwise, the requested operation shall take place and the RACF shall return the Result-Code AVP set to DIAMETER_SUCCESS in the transport resource information indication response.

7.2.3 Transport resource release notification

7.2.3.1 Overview

This procedure is used by the TLM-PE to report loss of IP connectivity. This enables the RACF to remove the access profile from its internal database. This event occurs in case the allocated IP address is released (e.g., DHCP leased timer expiry) or due to a release of the underlying layer 2 resources.

This procedure is mapped to the commands Push-Notification-Request/Answer in the Diameter application specified in clause 9. Tables 7-6 and 7-7 detail the involved information elements as defined in the RACF specification [ITU-T Y.2111] and their mapping to Diameter AVPs.

Table 7-6 – Transport resource release notification

Information element name	Mapping to Diameter AVP	Category
Globally unique IP address	Globally-Unique-Address	M
Transport subscriber ID	User-Name	O

Table 7-7 – Transport resource release notification response

Information element name	Mapping to Diameter AVP	Category
Result (see Note)	Result-Code/Experimental-Result	M
NOTE – Result of the request.		

Result-Code AVP shall be used for errors defined in the Diameter base protocol.

Experimental-Result AVP shall be used for other errors. This is a grouped AVP which contains a Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.

7.2.3.2 Procedure at the TLM-PE side

On receipt of an external event indicating that the allocated IP address has been released or the underlying layer 2 connection has been lost, the TLM-PE shall clear all information stored against the IP address and issue a Push-Notification-Request representing a transport resource release notification.

NOTE – Receipt of an indication that a layer 2 connection has been lost may lead the TLM-PE to issue several notifications, in case multiple access sessions where associated with this connection.

7.2.3.3 Procedure at the RACF side

If the globally unique identifier contained in the Globally-Unique-Address AVP is not known, the RACF shall stop processing the request and set the Experimental-Result-Code to DIAMETER_ERROR_USER_UNKNOWN in the transport resource release notification response.

If the globally unique identifier contained in the Globally-Unique-Address AVP is already known, the RACF shall:

– remove the existing session record;

– interact with transfer layer entities (i.e., PE-PE) to remove transport policies associated with the session and clear associated resources;

– notify the SCE.

If the RACF cannot fulfil the received request for reasons not stated in the above steps, e.g., due to database error, it shall stop processing the request and set Result-Code to DIAMETER_UNABLE_TO_COMPLY or an Experimental-Result-Code set to DIAMETER_SYSTEM_UNAVAILABLE. In the latter case, the TLM-PE is expected to retry after a provisioned time period.

Otherwise, the requested operation shall take place and the RACF shall return an IP-Connectivity-Release-Indication response with the Result-Code AVP set to DIAMETER_SUCCESS.

8 Selection and the use of the protocol

The Diameter base protocol [b-IETF RFC 3588] shall be used for the Ru interface with the clarifications listed in the following clauses.

8.1 Security

For secure transport of Diameter messages, Internet Protocol security (IPSec) may be used. Guidelines on the use of SCTP with IPSec can be found in [b-IETF RFC 3554].

8.2 Accounting

This functionality (accounting session state machine, related command codes and AVPs) is not used on the Ru interface.

8.3 Sessions

Diameter sessions are implicitly terminated. An implicitly terminated session is one for which the server does not maintain state information. The client does not need to send any re-authorization or session termination requests to the server.

The Diameter base protocol includes the Auth-Session-State AVP as the mechanism for the implementation of implicitly terminated sessions.

The client (server) shall include in its requests (responses) the Auth-Session-State AVP set to the value NO_STATE_MAINTAINED (1), as described in [b-IETF RFC 3588]. As a consequence, the server does not maintain any state information about this session and the client does not need to send any session termination request. Neither the Authorization-Lifetime AVP nor the Session-Timeout AVP shall be present in requests or responses.

8.4 Transport protocol

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

8.5 Routing considerations

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

Requests initiated by the TLM-PE towards the PD-PE shall include both Destination-Host and Destination-Realm AVPs. The TLM-PE obtains the Destination-Host AVP to use in requests towards a PD-PE from configuration data and/or the subscriber profile. Consequently, the Destination-Host AVP is declared as mandatory in the ABNF for all requests initiated by the TLM-PE.

Requests initiated by the PD-PE towards the TLM-PE shall include both Destination-Host and Destination-Realm AVPs. The PD-PE obtains the Destination-Host AVP to use in requests towards

a TLM-PE, from the configuration data. Consequently, the Destination-Host AVP is declared as mandatory in the ABNF for all requests initiated by the PD-PE.

Destination-Realm AVP is declared as mandatory in the augmented Bachus-Naur form (ABNF) for all requests.

8.6 Application advertisement

The TLM-PE and PD-PE shall advertise support of the Ru-specific application by including the application identifier in the Auth-Application-Id AVP within the Vendor-Specific-Application-Id grouped AVP of the Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands.

The vendor identifier value of ITU-T (11502) shall be included in the Supported-Vendor-Id AVP of the Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands, and in the Vendor-Id AVP within the Vendor-Specific-Application-Id grouped AVP of the Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands. Additionally, support of ETSI AVPs and/or 3GPP AVPs shall be advertised by adding the vendor identifier value of ETSI (13019) and/or 3GPP (10415) to the Supported-Vendor-Id AVP of the Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands.

NOTE – A Vendor-Id AVP included in the Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands that is not included in the Vendor-Specific-Application-Id AVPs as described above indicates the manufacturer of the Diameter node as per [b-IETF RFC 3588].

9 Ru protocol specification

This clause specifies a Diameter application that allows a Diameter server and a Diameter client to exchange information related to IP-connectivity sessions. The Diameter application identifier assigned to this application is 16777262.

The Diameter base protocol as specified in [b-IETF RFC 3588] is used to support information transfer on both interfaces.

[b-IETF RFC 3588] shall apply except as modified by the defined support of the methods and the defined support of the commands and AVPs, result and event codes specified in this clause. Unless otherwise specified, the procedures (including error handling and unrecognized information handling) are unmodified.

9.1 Commands

This Recommendation re-uses and modifies commands defined in the Sh application [ETSI TS 129 329] for the Sh interface. Existing Diameter command codes from the Sh application are used. Only the following commands defined in the Sh application are used. Any other command defined in the Sh application shall be ignored.

Table 9-1 – Command-code values

Command	Abbreviation	Defining reference	Command code
User-Data-Request	UDR	[ETSI TS 129 329]	306
User-Data-Answer	UDA	[ETSI TS 129 329]	306
Push-Notification-Request	PNR	[ETSI TS 129 329]	309
Push-Notification-Answer	PNA	[ETSI TS 129 329]	309

AVPs defined in the Sh application and not used in this Recommendation are not shown in the following clauses. When received, these AVPs shall be ignored by the TLM-PE and the PD-PE.

Table 9-2 defines the mapping between the information flows defined in clause 7.2 and Diameter commands.

Table 9-2 – Ru message mapping to Diameter command

Ru message	Source	Destination	Command name	Command code
Transport resource information request	PD-PE	TLM-PE	User-Data-Request	306
Transport resource information response	TLM-PE	PD-PE	User-Data-Answer	306
Transport resource information indication	TLM-PE	PD-PE	Push-Notification-Request	309
Transport resource information indication response	PD-PE	TLM-PE	Push-Notifications-Answer	309
Transport resource release notification	TLM-PE	PD-PE	Push-Notification-Request	309
Transport resource release notification response	PD-PE	TLM-PE	Push-Notifications-Answer	309

9.1.1 User-Data-Request (UDR) command

The User-Data-Request (UDR) command, indicated by the Command-Code field set to 306 and the "R" bit set in the command flags field, is sent by a Diameter client to a Diameter server in order to request user data. This command is defined in the Sh application and used with additional AVPs defined in the NASS e4 interface [ETSI ES 283 034].

Message format:

```
< User-Data-Request > ::= < Diameter Header: 306, REQ, PXY, 16777262 >
                         < Session-Id >
                         { Vendor-Specific-Application-Id }
                         { Auth-Session-State }
                         { Origin-Host }
                         { Origin-Realm }
                         [ Destination-Host ]
                         { Destination-Realm }
                         [Globally-Unique-Address]
                         [User-Name]
                         *[ AVP ]
                         *[ Proxy-Info ]
                         *[ Route-Record ]
```

9.1.2 User-Data-Answer (UDA) command

The User-Data-Answer (UDA) command, indicated by the Command-Code field set to 306 and the "R" bit cleared in the command flags field, is sent by a server in response to the User-Data-Request command. This command is defined in the Sh application and used with additional AVPs defined in the NASS e4 interface. The Experimental-Result AVP may contain one of the values defined in clause 9.2 or in the Cx and Dx application [ETSI TS 129 229].

Message format:

```
< User-Data-Answer > ::= < Diameter Header: 306, PXY, 16777262 >
                        < Session-Id >
                        { Vendor-Specific-Application-Id }
                        [ Result-Code ]
                        [ Experimental-Result ]
                        { Auth-Session-State }
                        { Origin-Host }
```

```
                        { Origin-Realm }
                        [Globally-Unique-Address]
                        [User-Name]
                        [Logical-Access-Id]
                        [Physical-Access-Id]
                        [Access-Network-Type]
                        [Initial-Gate-Setting]
                        *[QoS-Profile]
                        *[ AVP ]
                        *[ Failed-AVP ]
                        *[ Proxy-Info ]
                        *[ Route-Record ]
```

9.1.3 Push-Notification-Request (PNR) command

The Push-Notification-Request (PNR) command, indicated by the Command-Code field set to 309 and the "R" bit set in the command flags field, is sent by a Diameter server to a Diameter client in order to notify changes in the user data in the server. This command is defined in the Sh application and used with additional AVPs defined in the NASS e4 interface.

Message format:

```
< Push-Notification-Request > ::= < Diameter Header: 309, REQ, PXY, 16777262 >
                        < Session-Id >
                        { Vendor-Specific-Application-Id }
                        { Auth-Session-State }
                        { Origin-Host }
                        { Origin-Realm }
                        { Destination-Host }
                        { Destination-Realm }
                        [Globally-Unique-Address]
                        [User-Name]
                        [Logical-Access-Id]
                        [Physical-Access-Id]
                        [Access-Network-Type]
                        [Initial-Gate-Setting]
                        *[QoS-Profile]
                        *[ AVP ]
                        *[ Proxy-Info ]
                        *[ Route-Record ]
```

9.1.4 Push-Notification-Answer (PNA) command

The Push-Notification-Answer (PNA) command, indicated by the Command-Code field set to 309 and the "R" bit cleared in the command flags field, is sent by a client in response to the Push-Notification-Request command. This command is defined in the Sh application. The Experimental-Result AVP may contain one of the values defined in clause 9.2 or in the Cx and Dx application [ETSI TS 129 229].

Message format:

```
< Push-Notification-Answer > ::= < Diameter Header: 309, PXY, 16777262 >
                        < Session-Id >
                        { Vendor-Specific-Application-Id }
                        [ Result-Code ]
                        [ Experimental-Result ]
                        { Auth-Session-State }
                        { Origin-Host }
                        { Origin-Realm }
                        *[ AVP ]
                        *[ Failed-AVP ]
                        *[ Proxy-Info ]
                        *[ Route-Record ]
```

9.2 Result-Code AVP values

This clause defines new result code values that must be supported by all Diameter implementations that conform to this Recommendation. When one of the result codes defined here is included in a response, it shall be inside an Experimental-Result AVP and Result-Code AVP shall be absent.

9.2.1 Success

Result codes that fall within the success category are used to inform a peer that a request has been successfully completed. No result codes within this category have been defined so far.

9.2.2 Permanent failures

Errors that fall within the permanent failures category are used to inform the peer that the request failed, and should not be attempted again.

No errors within this category have been defined so far. However, the following error defined in the Cx and Dx application is used in this Recommendation:

– DIAMETER_ERROR_USER_UNKNOWN (5001).

When this result code is used, the 3GPP vendor ID shall be included in the vendor-Id AVP of the Experimental-Result AVP.

9.2.3 Transient failures

Errors that fall within the transient failures category are those used to inform a peer that the request could not be satisfied at the time that it was received. The request may be able to be satisfied in the future.

This Recommendation defines the following error with this category:

– DIAMETER_SYSTEM_UNAVAILABLE (4001).

This error is returned when a request could not be satisfied at the time that it was received due to a temporary internal failure or congestion. When this result code is used, the ETSI vendor ID shall be included in the Vendor-Id AVP of the Experimental-Result AVP.

The following error defined in the Sh application is also used in this Recommendation:

– DIAMETER_USER_DATA_NOT_AVAILABLE (4100)

When this result code is used, the 3GPP vendor ID shall be included in the Vendor-Id AVP of the Experimental-Result AVP.

9.3 AVPs

The following tables summarize the AVPs used in this Recommendation beyond those defined in the Diameter base protocol.

Table 9-3 describes the Diameter AVPs defined in this Recommendation, their AVP code values, types, possible flag values and whether the AVP may or not be encrypted. The Vendor-Id header of all AVPs defined in this Recommendation shall be set to ETSI (13019).

NOTE – In the following tables, AVP header bit denoted as "M" indicates that support of the AVP is mandatory. AVP header bit denoted as "V" indicates that the optional Vendor-ID field is present in the AVP header.

Table 9-3 – Diameter AVPs imported from the NASS e4 interface

				AVP flag rules				
Attribute name	**AVP code**	**Reference**	**Value type**	**Must**	**May**	**Should not**	**Must not**	**May encrypt**
Globally-Unique-Address	300	[ETSI ES 283 034]	Grouped	M, V				Yes
Address-Realm	301	[ETSI ES 283 034]	OctetString	M, V				Yes
Logical-Access-Id	302	[ETSI ES 283 034]	OctetString	V	M			Yes
Initial-Gate-Setting	303	[ETSI ES 283 034]	Grouped	V	M			Yes
QoS-Profile	304	[ETSI ES 283 034]	Grouped	V	M			Yes
IP-Connectivity-Status	305	[ETSI ES 283 034]	Enumerated	V	M			Yes
Access-Network-Type	306	[ETSI ES 283 034]	Grouped	V	M			Yes
Aggregation-Network-Type	307	[ETSI ES 283 034]	Enumerated	V	M			Yes
Maximum-Allowed-Bandwidth-UL	308	[ETSI ES 283 034]	Unsigned32	V	M			Yes
Maximum-Allowed-Bandwidth-DL	309	[ETSI ES 283 034]	Unsigned32	V	M			Yes
Transport-Class	311	[ETSI ES 283 034]	Unsigned32	V	M			Yes
Application-Class-ID	312	[ETSI ES 283 034]	UTF8String	V	M			Yes
Physical-Access-ID	313	[ETSI ES 283 034]	UTF8String	V	M			Yes

Table 9-4 describes the Diameter AVPs defined for the NAS application [b-IETF RFC 4005] and used in this Recommendation, their AVP code values, types, possible flag values and whether the AVP may or not be encrypted. Flag values are described in the context of this Recommendation rather than in the context of the application where they are defined. AVPs defined in [b-IETF RFC 4005] but not listed in Table 9-4 should not be sent by Diameter conforming to this Recommendation and shall be ignored by receiving entities. No Vendor-Id shall be included in the AVP header.

Table 9-4 – Diameter AVPs imported from the NAS application

				AVP flag rules				
Attribute name	**AVP code**	**Reference**	**Value type**	**Must**	**May**	**Should not**	**Must not**	**May encrypt**
NAS-Port-Type	61	[IETF RFC 4005]	Enumerated		M		V	Yes
NAS-Filter-Rule	400	[IETF RFC 4005]	IPFilterRule		M		V	Yes
Framed-IP-Address	8	[IETF RFC 4005]	OctetString		M		V	Yes
Framed-IPv6-Prefix	97	[IETF RFC 4005]	OctetString		M		V	Yes

Table 9-5 describes the Diameter AVPs defined for the Gq' application [ETSI TS 183 017] and used in this Recommendation, their AVP code values, types, possible flag values and whether the AVP may or not be encrypted. Flag values are described in the context of this Recommendation rather than in the context of the application where they are defined. AVPs defined in [ETSI TS 183 017] but not listed in Table 9-5 should not be sent by Diameter conforming to this Recommendation and shall be ignored by receiving entities. The Vendor-Id header for these AVPs shall be set to ETSI (13019).

Table 9-5 – Diameter AVPs imported from the Gq' specification

				AVP flag rules				
Attribute name	**AVP code**	**Reference**	**Value type**	**Must**	**May**	**Should not**	**Must not**	**May encrypt**
Reservation-Priority	458	[ETSI TS 183 017]	Unsigned32	V			M	Yes

9.3.1 Globally-Unique-Address AVP

The Globally-Unique-Address AVP is defined in the NASS e4 interface, specified in [ETSI ES 283 034].

9.3.2 Address-Realm AVP

The Address-Realm AVP is defined in the NASS e4 interface, specified in [ETSI ES 283 034].

9.3.3 Logical-Access-Id AVP

The Logical-Access-Id AVP is defined in the NASS e4 interface, specified in [ETSI ES 283 034].

9.3.4 Initial-Gate-Setting AVP

The Initial-Gate-Setting AVP is defined in the NASS e4 interface, specified in [ETSI ES 283 034].

9.3.5 QoS-Profile AVP

The QoS-Profile AVP is defined in the NASS e4 interface, specified in [ETSI ES 283 034].

9.3.6 IP-Connectivity-Status AVP

The IP-Connectivity-Status AVP is defined in the NASS e4 interface, specified in [ETSI ES 283 034].

9.3.7 Access-Network-Type AVP

The Access-Network-Type AVP is defined in the NASS e4 interface, specified in [ETSI ES 283 034].

9.3.8 Aggregation-Network-Type AVP

The Aggregation-Network-Type AVP is defined in the NASS e4 interface, specified in [ETSI ES 283 034].

9.3.9 Maximum-Allowed-Bandwidth-UL AVP

The Maximum-Allowed-Bandwidth-UL AVP is defined in the NASS e4 interface, specified in [ETSI ES 283 034].

9.3.10 Maximum-Allowed-Bandwidth-DL AVP

The Maximum-Allowed-Bandwidth-DL AVP is defined in the NASS e4 interface, specified in [ETSI ES 283 034].

9.3.11 Transport-Class AVP

The Transport-Class AVP is defined in the NASS e4 interface, specified in [ETSI ES 283 034].

9.3.12 Application-Class-ID AVP

The Application-Class-ID AVP is defined in the NASS e4 interface, specified in [ETSI ES 283 034].

9.3.13 Physical-Access-ID AVP

The Physical-Access-ID AVP is defined in the NASS e4 interface, specified in [ETSI ES 283 034].

9.3.14 NAS-Port-Type AVP

The NAS-Port-Type AVP is defined in the NAS application, specified in [b-IETF RFC 4005].

9.3.15 NAS-Filter-Rule AVP

The NAS-Filter-Rule AVP is defined in the NAS application, specified in [b-IETF RFC 4005].

9.3.16 Framed-IP-Address AVP

The Framed-IP-Address AVP is defined in the NAS application, specified in [b-IETF RFC 4005].

9.3.17 Framed-IPv6-Prefix AVP

The Framed-IPv6-Prefix AVP is defined in the NAS application, specified in [b-IETF RFC 4005].

9.3.18 Reservation-Priority AVP

The Reservation-Priority AVP is defined in the 3GPP Gq' interface, specified in [ETSI TS 183 017].

9.4 Use of namespaces

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

9.4.1 AVP codes

This Recommendation uses AVP values from the AVP code namespace managed by ETSI for its Diameter vendor-specific applications. See clause 9.3, Tables 9-3 to 9-5.

9.4.2 Experimental-Result-Code AVP values

This Recommendation uses the Experimental-Result-Code AVP values from the AVP Code namespace managed by ETSI for its Diameter vendor-specific applications.

9.4.3 Command code values

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

9.4.4 Application-ID value

This Recommendation defines the Ru Diameter application with application ID 16777262. The vendor identifier assigned by IANA to ITU-T (http://www.iana.org/assignments/enterprise-numbers) is 11502.

10 Security considerations

The security requirements within the functional requirements and architecture of the NACF are addressed by the security requirements for NGN [ITU-T Y.2701]. The Ru interface shall follow the security requirements of the NACF.

Clause 8.1 recommends the use of IPSec to ensure secure transport of Diameter messages. Guidelines on the use of SCTP with IPSec can be found in [b-IETF RFC 3554].

Further security considerations are provided in the security considerations section of [b-IETF RFC 3588], which operators are advised to consult.

Bibliography

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

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

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

[b-IETF RFC 3554] IETF RFC 3554 (2003), *On the Use of Stream Control Transmission Protocol (SCTP) with IPSec*.

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

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

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