International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.3231

(08/2016)

SERIES Q: SWITCHING AND SIGNALLING

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

Signalling requirements and protocol at the Ne interface between the transport location management physical entity and the network access configuration physical entity

Recommendation ITU-T Q.3231

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.3709
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.3616
Service and session control protocols – supplementary services based on SIP-IMS	Q.3617–Q.3639
NGN applications	Q.3700–Q.3709
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR SDN	Q.3710–Q.3899
TESTING SPECIFICATIONS	Q.3900–Q.4099

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

Recommendation ITU-T Q.3231

Signalling requirements and protocol at the Ne interface between the transport location management physical entity and the network access configuration physical entity

Summary

Recommendation ITU-T Q.3231 provides the protocol for the interface between the transport location management physical entity (TLM-PE) and the network access configuration physical entity (NAC-PE) of the network attachment control entity (NACE). The Ne reference point allows the network access configuration physical entity to register in the transport location management physical entity the binding between an allocated IP address and a customer premises equipment (CPE) as well as other transport related information such as logical/physical port addresses.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Q.3231	2016-08-29	11	11.1002/1000/12986

Keywords

Customer premises equipment, CPE, NACE, NAC-PE, Ne interface, network access configuration physical entity, TLM-PE, transport location management physical entity.

---

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

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/.

Table of Contents

		Page
1	Scope	1
2	References	1
3	Definitions	2
	3.1 Terms defined elsewhere	2
	3.2 Terms defined in this Recommendation	2
4	Abbreviations and acronyms	2
5	Conventions	4
6	Ne interface	4
	6.1 Overview	4
	6.2 Ne Reference model	4
	6.3 Physical entities and capabilities	4
7	Signalling requirements	5
	7.1 Bind indication	6
	7.2 Bind acknowledgement	6
	7.3 Unbind indication	7
	7.4 Bind information query	7
	7.5 Bind information query acknowledgement	7
	7.6 Mobility service parameters indication	8
8	Description of procedures	9
	8.1 General	9
	8.2 Procedure on the Ne interface	9
9	Use of Diameter-based protocol	14
	9.1 Securing Diameter messages	14
	9.2 Accounting functionality	14
	9.3 Use of sessions	14
	9.4 Transport protocol	14
	9.5 Routing considerations	14
	9.6 Advertising application support	15
10	Message specification	15
	10.1 Commands	15
	10.2 Experimental-Result-Code AVP values	18
	10.3 Attribute value pairs (AVPs)	18
	10.4 Use of namespaces	21
11	Security considerations	21
Bibliography		23

Recommendation ITU-T Q.3231

Signalling requirements and protocol at the Ne interface between the transport location management physical entity and the network access configuration physical entity

1 Scope

This Recommendation specifies the protocol for the Ne interface [ITU-T Y.2014] between the transport location management physical entity (TLM-PE) and the network access configuration physical entity (NAC-PE).

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.1910] Recommendation ITU-T Y.1910 (2008), *IPTV functional architecture*.

[ITU-T Y.2014] Recommendation ITU-T Y.2014 (2010), *Network attachment control functions in next generation networks*.

[ITU-T Y.2021] Recommendation ITU-T Y.2021 (2006), *IMS for Next Generation Networks*.

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

[ITU-T Y.3232] Recommendation ITU-T Y.3232 (2014), *Signalling requirements and protocol at the Nc interface between the transport location management physical entity and the transport authentication and authorization physical entity*.

[ETSI ES 283 034] ETSI ES 283 034 V2.2.0 (2008), *Telecommunications and Internet converged Services and Protocols for Advanced Networks (TISPAN); Network Attachment Sub-System (NASS); e4 interface based on the DIAMETER protocol*.

[ETSI ES 283 035] ETSI ES 283 035 V3.1.1 (2015), *Network Technologies (NTECH); Network Attachment; e2 interface based on the DIAMETER protocol.*

[ETSI TS 129 229] ETSI TS 129 229 V13.0.0 (2016), *Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Cx and Dx interfaces based on the Diameter protocol; Protocol details (3GPP TS 29.229 version 13.0.0 Release 13).*

[ETSI TS 129 329] ETSI TS 129 329 V12.6.0 (2016), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Sh interface based on the Diameter protocol; Protocol details (3GPP TS 29.329 version 12.6.0 Release 12).*

[ETSI TS 183 059-1] ETSI TS 183 059-1 V2.1.1 (2009), *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Network Attachment Sub-System (NASS); a2 interface based on the DIAMETER protocol.*

[IETF RFC 4960] IETF RFC 4960 (2007), *Stream Control Transmission Protocol*.

[IETF RFC 5580] IETF RFC 5580 (2009), *Carrying Location Objects in RADIUS and Diameter*.

[IETF RFC 6733] IETF RFC 6733 (2012), *Diameter Base 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 location information [b-ITU-T Q.1001]: The location register should as a minimum contain the following information about a mobile station:

– international mobile station identity;

– actual location of the mobile station (e.g., PLMN, MSC area, location area, as required).

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ABNF Augmented Backus-Naur Form

AM-PE Access Management Physical Entity

AR-PE Access Relay Physical Entity

ATM Asynchronous Transfer Mode

AVP Attribute-Value Pair

CPE Customer Premises Equipment

DHCP Dynamic Host Configuration Protocol

DNS Domain Name Service

FQDN Fully Qualified Domain Name

GTP GPRS Tunnelling Protocol

HDC-PE Handover Decision and Control Physical Entity

HGW Home Gateway

HGWC-PE Home Gateway Configuration Physical Entity

ID Identifier

IMS IP multimedia Subsystem

IP	Internet Protocol
IPsec	IP security protocol
IPTV	Internet Protocol Television
MIP	Mobile IP
MLM-PE	Mobile Location Management Physical Entity
MMCE	Mobility Management Control Entity
MPLS	Multi-Protocol Label Switching
MSC	Mobile Switching Center
NACE	Network Attachment Control Entity
NACF	Network Attachment Control Functions
NAC-PE	Network Access Configuration Physical Entity
NID-PE	Network Information Distribution Physical Entity
NIR-PE	Network Information Repository Physical Entity
P-CSC-PE	Proxy Call Session Control Physical Entity
PD-PE	Policy Decision Physical Entity
PIA	Persistent IP address
PLMN	Public Land Mobile Network
PPP	Point-to-Point Protocol
RACE	Resource Admission and Control Entity
SADS	Service and Application Discovery and Selection
SCE	Service Control Entity
SCTP	Stream Control Transmission Protocol
TAA-PE	Transport Authentication and Authorization Physical Entity
TE	Terminal Equipment
TFTP	Trivial File Transfer Protocol
TIA	Temporary IP address
TLM-PE	Transport Location Management Physical Entity
TRC-PE	Transport Resource Control Physical Entity
TUP-PE	Transport User Profile Physical Entity
UE	User Equipment
VC	Virtual Channel
VCI	Virtual Channel Identifier
VP	Virtual Path
VPI	Virtual Path Identifier
VPN	Virtual Private Network

5 Conventions

None.

6 Ne interface

6.1 Overview

The Ne reference point allows the NAC-PE to register in the TLM-PE the binding between an allocated IP address and a CPE as well as other transport related information, such as logical/physical port addresses.

The following information flows are used on the TLM-PE to NAC-PE reference point:

– Bind indication;
– Bind acknowledgement;
– Unbind indication;
– Bind information query;
– Bind information query acknowledgement;
– Mobility service parameters indication.

6.2 Ne Reference model

This clause describes the reference architecture. As the initial architecture, Figure 6-1 can be used:

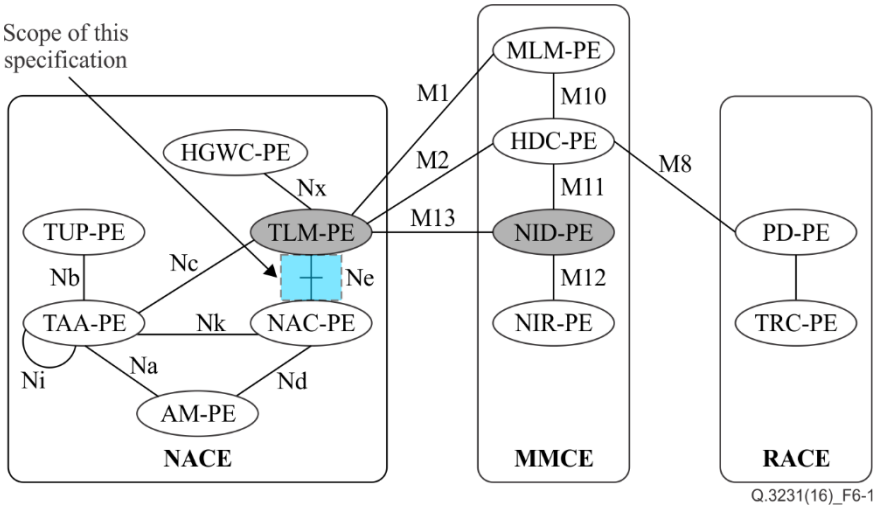

Figure 6-1 – Ne reference model [ITU-T Y.2014]

6.3 Physical entities and capabilities

6.3.1 Transport location management physical entity (TLM-PE)

TLM-PE responds to location queries from service control functions and applications. The actual information delivered by TLM-PE may take various forms (network location, geographical coordinates, postal address, etc.) depending on the agreement with the requester and on user preferences regarding the privacy of its location.

The TLM-PE may play several roles, i.e. the Home role, the Local role, or both. In its Home role the TLM-PE stores a pointer to the TLM-PE instance that is playing the Local role for the attachment. The current location information of the user/CPE in the access domain is stored and bound in the Local TLM-PE. So when the user/CPE moves in the same access domain, only the location binding

information of the Local TLM-PE needs to be updated; the location binding information of the Home TLM-PE does not need to be updated.

The Local TLM-PE is in the access network to which the terminal equipment is attached. The Home TLM-PE is in the network designated by the Transport User Profile Physical Entity. Where these networks differ, communication between the Local and Home TLM-PE instances takes place over the Ng reference point. Namely, the home TLM-PE may provide the SCE with user network profile information through the local TLM-PE of visit network to support mobility when the user is nomadic.

Similarly, the home TLM-PE is able to provide the SCE with user network profile information through the local TLM-PE of another service provider for roaming on such access network.

The functionality of the TLM-PE is further detailed in clause 7.2.3 of [ITU-T Y.2014].

6.3.2 Network access configuration physical entity (NAC-PE)

The NAC-PE is responsible for the IP address allocation to the CPE. It may also distribute other network configuration parameters such as address of DNS server(s), address of signalling proxies for specific service stratum components.

The NAC-PE should be able to provide the CPE access network information. This information uniquely identifies the access network to which the CPE is attached. The CPE may send this information to SCEs as a hint to locate the TLM-PE.

The NAC-PE may be able to allocate two kinds of IP addresses, persistent IP address (PIA) and temporary IP address (TIA), to the TE in order to support mobility. A persistent IP address is not changed during the movement of TE, after it has once been allocated to TE. However, it is noted that a different persistent IP address can be allocated to the same TE in certain cases, for example, when the TE is rebooted. The home address of MIP is an example of the persistent IP address. On the other hand, a different temporary IP address is allocated to a TE whenever the TE moves into a new subnet. The care-of address of MIP is an example of the temporary IP address. The NAC-PE may allocate IP addresses with associated TAA-PE, if an address needs to be allocated during the process of authentication.

The functionality of the TLM-PE is further detailed in clause 7.2.1 of [ITU-T Y.2014].

7 Signalling requirements

The Ne reference point allows the NAC-PE to register in the TLM-PE the binding between an allocated IP address and a CPE as well as other transport related information, such as logical/physical port addresses.

The following information flows are used on the TLM-PE to NAC-PE reference point:

– Bind indication;
– Bind acknowledgement;
– Unbind indication;
– Bind information query;
– Bind information query acknowledgement;
– Mobility service parameters indication.

For additional information, refer to clause 8.1.2 of [ITU-T Y.2014].

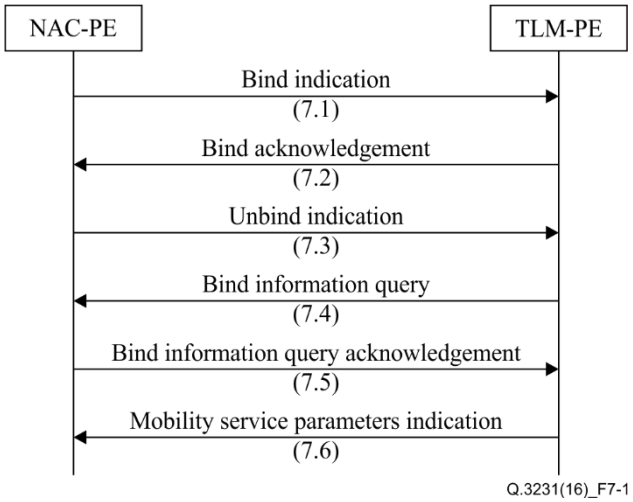

Figure 7-1 – Information flow

7.1 Bind indication

Table 7-1 describes the elements contained in the bind indication information flow.

Table 7-1 – Bind indication (NAC-PE → TLM-PE)

Globally Unique IP Address Information	A set of IP address information used for locating the access network to which the CPE is attached.
– Unique IP Address	The IP address allocated to the attached CPE.
– Address Realm	The addressing domain in which the IP address is significant.
Physical Connection Identifier (optional)	A local identifier for physical connection of the access transport network to which the CPE is attached (e.g., IP address of PE-PE device, and MAC address or link ID and physical port ID).
Logical Connection Identifier (Note 1)	A local identifier for logical connection of the access transport network to which the CPE is connected (e.g., ATM VPI/VCI, PPP, MPLS label, GTP tunnel or logical port).
CPE Type (optional) (Note 2)	The type of CPE.
NOTE 1 – If the NAC-PE is implemented as a DHCP server, this parameter is mapped to the DHCP option 82, sub-options 1 and 2 [b-IETF RFC 2131]. NOTE 2 – If the NAC-PE is implemented as a DHCP server, this parameter is mapped to the DHCP option 77 [b-IETF RFC 2131].	

7.2 Bind acknowledgement

The bind acknowledgement information flow conveys information that may be sent back to the CPE. The information returned by the TLM-PE in response to a bind indication is received from the TAA-PE or retrieved by the TLM-PE from the TUP-PE, via the TAA-PE.

Table 7-2 describes the elements contained in the bind acknowledgement information flow.

Table 7-2 – Bind acknowledgement (TLM-PE → NAC-PE)

HGWC-PE address (optional)	The address of the HGWC-PE entity from which configuration data may be retrieved by the CPE.
Geographic Location Information (optional)	Geographic location information.
P-CSC-PE Identity (optional)	The identifier of the P-CSC-PE for accessing IMS services [ITU-T Y.2021].
SADS Identity (optional)	The identifier of the SADS for accessing IPTV services [ITU-T Y.1910].

7.3 Unbind indication

The unbind indication information flow is sent by the NAC-PE on expiry of the binding between an IP address and a CPE or when an underlying PPP connection or layer 2 connection is released.

Table 7-3 describes the elements contained in the unbind indication information flow.

Table 7-3 – Unbind indication (NAC-PE → TLM-PE)

Globally Unique IP Address Information	A set of IP address information used for locating the access network to which the CPE is attached.
– Unique IP Address	The IP address for identifying the attached CPE.
– Address Realm	The addressing domain of the IP address (e.g., Subnet prefix or VPN ID).

7.4 Bind information query

The bind information query information flow is used by the TLM-PE to request bind information (e.g., in the context of recovery procedures) from the NAC-PE.

Table 7-4 describes the elements contained in the bind information query information flow.

Table 7-4 – Bind information query (TLM-PE → NAC-PE)

Globally Unique IP Address information	A set of IP address information used for locating the access network to which the CPE is attached.
– Unique IP Address	The IP address for identifying the attached CPE.
– Address Realm	The addressing domain of the IP address (e.g., Subnet prefix or VPN ID).

7.5 Bind information query acknowledgement

The bind information query acknowledgement information flow is used by NAC-PE to inform the TLM-PE of the result of a bind information query request. When the information query is successful, the acknowledgement information flow contains the information described in Table 7-5.

Table 7-5 – Bind information query acknowledgement (NAC-PE → TLM-PE)

Physical Connection Identifier (optional)	A local identifier for physical connection of the access transport network to which the CPE is attached to (e.g., IP address of PE-PE device, and MAC address or link ID and physical port ID).
Logical Connection Identifier (Note 1)	A local identifier for logical connection of the access transport network to which the CPE is connected (e.g., ATM VPI/VCI, PPP, MPLS Label, GTP tunnel or logical port).
CPE Type (optional) (Note 2)	The type of CPE.
NOTE 1 – If the NAC-PE is implemented as a DHCP server, this parameter is mapped to the DHCP option 82, sub-options 1 and 2 [b-IETF RFC 2131]. NOTE 2 – If the NAC-PE is implemented as a DHCP server, this parameter is mapped to the DHCP option 77 [b-IETF RFC 2131].	

7.6 Mobility service parameters indication

The mobility service parameters indication information flow is used to push mobility service information from the TLM-PE to the NAC-PE, upon successful authentication of the user.

Table 7-6 describes the elements contained in the mobility service parameters indication information flow.

Table 7-6 – Mobility service parameters indication (TLM-PE → NAC-PE)

Transport Subscriber Identifier	A globally unique identifier of the attached CPE. This identifier can be used for locating the transport subscription information for the CPE.
Globally Unique IP Address Information (Note 1)	A set of IP address information used for locating the access network in which the CPE is attached.
– Unique IP Address	The IP address for identifying the attached CPE.
– Address Realm	The addressing domain of the IP address (e.g., Subnet prefix or VPN ID).
Mobility Service Parameters (optional) (Note 2)	
– Address of MLM-PE(C) (Note 3)	The address of the instance of the MLM-PE containing the mobile address binding information.
– Address of MLM-PE(P) (Note 3)	The address of the MLM-PE instance which sends the location registration.
– Keying Material (Note 3)	The material used for the security association between the UE and MMCE.
– Mobility Protocol Type	The type of mobility protocol that TE or CPE could support, for example host-based or network-based mobility.
– Anchor point address (optional)	The upper tunnel end point address, from the point of view of the UE.
– Tunnel end point address (optional) (Note 4)	The tunnel end point address for the network node which works as UE's proxy (lower tunnel end point).
NOTE 1 – The globally unique IP address information is included if it is retrieved by the TAA-PE. It is identical to the persistent IP address from the viewpoint of MMCE. NOTE 2 – It is available only if the mobility service is applied. NOTE 3 – It is available only if the host-based mobility is applied. NOTE 4 – If the tunnel end point address is statically provisioned or the MLM-PE can obtain it with its own mechanisms, this information is not required. It is available only if the network-based mobility is applied.	

8 Description of procedures

8.1 General

The following clauses describe the realization of the functional procedures defined in the NACE specifications using Diameter commands described in clause 10. This involves describing a mapping between the Information Elements defined in the NACE specification and Diameter AVPs.

In the tables that describe this mapping, each Information Element is marked as (M) mandatory, (C) conditional or (O) optional. [ETSI ES 283 035].

8.2 Procedure on the Ne interface

8.2.1 Bind indication

8.2.1.1 Overview

This procedure is used to report the binding between the IP address allocated to a user equipment and identity of the access to which this equipment is connected from the NAC-PE to the TLM-PE. This information flow occurs when an IP address has been allocated to a user equipment.

The NAC-PE should trigger this procedure as soon as an IP address has been allocated.

This procedure is mapped to the commands Push-Notification-Request/Answer in the Diameter application specified in clause 10. Tables 8-1 and 8-2 detail the relevant information elements as defined in the NACE and their mapping to Diameter AVPs.

Table 8-1 – Bind indication

Information element name	Mapping to Diameter AVP	Category
Unique IP Address	Globally-Unique-Address	M
Address Realm		
Physical Connection Identifier (optional)	Physical-Access-Id	O
Logical Connection Identifier	Logical-Access-Id	M
CPE Type(optional)	Terminal-Type	O

Table 8-2 – Bind acknowledgement

Information Element name	Mapping to Diameter AVP	Category
Result	Result-Code /Experimental_Result	M
HGWC-PE address(optional)	CNGCF-Address	O
Geographic Location Information (optional)	Location-Data	O
P-CSCF Identity (optional)	SIP-Outbound-Proxy	O
SADS Identity (optional)	SADS-Id	O

8.2.1.2 Procedure at the NAC-PE side

After allocating the IP address to a user equipment, or when a Renew is received from a different access line, the NACE shall send a Bind Indication with the following information to TLM-PE:

– 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.

– Physical Access ID and Terminal Type may be present if available.

If the NACE is implemented as a DHCP v4 server, the Logical-Access-Id AVP shall be derived from the value of the DHCP option 82, sub-option 1 and 2 received from the AR-PE. The Physical-Access-ID may also be derived from the value of these sub-options. If the NACE is implemented as a DHCP v4 server, the Terminal-Type AVP shall be set from the value of the DHCP option 77 received from the user equipment. On receipt of a Bind Acknowledgement with a Result-Code AVP indicating DIAMETER_SUCCESS, the NACE shall process the received AVPs as follows:

– If the NACE is implemented as a DHCP v4 server, the CNGCF-Address AVP shall be used to set the value of DHCP Option 43 (DSL Forum Autoconfiguration Server) or DHCP Option 66 (TFTP server).

– If the NACE is implemented as a DHCP v4 server, the Location-Information AVP shall be mapped to the DHCP option 123 or 99.

– If the NACE is implemented as a DHCP v4 server, the SIP-Outbound-Proxy AVP shall be mapped to the DHCP option 120.

The behaviour when the NACE does not receive a Bind acknowledgement, or when it arrives after the internal timer waiting for it has expires, or when it arrives with an indication that is different to DIAMETER_SUCCESS, is outside of the scope of this Recommendation.

8.2.1.3 Procedure at the TLM-PE side

If at least one of the specified AVP(s) is invalid, the TLM-PE shall return a Bind acknowledgement with a Result-Code AVP value set to DIAMETER_INVALID_AVP_VALUE and a Failed-AVP AVP containing a copy of the invalid AVP(s).

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

– Create an internal record to store the received information for future use.

If the globally unique identifier contained in the Globally-Unique-Address AVP is already known and the received Logical access ID is different than the one stored in the internal record, the TLM-PE shall:

– interact with RACE entities (i.e., PD-PE) to remove transport policies associated with the existing record and clear associated resources;

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

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 return a Bind acknowledgement with a Result-Code AVP value set to DIAMETER_UNABLE_TO_COMPLY or an Experimental-Result-Code AVP set to DIAMETER_SYSTEM_UNAVAILABLE.

Otherwise, the requested operation shall take place and the TLM-PE shall return a Bind acknowledgement with the Result-Code AVP set to DIAMETER_SUCCESS and one or more of the AVPs identified in Table 8-2.

8.2.2 Unbind indication

8.2.2.1 Overview

This procedure is used by the NAC-PE to report the 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 enables the TLM-PE to remove the corresponding record from its internal database.

This procedure is mapped to the Push-Notification-Request/Answer commands in the Diameter application specified in clause 10. Tables 8-3 and 8-4 detail the relevant information elements as defined in the NACE and their mapping to Diameter AVPs.

Table 8-3 – Unbind indication

Information element name	Mapping to Diameter AVP	Category
Unique IP Address	Globally-Unique-Address	M
Address Realm		
IP Connectivity Status	IP-Connectivity-Status	M

Table 8-4 – Unbind indication acknowledgement

Information element name	Mapping to Diameter AVP	Category
Result	Result-Code /Experimental_Result	M

8.2.2.2 Procedure on the NAC-PE side

On receipt of release request for the allocated IP address from the user equipment or in case of expiry of the lease period or on receipt of an indication that the underlying layer 2 connection has been lost, the NACE shall clear all information stored against the IP address and issue a Push-Notification-Request representing a Globally-Unique-Address.

The IP-Connectivity-Status AVP shall be set to IP CONNECTIVITY LOST.

8.2.2.3 Procedure on the TLM-PE side

If the globally unique identifier contained in the Globally-Unique-Address AVP is not known, the TLM-PE shall stop processing the request and set the Experimental-Result-Code to IAMETER_ERROR_USER_UNKNOWN in the Unbind indication acknowledgement. If the globally unique identifier contained in the Globally-Unique-Address AVP is already known, the TLM-PE shall:

– remove the existing session record;

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

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 set to DIAMETER_SYSTEM_UNAVAILABLE. Otherwise, the requested operation shall take place and the TLM-PE shall return an Unbind indication acknowledgement with the Result-Code AVP set to DIAMETER_SUCCESS.

8.2.3 Bind information query

8.2.3.1 Overview

This procedure is used by the TLM-PE to request binding information from the NAC-PE, in the context of recovery procedures.

This procedure is mapped to the User-Data-Request/Answer commands in the Diameter application specified in clause 10. Tables 8-5 and 8-6 detail the relevant information elements as defined in the NACE and their mapping to Diameter AVPs.

Table 8-5 – Bind information query

Information element name	Mapping to Diameter AVP	Category
Unique IP Address	Globally-Unique-Address	M
Address Realm		

Table 8-6 – Bind information query acknowledgement

Information element name	Mapping to Diameter AVP	Category
Result	Result-Code /Experimental_Result	M
Unique IP Address(optional)	Globally-Unique-Address	O
Address Realm(optional)		
Physical Connection Identifier (optional)	Physical-Access-Id	O
Logical Connection Identifier (optional)	Logical-Access-Id	O
CPE Type(optional)	Terminal-Type	O

8.2.3.2 Procedure on the TLM-PE side

The TLM-PE may use this procedure after a restart, upon reception of the query request from entity associated with an IP-Address for which no record is stored.

The TLM-PE determines the NACE responsible for this IP address from the IP realm, and possibly the address range within this realm, it belongs to. In order to cope with network configurations where multiple NACE are associated with the same IP realm and are using overlapping address ranges, the TLM-PE may apply one of the following procedures:

– The TLM-PE queries each of the NACE until it gets a Bind Information Query acknowledgement with the Result-Code AVP set to DIAMETER_SUCCESS.

– The TLM-PE sends the query to a Diameter Agent that has sufficient routing information to enable this query to be delivered to the appropriate NACE instance.

If no successful answer is received, the TLM-PE shall delete all information that may have been stored regarding this IP address and provides an appropriate response to the requesting entity.
The TLM-PE shall populate the Binding Information Query as follows:

1) The Globally-Unique-Address AVP shall be included.

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

8.2.3.3 Procedure on the NAC-PE side

Upon reception of the Bind information query, the NACE 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 no session record is stored for the Globally-Unique-Address AVP, return a Bind Information Query Acknowledgment with the Experimental-Result-Code AVP set to DIAMETER_ERROR_USER_UNKNOWN.

If the NACE 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 NACF shall return a Bind information query acknowledgement with the Result-Code AVP set to DIAMETER_SUCCESS and the session data described in Table 8-6.

8.2.4 Mobility service parameters indication

8.2.4.1 Overview

This procedure is used by the TLM-PE to report mobility service information to the NAC-PE, upon successful authentication of the user.

This procedure is mapped to the Push-Notification-Request/Answer commands in the Diameter application specified in clause 10. Tables 8-7 and 8-8 detail the relevant information elements as defined in the NACE and their mapping to Diameter AVPs.

Table 8-7 – Mobility service parameters indication

Information element name	Mapping to Diameter AVP	Category
Transport Subscriber Identifier (Note 1)	User-Name	M
Unique IP Address	Globally-Unique-Address	M
Address Realm		
Mobility Service Parameters (optional)	Mobility-Service-Parameters	O
– Address of MLM-PE(C)	Central-MLM-PE-Contact-Point	O
– Address of MLM-PE(P)	Proxy-MLM-PE-Contact-Point	O
– Keying Material	Keying-Material	O
– Mobility Protocol Type	Mobility-Protocol-Type	O
– Anchor point address	Anchor-Point-Address	O
– Tunnel end point address (optional)	Tunnel-End-Point-Address	O

Table 8-8 – Mobility service parameters indication acknowledgement

Information element name	Mapping to Diameter AVP	Category
Result	Result-Code /Experimental_Result	M

8.2.4.2 Procedure at the TLM-PE side

The TLM-PE knows the address of the NAC-PE entity where the information should be pushed, either from the configuration data or from the transport resource information (i.e., received from the TUP-PE).

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

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

– In case PPP is applied, the Globally-Unique-Address AVP shall be present. In case DHCP is applied, this AVP is optional. The Globally-Unique-Address AVP shall contain a Frame-IP-Address or Frame-IPv6-Prefix AVP value and an Address-Realm AVP.

– If available in the TAA-PE, the User-Name AVP shall be present.

The presence of the other AVPs depends on the transport resource information and the local policy rules.

8.2.4.3 Procedure at the NAC-PE side

If the Globally-Unique-Address AVP is not present or is invalid, the NAC-PE shall return a mobility service parameters indication acknowledgement with a Result-Code AVP value set to DIAMETER_INVALID_AVP_VALUE.

If the contents of the request are invalid the NAC-PE shall return a mobility service parameters indication acknowledgement with a Result-Code AVP value set to the appropriate value.

If the NAC-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 return a mobility service parameters indication acknowledgement 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 NAC-PE shall return the Result-Code AVP set to DIAMETER_SUCCESS in the Mobility service parameters indication acknowledgement.

9 Use of Diameter-based protocol

With the clarifications listed in the following clauses, the Diameter base protocol defined by [IETF RFC 6733] shall apply.

9.1 Securing Diameter messages

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

9.2 Accounting functionality

Accounting functionality (Accounting session state machine, related command codes and AVPs) is not used at the Ne interface.

9.3 Use of 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 [IETF RFC 6733].

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 [IETF RFC 6733]. 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.

9.4 Transport protocol

Diameter messages over the Ne interface shall make use of SCTP [IETF RFC 4960] and shall utilize the new SCTP checksum method specified in [IETF RFC 4960].

9.5 Routing considerations

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

With regard to the Diameter protocol used at the Ne interface, the TLM-PE acts as a Diameter server and the NAC-PE acts as the Diameter client.

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

9.6 Advertising application support

The Capabilities-Exchange-Request (CER) and Capabilities-Exchange-Answer (CEA) commands are specified in [IETF RFC 6733]. The Diameter base application identifier (0) shall be used in the Diameter message header of these messages.

If TLM-PE and NAC-PE indicate support of the Ne application, then the Ne application identifier (16777326) shall be used in the Diameter message header of all subsequent messages exchanged within this association.

Support of the Ne application within the CER/CEA is indicated by supplying an instance of the Vendor-Specific-Application-Id containing a Vendor-Id AVP set to ITU-T (11502) and an Auth-Application-Id AVP set to Ne (16777326).

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

Table 9-1 – Vendor identifiers for Ne

Vendor	Vendor identifier
3GPP	10415
ETSI	13019
ITU-T	11502

NOTE – The Vendor-Id AVP included in Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands that are not included in the Vendor-Specific-Application-Id AVPs as described above shall indicate the manufacturer of the Diameter node as per [IETF RFC 6733].

10 Message specification

10.1 Commands

This Recommendation re-uses the Diameter commands defined in [ETSI TS 129 329]. Other commands shall be ignored by the TLM-PE and NAC-PE.

Table 10-1 – Command code

Command	Abbreviation	Defining reference	Command code	See clause
Push-Notification-Request	PNR	ETSI TS 129 329	309	10.1.1
Push-Notification-Answer	PNA	ETSI TS 129 329	309	10.1.2
User-Data-Request	UDR	ETSI TS 129 329	306	10.1.3
User-Data-Answer	UDA	ETSI TS 129 329	306	10.1.4
Push-Notification-Request	PNR	ETSI TS 129 329	309	10.1.5
Push-Notification-Answer	PNA	ETSI TS 129 329	309	10.1.6

10.1.1 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 [ETSI TS 129 329] and used with additional AVPs defined in this Recommendation.

Message Format:

```
< Push-Notification-Request > ::= < Diameter Header: 309, REQ, PXY, 16777326>
                              < Session-Id >
                              { Vendor-Specific-Application-Id }
                              { Auth-Session-State }
                              { Origin-Host }
                              { Origin-Realm }
                              [ Destination-Host ]
                              { Destination-Realm }
                              [ Globally-Unique-Address ]
                              [ Physical-Access-Id ]
                              [ Logical-Access-Id ]
                              [ Terminal-Type ]
                              [ IP-Connectivity-Status]
                              *[ AVP ]
                              *[ Proxy-Info ]
                              *[ Route-Record ]
```

10.1.2 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. The Experimental-Result AVP may contain one of the values defined in clause 10.2.

Message Format:

```
< Push-Notification-Answer > ::= < Diameter Header: 309, PXY, 16777326>
                             < Session-Id >
                             { Vendor-Specific-Application-Id }
                             [ Result-Code ]
                             [ Experimental-Result ]
                             { Auth-Session-State }
                             { Origin-Host }
                             { Origin-Realm }
                             [ CNGCF-Address ]
                             [ Location-Data ]
                             [ SIP-Outbound-Proxy ]
                             [ SADS-Id ]
                             *[ AVP ]
                             *[ Failed-AVP ]
                             *[ Proxy-Info ]
                             *[ Route-Record ]
```

10.1.3 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 server to a Diameter client in order to notify changes in the user data in the server. This command is defined in [ETSI TS 129 329] and used with additional AVPs defined in this Recommendation.

Message Format:

```
< User-Data-Request > ::= < Diameter Header: 306, REQ, PXY, 16777326>
                          < Session-Id >
                          { Vendor-Specific-Application-Id }
                          { Auth-Session-State }
                          { Origin-Host }
```

```
                                { Origin-Realm }
                                [ Destination-Host ]
                                { Destination-Realm }
                                { Globally-Unique-Address }
                                *[ AVP ]
                                *[ Proxy-Info ]
                                *[ Route-Record ]
```

10.1.4 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 client in response to the User-Data-Request command. The Experimental-Result AVP may contain one of the values defined in clause 10.2.

Message Format:

```
< User-Data-Answer > ::= < Diameter Header: 306, PXY, 16777326>
                                < Session-Id >
                                { Vendor-Specific-Application-Id }
                                [ Result-Code ]
                                [ Experimental-Result ]
                                { Auth-Session-State }
                                { Origin-Host }
                                { Origin-Realm }
                                [ Globally-Unique-Address ]
                                [ Physical-Access-Id ]
                                [ Logical-Access-Id ]
                                [ Terminal-Type ]
                                *[ AVP ]
                                *[ Failed-AVP ]
                                *[ Proxy-Info ]
                                *[ Route-Record ]
```

10.1.5 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 [ETSI TS 129 329] and used with additional AVPs defined in this Recommendation.

Message Format:

```
< Push-Notification-Request > ::= < Diameter Header: 309, REQ, PXY, 16777326>
                                < Session-Id >
                                { Vendor-Specific-Application-Id }
                                { Auth-Session-State }
                                { Origin-Host }
                                { Origin-Realm }
                                [ Destination-Host ]
                                { Destination-Realm }
                                { User-Name }
                                { Globally-Unique-Address }
                                [ Mobility-Service-Parameters ]
                                *[ AVP ]
                                *[ Proxy-Info ]
                                *[ Route-Record ]
```

10.1.6 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. The Experimental-Result AVP may contain one of the values defined in clause 10.2.

Message Format:

```
< Push-Notification-Answer > ::= < Diameter Header: 309, PXY, 16777326>
                               < Session-Id >
                               { Vendor-Specific-Application-Id }
                               [ Result-Code ]
                               [ Experimental-Result ]
                               { Auth-Session-State }
                               { Origin-Host }
                               { Origin-Realm }
                               *[ AVP ]
                               *[ Failed-AVP ]
                               *[ Proxy-Info ]
                               *[ Route-Record ]
```

10.2 Experimental-Result-Code AVP values

This sub-clause defines specific values of the Experimental-Result-Code AVP used in this specification. Most of these are imported from 3GPP and ETSI specifications, as indicated in the subclauses below.

10.2.1 Experimental-Result-Code AVP values imported from ETSI TS 129 229

This sub-clause defines the specific values of the Experimental-Result-Code AVP imported from [ETSI TS 129 229] (vendor-id is ETSI):

DIAMETER_ERROR_USER_UNKNOWN (5001)

The request failed because the IP address or Globally-Unique Address is not found.

DIAMETER_USER_DATA_NOT_AVAILABLE (4100)

The requested data is not available at this time to satisfy the requested operation

10.3 Attribute value pairs (AVPs)

The following tables (Tables 10-2 to 10-7) summarize the AVPs used in this Recommendation. These are, in addition to the AVPs, defined in [IETF RFC 6733].

Table 10-2 describes the Diameter AVPs defined by [ETSI ES 283 034] and used within this Recommendation. These AVPs are described in this Recommendation for information; however, the normative detail for these AVPs is contained in [ETSI ES 283 034]. The Vendor-Id header of all AVPs defined in Table 10-2 shall be set to ETSI (13019).

Table 10-2 – Diameter AVPs imported from [ETSI ES 283 034]

Attribute name	AVP code	Clause defined	Value type	AVP flag rules				May encrypt
				Must	May	Should not	Must not	
Globally-Unique-Address	300	10.3.1	Grouped	M,V				Y
Logical-Access-ID	302	10.3.2	OctetString	V	M			Y
IP-Connectivity-Status	305	10.3.3	Enumerated	V	M			Y
Physical-Access-ID	313	10.3.4	UTF8String	V	M			Y

Table 10-3 describes the Diameter AVPs defined by [ETSI ES 283 035] and used within this Recommendation. These AVPs are described in this Recommendation for information; however, the normative detail for these AVPs is contained in [ETSI ES 283 035]. The Vendor-Id header of all AVPs defined in Table 10-3 shall be set to ETSI (13019).

Table 10-3 – Diameter AVPs imported from [ETSI ES 283 035]

Attribute name	AVP code	Clause defined	Value type	AVP flag rules				May encrypt
				Must	May	Should not	Must not	
Terminal-Type	440	10.3.5	Grouped	V	M			Y

Table 10-4 describes the Diameter AVPs defined by [ETSI TS 183 059-1] and used within this Recommendation. These AVPs are described in this Recommendation for information; however, the normative detail for these AVPs is contained in [ETSI TS 183 059-1]. The Vendor-Id header of all AVPs defined in Table 10.4 shall be set to ETSI (13019).

Table 10-4 – Diameter AVPs imported from [ETSI TS 183 059-1]

Attribute name	AVP code	Clause defined	Value type	AVP flag rules				May encrypt
				Must	May	Should not	Must not	
CNGCF-Address	600	10.3.6	Grouped	V	M			Y
SIP-Outbound-Proxy	601	10.3.7	OctetString	V	M			Y

Table 10-5 describes the Diameter AVPs defined by [IETF RFC 5580] and used in this Recommendation, their AVP Code values, types, possible flag values. Flags values are described in the context of this Recommendation rather than in the context of the application where they are defined.

Table 10-5 – Diameter AVPs imported from [IETF RFC 5580]

Attribute name	AVP code	Clause defined	Value type	AVP flag rules				May encrypt
				Must	May	Should not	Must not	
Location-Data	128	10.3.8	OctetString	V	M			Y

Table 10-6 describes the Diameter AVPs defined by [ITU-T Q.3232] and used in this Recommendation. These AVPs are described in this Recommendation for information; however, the normative detail for these AVPs is contained in [ITU-T Q.3232]. The Vendor-Id header of all AVPs defined in Table 10-6 shall be set to ITU-T (11502).

Table 10-6 – Diameter AVPs imported from [ITU-T Q.3232]

Attribute name	AVP code	Clause defined	Value type	AVP flag rules				May encrypt
				Must	May	Should not	Must not	
Mobility-Service-Parameters	1050	10.3.9	Grouped	V	M			Y

Table 10-7 describes the AVPs defined solely within this Recommendation. The ITU-T Vendor-Id (11502) shall be used in the Vendor-Id field of the AVP header.

Table 10-7 – Diameter AVPs defined in this Recommendation

Attribute name	AVP code	Clause defined	Value type	AVP flag rules				May encrypt
				Must	May	Should not	Must not	
SADS-Id	1059	10.3.10	OctetString	V	M			Y

10.3.1 Globally-Unique-Address AVP

The Globally-Unique-IP-Address AVP (AVP code 300 13019) is of type Grouped.

AVP format:

```
Globally-Unique-Address ::= < AVP Header: 300 13019 >
       [Framed-IP-Address]
       [Framed-IPv6-Prefix]
       [Address-Realm]
```

10.3.2 Logical-Access-ID AVP

The Logical-Access-ID AVP (AVP code 302 13019) is of type OctetString. This AVP contains either a circuit identifier or a technology independent identifier.

NOTE – In the ATM case, the Logical Access ID may explicitly contain the identity of the VP and VC carrying the traffic.

10.3.3 IP-Connectivity-Status AVP

The IP-Connectivity-Status AVP (AVP code 305 13019) is of type Enumerated. The following values are defined:

– IP-CONNECTIVITY-ON (0).

– IP-CONNECTIVITY-LOST (1).

10.3.4 Physical-Access-ID AVP

The Physical-Access-ID AVP (AVP code 313 13019) is of type UTF8String and identifies the physical access to which the user equipment is connected. It includes a port identifier and the identity of the access node where the port resides.

10.3.5 Terminal-Type AVP

The Terminal-Type AVP (AVP code 352 13019) is of type OctetString and contains a value of the User Class DHCP Option (77).

10.3.6 CNGCF-Address AVP

The CNGCF-Address AVP (AVP code 600 13019) is of type Grouped and contains one or more CNGCF addresses, each of which identifying different types of CNGCF implementation.

AVP Format:

```
CNGCF-Address ::= < AVP Header: 600 13019 >
       [TFTP-Server]
       [ACS-Server]
```

10.3.7 SIP-Outbound-Proxy AVP

The SIP-Outbound-Proxy AVP (AVP code 601 13019) is of type OctetString and identifies a SIP outbound proxy (e.g. a P-CSC-PE when accessing to the SCF) in the form of an FQDN.

10.3.8 Location-Data AVP

The Location-Data AVP (AVP code 128 0) is of type OctetString. It contains location data in the form of either Civic Location or Geospatial Location.

10.3.9 Mobility-Service-Parameters AVP

The Mobility-Service-Parameters AVP (AVP code 1050 11502) is of type Grouped and provides mobility service parameters.

AVP Format:

```
Mobility-Service-Parameters ::= < AVP Header: 1050 11502 >
       [Central-MLM-PE-Contact-Point]
       [Proxy-MLM-PE-Contact-Point]
       [Keying-Material]
       [Mobility-Protocol-Type]
       [Anchor-Point-Address]
       [Tunnel-End-Point-Address]
```

10.3.10 SADS-Id AVP

The SADS-Id AVP (AVP code 1059 11502) is of type OctetString and identifies the SADS for accessing IPTV services.

10.4 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 the Internet Assigned Numbers Authority (IANA).

10.4.1 AVP codes

This Recommendation uses AVP values from the AVP Code namespace managed by ETSI for its Diameter vendor-specific applications. In addition, this Recommendation assigns AVP code values within the Diameter AVP Code namespace managed by ITU-T. See clause 10.3.

10.4.2 Experimental-Result-Code AVP values

This Recommendation assigns the Experimental-Result-Code AVP values from the AVP Code namespace managed by ETSI for its Diameter vendor-specific applications. See clause 10.2.

10.4.3 Command code values

This Recommendation does not assign command code values but uses existing commands defined by the Internet Engineering Task Force (IETF), including those requested by 3GPP.

10.4.4 Application-ID value

This Recommendation defines the Ne Diameter application with application ID 16777326. The vendor identifier assigned by IANA to ITU-T is 11502 (http:/www.iana.org/assignments/enterprise-numbers).

11 Security considerations

Security requirements within the functional requirements and architecture of the NACF are addressed by the security requirements for NGN [ITU-T Y.2701]. The Ne interface shall follow the security requirements of the network attachment control functions (NACF) [ITU-T Y.2014].

Clause 9.1 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].

Additional considerations are provided in the security considerations section of [IETF RFC 6733].

Bibliography

[b-ITU-T Q.1001] Recommendation ITU-T Q.1001 (1988), *General aspects of public land mobile networks.*

[b-IETF RFC 2131] IETF RFC 2131 (1997), *Dynamic Host Configuration Protocol*.

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

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	Environment and ICTs, climate change, e-waste, energy efficiency; 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, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2016