

IPWorks 3GPP AAA Server-PDN GW S6b Interface

INTERWORK DESCRIPTION

Copyright

© Ericsson AB 2016. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

All trademarks mentioned herein are the property of their respective owners. These are shown in the document IPWorksTrademark Information.



Contents

1	Introduction	1
1.1	Prerequisites	1
1.2	Related Information	1
2	Interface Overview	3
2.1	Interface Role	3
2.2	Services	3
2.3	Encapsulation and Addressing	3
3	Procedures	5
3.1	PDN GW Initiated Authorization	5
3.2	PDN GW Initiated Session Termination	5
3.3	AAA Server Initiated Re-Authorization	6
3.4	HSS Initiated P-CSCF Restoration	7
4	Information Model	11
4.1	PDN GW Initiated Authorization	11
4.2	PDN GW Initiated Session Termination	12
4.3	AAA Server Initiated Re-Authorization	13
5	Diameter AVPs	15
5.1	IETF Protocol AVPs	15
5.2	3GPP AVPs	19
6	Formal Syntax	29
7	Diameter Error Handling	31
8	Related Standards	33
	Reference List	35





1 Introduction

This document describes the S6b interface between the PDN GW and the 3GPP AAA server in EPC network.

Scope

The scope of this document includes the S6b interface protocol described in TS 29.273. Now the S6b interface is used to update the PDN GW information to HSS in the case the UE attaches to the PDN GW using the s2a reference point.

This document covers the following topics:

- Interface Overview
- Interface Role
- Services
- Encapsulation and Addressing
- Procedures
- Information Model
- Diameter AVPs
- Diameter Error Handling
- Formal Syntax
- Related Standards

Target Groups

This document is intended for personnel needing to understand the logical entity, including interfaces and protocols, of the IPWorks.

1.1 Prerequisites

N/A

1.2 Related Information

Trademark information, typographic conventions, definition and explanation of acronyms and terminology can be found in the following documents:

- Glossary of Terms and Acronyms, Reference [1]



- Trademark Information, Reference [2]
- Typographic Conventions, Reference [3]

The standard, related to the S6b interface, can be found in the section Reference.



2 Interface Overview

This section describes the interface between the PDN GW and the 3GPP AAA server in EPC network. The PDN GW uses this interface to do the authorization and update the PDN GW information to HSS.

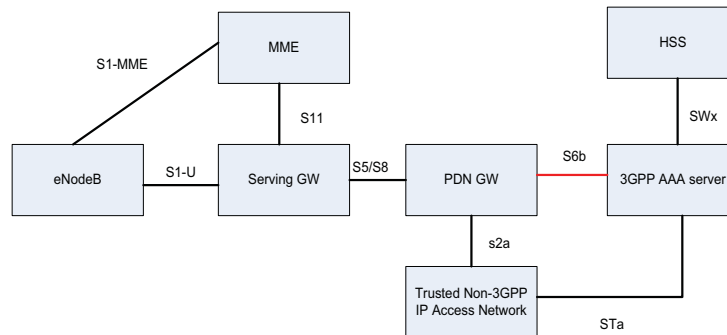


Figure 1 S6b Interface

2.1 Interface Role

S6b interface uses the Diameter Protocol to do the authorization of the PDN GW, and the 3GPP AAA server will update or remove the PDN GW information to/from HSS when PDN attaches or detaches to 3GPP AAA server. For S6b interface, the IPWorks AAA server will take the role of 3GPP AAA server in EPC network.

2.2 Services

This section describes the services the S6b interface offers.

The services offered by the S6b interface are shown in Table 1.

Table 1 Offered Services

Offered Service	Description
Authorization	The PDN GW shall update its address information to the 3GPP AAA Server and HSS. Static QoS profile information may also be downloaded at the same time.

2.3 Encapsulation and Addressing

The following lower level protocols are used on this interface:

- SCTP



- TCP
- DIAMETER



3 Procedures

This section describes the procedures used in connection with the offered and used interfaces of IPWorks:

- PDN GW Initiated Authorization
- PDN GW Initiated session Termination
- AAA Server Initiated Re-Authorization
- HSS Initiated P-CSCF Restoration

3.1 PDN GW Initiated Authorization

This procedure is triggered when the PDN GW receives a PBU message from the MAG. The PDN GW initiates an authorization procedure by sending an Authorization Request message to the 3GPP AAA server in order to update the PGW Address for the APN, as well as to download UE specific APN profile information.

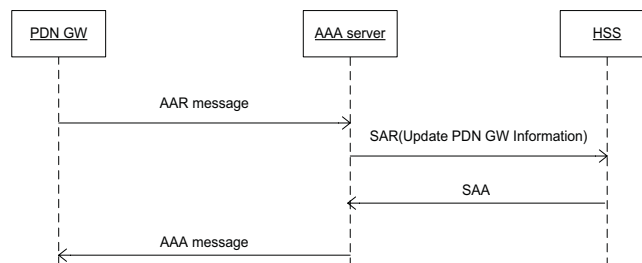


Figure 2 Authorization procedure

3.2 PDN GW Initiated Session Termination

This procedure is triggered by PDN GW when the UE disconnect a PDN connection associated to an APN.

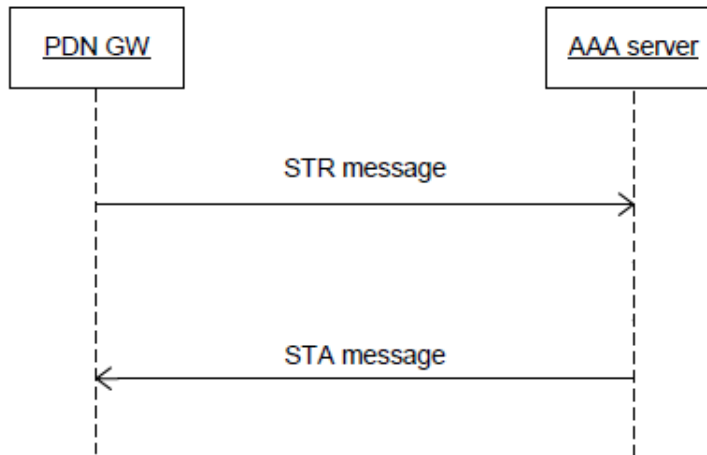


Figure 3 Session Termination Procedure

3.3 AAA Server Initiated Re-Authorization

This procedure is triggered when the subscriber profile is modified in HSS. The procedure is based on Diameter RAR (see Section 4.3 on page 13) and AAR(Section 4.1.1 on page 11) messages.

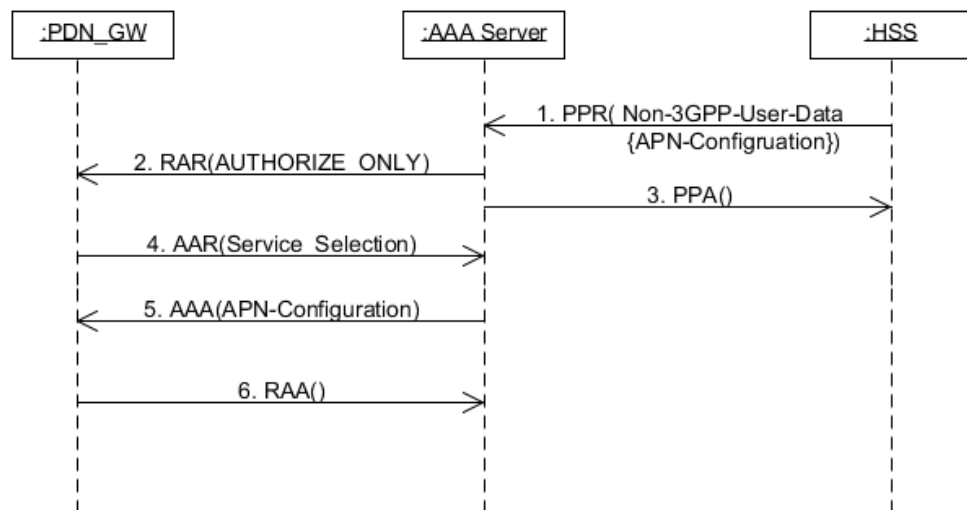


Figure 4 AAA Server Initiated Re-Authorization



3.4 HSS Initiated P-CSCF Restoration

If there is a stored information that IMS PDN connection is established via a WLAN access, with checking that the PGW supports the HSS-based P-CSCF restoration for WLAN, the 3GPP AAA Server must send a P-CSCF restoration indication to the PGW over S6b in a RAR command.

For the basic P-CSCF restoration mechanism, the PDN GW must send a Session Termination Request to the 3GPP AAA Server.

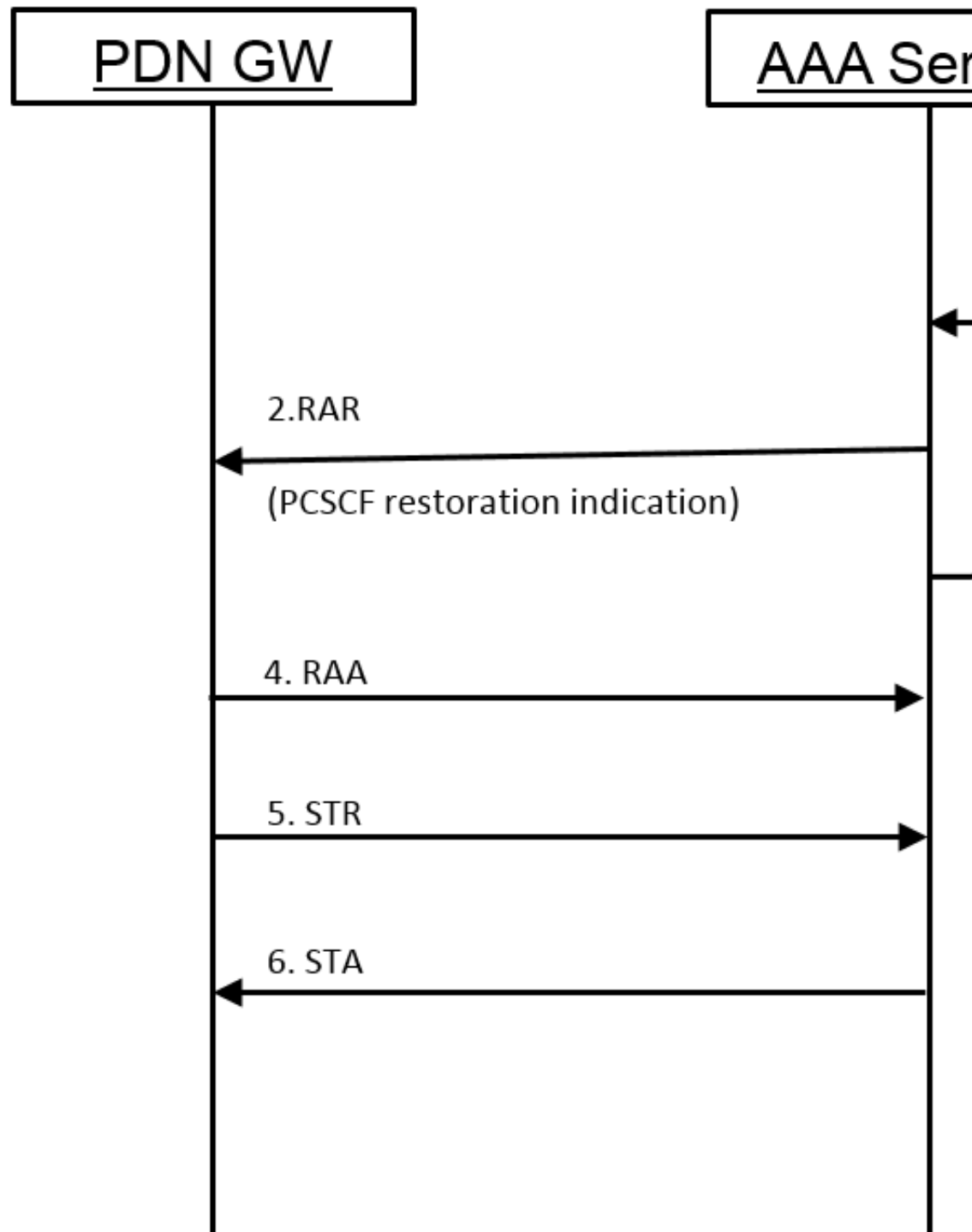


Figure 5 Basic P-CSCF Restoration Mechanism



For the extended P-CSCF restoration mechanism, the PDN GW might send the authorization request with only mandatory AVPs.

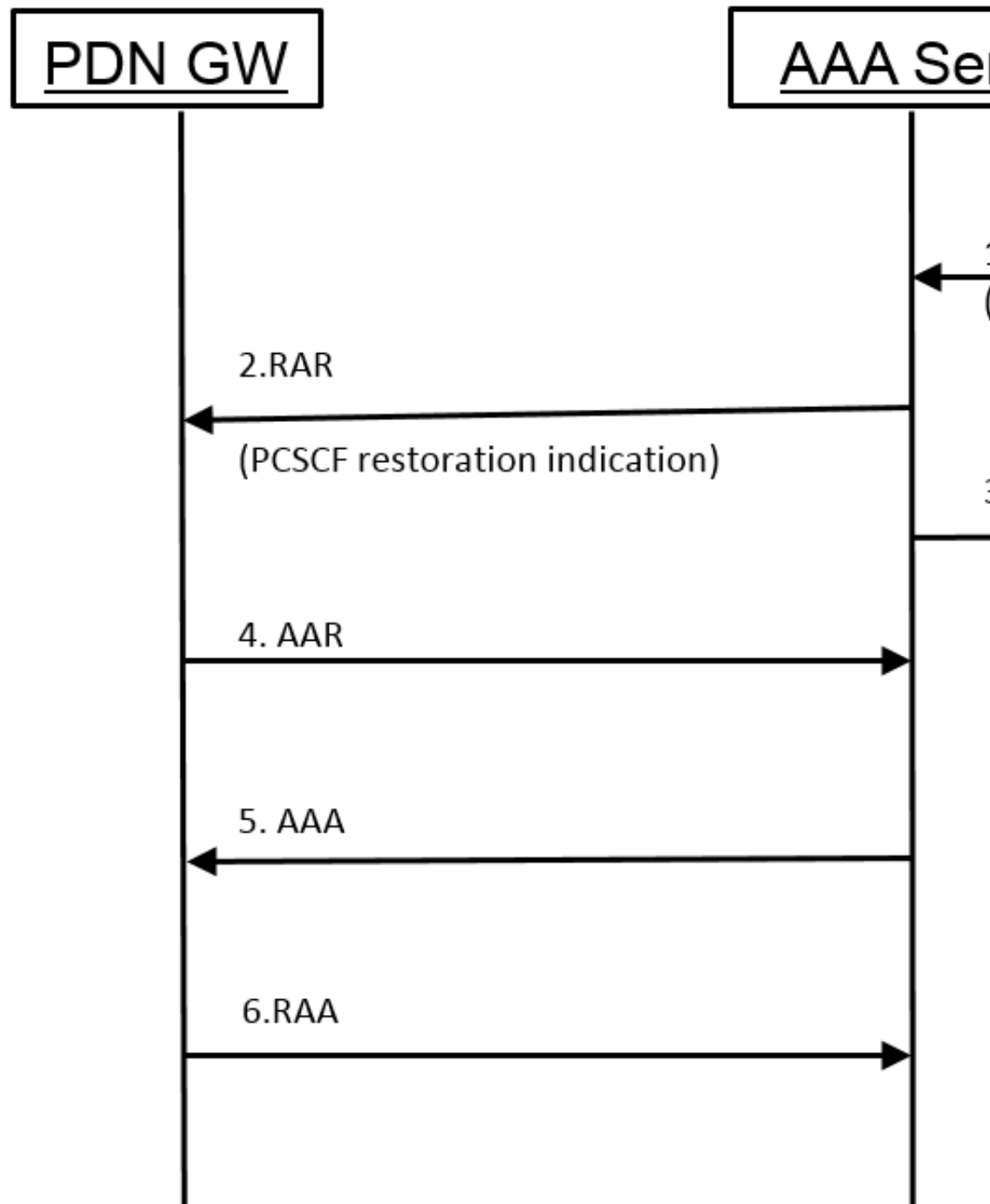


Figure 6 Extended P-CSCF Restoration Mechanism





4 Information Model

This section describes the information model including mandatory and optional parameters of each service operation. This document only covers the diameter messages and the AVPs.

Note: Description about the format of the Base Protocol is described in Reference [4]

Table 2 shows the Naur Form (ABNF) format in Augmented Backus used in the subsections.

Table 2 Naur Form (ABNF) format

{ }	Mandatory
< >	Mandatory with fixed place
[]	Optional
*	Zero or more Occurrences
*n	At most
n	Occurrences

4.1 PDN GW Initiated Authorization

4.1.1 AA-Request (AAR) Command

The AA-Request (AAR) command, indicated by the Command-Code field set to 265 and the “R” bit set in the Command Flags field, is sent from a PDN GW to a 3GPP AAA server. The Command Code value and ABNF are reused from the IETF RFC 4005 AA-Request command. New AVPs are added using the *[AVP] extension mechanism in the original ABNF.

Message Format:

```
<AA-Request> ::= <Diameter Header: 265, REQ, PXY, 16777272>
    <Session-Id>
    {Auth-Application-Id}
    {Origin-Host}
    {Origin-Realm}
    {Destination-Realm}
    {Auth-Request-Type}
    [User-Name]
    [Visited-Network-Identifier]
    [MIP6-Agent-Info]
    [MIP6-Feature-Vector]
    [QoS-Capability]
```

```
[Service-Selection]
[Emergency-Services]
*[Supported-Features]
*[Proxy-Info]
*[Route-Record]
*[AVP]
```

4.1.2 AA-Answer (AAA) Command

The AA-Answer (AAA) command, indicated by the Command-Code field set to 265 and the “R” bit cleared in the Command Flags field, is sent from a 3GPP AAA server to a PDN GW. The Command Code value and ABNF are reused from the IETF RFC 4005 AA-Answer command. New AVPs are added using the *[AVP] extension mechanism in the original ABNF.

Message Format:

```
<AA-Answer> ::= <Diameter Header: 265, PXY, 16777272>
    <Session-Id>
    {Auth-Application-Id}
    {Auth-Request-Type}
    {Result-Code}
    {Origin-Host}
    {Origin-Realm }
    [MIP6-Feature-Vector]
    [APN-Configuration]
    [Service-Selection]
    [Session-Timeout]
    [QoS-Resources]
    *[Redirect-Host]
    [Trace-Info]
    [Redirect-Host-Usage]
    [Redirect-Max-Cache-Time]
    *[Supported-Features]
    *[Proxy-Info]
    *[AVP]
```

4.2 PDN GW Initiated Session Termination

4.2.1 Session-Termination-Request (STR) Command

The Session-Termination-Request (STR) command, indicated by the Command-Code field set to 275 and the “R” bit set in the Command Flags field, is sent from a PDN GW to a 3GPP AAA server. The Command Code value and ABNF are re-used from the IETF RFC 3588 Session-Termination-Request command. New AVPs are added using the *[AVP] extension mechanism in the original ABNF.



Message Format:

```
<Session-Termination-Request> ::= <Diameter Header: 275, REQ, PXY,
    16777272>
    <Session-Id>
    {Auth-Application-Id}
    {Origin-Host}
    {Origin-Realm}
    {Destination-Realm}
    {Termination-Cause}
    [User-Name]
    *[Proxy-Info]
    *[Route-Record]
    *[AVP]
```

4.2.2 Session-Termination-Answer (STA) Command

The Session-Termination-Answer (STA) command, indicated by the Command-Code field set to 275 and the “R” bit cleared in the Command Flags field, is sent from a 3GPP AAA server to a PDN GW. The Command Code value and ABNF are re-used from the IETF RFC 3588 Session-Termination-Answer command.

Message Format:

```
<Session-Termination-Answer> ::= <Header: 275, PXY, 16777272>
    <Session-Id>
    {Result-Code}
    {Origin-Host}
    {Origin-Realm}
    [Redirect-Host-Usage]
    [Redirect-Max-Cache-Time]
    *[Proxy-Info]
    *[AVP]
```

4.3 AAA Server Initiated Re-Authorization

4.3.1 Re-Auth-Request (RAR) Command

The Diameter Re-Auth-Request (RAR) command shall be indicated by the Command-Code field set to 258 and the “R” bit set in the Command Flags field and is sent from a 3GPP AAA Server or 3GPP AAA Proxy to a PDN-GW. The ABNF for the RAR command shall be as follows:

```
< Re-Auth-Request > ::=
< Diameter Header: 258, REQ, PXY, 16777272 >
    < Session-Id >
```



```
{ Origin-Host }
{ Origin-Realm }
{ Destination-Realm }
{ Destination-Host }
{ Auth-Application-Id }
{ Re-Auth-Request-Type }
[ User-Name ]
[RAR-Flags ]
...
*[ AVP ]
```

Note: AAA Server does not use RAR-Flags AVP in AAA initiated Re-Authorization procedure.

4.3.2 Re-Auth-Answer(RAA) Command

The Diameter Re-Auth-Answer (ASA) command shall be indicated by the Command-Code field set to 258 and the "R" bit cleared in the Command Flags field and is sent from a PDN-GW to a 3GPP AAA Server or 3GPP AAA Proxy. The ABNF for the RAA commands shall be as follows:

```
< Re-Auth-Answer > ::=
< Diameter Header: 258, PXY, 16777272 >
    < Session-Id >
        { Result-Code }
        { Origin-Host }
        { Origin-Realm }
        [ User-Name ]
        ...
    *[ AVP ]
```



5 Diameter AVPs

5.1 IETF Protocol AVPs

Diameter Base Protocol (RFC3588) AVPs that are included in the STa messages, are described in Reference [4].

Table 3

Attribute Name	AVP Code	Value Type	Must	May	Should not	Must not
MIP6-Feature-Vector	124	Unsigned64	M			V
MIP6-Home-Link-Prefix	125	OctetString	M	P		V
Re-Auth-Request-Type	285	Enumerated	M	P		V
MIP-Home-Agent-Addresses	334	Address	M			V
MIP-Home-Agent-Host	348	Grouped	M			V
MIP6-Agent-Info	486	Grouped	M			V
Service-Selection	493	UTF8String	M	P		V
QoS-Resources	508	Grouped	M			V
Filter-Rule	509	Grouped	M			V
QoS-Profile-Id	573	Unsigned32	M			V
QoS-Profile-Template	574	Grouped	M			V
QoS-Capability	578	Grouped	M			V



Attribute Name	AVP Code	Value Type	Must	May	Should not	Must not
Proxy-Info	284	Grouped	M			P, V
Route-Record	282	DiamIdent	M			V

5.1.1 MIP6-Feature-Vector

The MIP6-Feature-Vector AVP contains a 64 bit flags field of supported mobility capabilities of the NAS. This AVP is defined in IETF RFC 5447. The NAS may include this AVP in a request message to indicate the mobility capabilities of the NAS to the 3GPP AAA server. Similarly, the Diameter server may include this AVP in an answer message to inform the NAS about which of the NAS indicated capabilities are supported or authorized by the 3GPP AAA Server.

Following capabilities are supported on S6b reference point in PMIPv6 mode:

- PMIPv6_SUPPORTED
- IP4_HOA_SUPPORTED

5.1.2 MIP6-Home-Link-Prefix

The MIP6-Home-Link-Prefix AVP defined in RFC 5447 is of type OctetString and contains the Mobile IPv6 home network prefix information in a network byte order.

5.1.3 Re-Auth-Request-Type

The Re-Auth-Request-Type AVP (AVP Code 285) is of type Enumerated. And it indicates whether the user is to be authorized only or authenticated and authorized.

AUTHORIZE_ONLY	0
AUTHORIZE_AUTHENTICATE	1

5.1.4 MIP6-Agent-Info

The MIP6-Agent-Info AVP is of type Grouped as defined in Reference RFC 5447. It contains the identity of the PDNGW as defined in Reference 3GPP TS 29.272. The identity of PDN GW is either an IP address transported in MIP-Home-Agent-Address or an FQDN transported in MIP-Home-Agent-Host. FQDN shall be used if known.



The Data field of this AVP has the following ABNF grammar:

```
MIP6-Agent-Info ::= <AVP Header: 48>
    *2[ MIP-Home-Agent-Address]
    [MIP-Home-Agent-Host]
    [MIP6-Home-Link-Prefix]
    *[AVP]
```

Within the MIP6-Agent-Info AVP, if static address allocation is used, there may be either: an IPv4 address or an IPv6 address of the PGW contained in one MIP-Home-Agent-Address AVP; both IPv4 address and IPv6 address of the PGW contained in two MIP-Home-Agent-Address AVPs.

5.1.5 Service-Selection

The Service-Selection AVP is of type UTF8String defined in Reference RFC5778. This AVP shall contain either the APN Network Identifier (i.e. an APN without the Operator Network Identifier) or the wild card value as defined in Reference 3GPP TS 29.272.

The contents of the Service-Selection AVP shall be formatted as a character string composed of one or more labels separated by dots (“.”) or as the wild card APN, for example, consisting of only one ASCII label.

5.1.6 QoS-Capability

The QoS-Capability AVP contains a list of supported Quality of Service profile templates (and therefore the support of the respective parameter AVPs). This AVP is defined in IETF RFC 5777.

```
QoS-Capability ::= <AVP Header: 578>
    1*{QoS-Profile-Template}
    * [AVP]
```

5.1.7 MIP-Home-Agent-Address

The MIP-Home-Agent-Address AVP is of type Address defined in Reference RFC 4004. This AVP shall contain either IPv4 or IPv6 address of the PDN-GW, and this IP address shall be used as the PDN-GW IP address as indicated defined in Reference 3GPP TS 29.272.

5.1.8 MIP-Home-Agent-Host

The MIP-Home-Agent-Host AVP is of type Grouped and is defined in RFC 4004. This AVP shall contain a FQDN of the PDN-GW which shall be used to resolve

the PDN-GW IP address using the Domain Name Service function as defined in Reference 3GPP TS 29.272.

The Data field of this AVP has the following ABNF grammar:

```
MIP-Home-Agent-Host ::= <AVP Header: 348>
                        {Destination-Realm}
                        {Destination-Host}
                        *[AVP]
```

5.1.9 QoS-Profile-Template

The QoS-Profile-Template AVP (AVP Code 574) is of type Grouped defined in RFC 5777 and defines the namespace of the QoS profile (indicated in the Vendor-ID AVP) followed by the specific value for the profile.

The Vendor-Id AVP contains a 32-bit IANA Private Enterprise Number(PEN), and the QoS-Profile-Id AVP contains the template identifier assigned by the vendor. The vendor identifier of zero (0) is used for the IETF.

```
QoS-Profile-Template ::= <AVP Header: 574>
                        {Vendor-Id}
                        {QoS-Profile-Id}
                        *[AVP]
```

5.1.10 QoS-Profile-Id

The QoS-Profile-Id AVP (AVP Code 573) is of type Unsigned32 defined in RFC 5777 and contains a QoS profile template identifier. An initial QoS profile template is defined with value of 0 and can be found in [RFC5624]. The registry for the QoS profile templates is created with the same document.

5.1.11 QoS-Resources

The QoS-Resources AVP is of type Grouped defined in RFC 5777 and contains a list of filter policy rules.

```
QoS-Resources ::= <AVP Header: 508>
                  1*{Filter-Rule}
                  * [AVP]
```

5.1.12 Filter-Rule

The Filter-Rule AVP is of type Grouped defined in RFC 5777 and defines a specific condition and action combination.



```
Filter-Rule ::= <AVP Header: 509>
               [QoS-Profile-Template]
               *[AVP]
```

If the QoS-Profile-Template AVP is not included in the Filter-Rule AVP and the Treatment-Action AVP is set to “shape” or “mark”, then the default setting is assumed, namely, a setting of the Vendor-Id AVP to 0 (for IETF) and the QoS-Profile-Id AVP to zero (0) (for the profile defined in [RFC 5624]). Note that the content of the QoS-Parameters are defined in the respective specification defining the QoS parameters. When the Vendor-Id AVP is set to 0 (for IETF) and the QoS-Profile-Id AVP is set to zero (0), then the AVPs included in the QoS-Parameters AVP are the AVPs defined in [RFC5624].

5.1.13 Proxy-Info

The Proxy-Info AVP is of type Grouped defined in RFC 6733. This AVP shall contain the identity and local state information of the Diameter node that creates and adds it to a message.

5.1.14 Route-Record

The Route-Record AVP is of type DiameterIdentity defined in RFC 6733. The identity added in this AVP must be the same as the one received in the Origin-Host of the Capabilities Exchange message.

5.2 3GPP AVPs

The following table describes the 3GPP AVPs defined in the STa application, their AVP Code values, types and possible AVP flag values. The 3GPP AVPs have Vendor-ID= 10415.

Table 4 3GPP AVPs

Attribute Name	AVP Code	Value Type	Must	May	Should not	Must not
3GPP-Charging-Characteristics	13	UTF8String	V			M
Max-Requested-Bandwidth-DL	515	Unsigned32	M,V			
Max-Requested-Bandwidth-UL	516	Unsigned32	M,V			
Visited-Network-Identifier	600	OctetString	V			M
Supported-Features	628	Grouped	V			M



Attribute Name	AVP Code	Value Type	Must	May	Should not	Must not
Feature-List-ID	629	Unsigned32	V			M
Feature-List	630	Unsigned32	V			M
Served-Party-IP-Addresses	848	Address	M,V			
QoS-Class-Identifier	1028	Enumerated	M,V			
Allocation-Retention-Priority	1034	Grouped	V			M
Priority-Level	1046	Unsigned32	V			M
Context-Identifier	1423	Unsigned32	M,V			
APN-Configuration	1430	Grouped	M,V			
EPS-Subscribed-QoS-Profile	1431	Grouped	M,V			
VPLMN-Dynamic-Addresses-Allowed	1432	Enumerated	M,V			
AMBR	1435	Grouped	M,V			
PDN-GW-Allocation-Type	1438	Enumerated	M,V			
PDN-Type	1456	Enumerated	M,V			
Trace-Data	1458	Grouped	M,V			
Trace-Reference	1459	OctetString	M,V			
Trace-Depth	1462	Enumerated	M,V			
Trace-NE-Type-List	1463	OctetString	M,V			
Trace-Interface-List	1464	OctetString	M,V			
Trace-Event-List	1465	OctetString	M,V			
OMC-Id	1466	OctetString	M,V			
Trace-Info	1505	Grouped	V			
Emergency-Services	1538	Unsigned32	V			M, P

5.2.1 Supported-Features

The Supported-Features AVP is of type Grouped and it is defined in Reference 3GPP TS 29.229. If this AVP is present, it may inform the destination host about the features that the origin host supports. The Feature-List AVP contains a list of



supported features of the origin host. The Vendor-Id AVP and the Feature-List AVP together can identify which feature list is carried in the Supported-Features AVP. Where a Supported-Features AVP is used to identify features that have been defined by 3GPP, the Vendor-Id AVP contains the vendor ID of 3GPP.

Vendors may define proprietary features, but it is strongly recommended that the possibility is used only as the last resort. Where the Supported-Features AVP is used to identify features that have been defined by a vendor other than 3GPP, it contains the vendor ID of the specific vendor in question. If there are multiple feature lists defined by the same vendor, the Feature-List-ID AVP differentiates those lists from one another.

The destination host uses the value of the Feature-List-ID AVP to identify the feature list. Its Data field has the following ABNF grammar:

```
Supported-Features ::= <AVP Header: 628, Vendor-Id: 10415>
                        {Vendor-Id}
                        {Feature-List-ID}
                        {Feature-List}
                        *[AVP]
```

5.2.2 Feature-List-ID

The Feature-List-ID AVP is of type Unsigned32 defined in 3GPP TS 29.229 and it contains the identity of a feature list.

5.2.3 Feature-List

The Feature-List AVP is of type Unsigned32 defined in 3GPP TS 29.229. It contains a bit mask indicating the supported features of an application. When the bit set, indicates the corresponding feature is supported by the application.

5.2.4 APN-Configuration

The APN-Configuration AVP is of type Grouped defined in 3GPP TS 29.272. It contains the information related to APN configuration for a single APN.

The Data field of this AVP has the following ABNF grammar:

```
APN-Configuration ::= <AVP Header: 1430 , Vendor-Id: 10415>
                      {Context-Identifier}
                      {Service-Selection}
                      {PDN-Type}
                      *2[Served-Party-IP-Address]
                      [MIP6-Agent-Info]
                      [Visited-Network-Identifier]
                      [PDN-GW-Allocation-Type]
                      [EPS-Subscribed-QoS-Profile]
```



[VPLMN-Dynamic-Address-Allowed]
[3GPP-Charging-Characteristics]
[AMBR]
*[Specific-APN-Info]
*[AVP]

5.2.5 PDN-Type

The PDN-Type AVP is of type Enumerated defined in 3GPP TS 29.272 and indicates the address type of PDN. The following values are defined:

Table 5 PDN-Type AVP

AVP value	Description
0	IPv4: This value shall be used to indicate that the PDN can be accessed only in IPv4 mode.
1	IPv6: This value shall be used to indicate that the PDN can be accessed only in IPv6 mode.
2	IPv4v6: This value shall be used to indicate that the PDN can be accessed both in IPv4 mode, in IPv6 mode, and also from UEs supporting dualstack IPv4v6.
3	IPv4_OR_IPv6: This value shall be used to indicate that the PDN can be accessed either in IPv4 mode, or in IPv6 mode, but not from UEs supporting dualstack IPv4v6.

5.2.6 Served-Party-IP-Address

The Served-Party-IP-Address AVP defined in Reference 3GPP TS 32.299 is of type Address. It contains the IPv4 address, the IPv6 address or the IPv6 prefix of the user, if static IP address allocation is used. For the IPv6 prefix, the lower 64 bits of the address shall be set to zero.

5.2.7 Visited-Network-Identifier

The Visited-Network-Identifier AVP defined in Reference 3GPP TS 29.229 is of type OctetString. It contains an identifier of the visited network when it is received in MAR message. Otherwise it contains the identity of the network where the PDN-GW was allocated, in the case of dynamic PDN-GW assignment.

The AVP shall be encoded as defined in Reference 3GPP TS 29.272:

mnc<MNC>.mcc<MCC>.3gppnetwork.org



5.2.8 PDN-GW-Allocation-Type

The PDN-GW-Allocation-Type AVP is of type Enumerated defined in 3GPP TS 29.212 and indicates whether the PDN GW address is statically allocated or dynamically selected by other nodes.

The following values are defined:

Table 6 PDN-GW-Allocation-Type AVP

AVP value	Description
0	STATIC
1	DYNAMIC

5.2.9 EPS-Subscribed-QoS-Profile

The EPS-Subscribed-QoS-Profile AVP is of type Grouped defined in 3GPP TS 29.272 and contains the bearer-level QoS parameters (QoS Class Identifier and Allocation Retention Priority) associated to the default bearer for an APN. See Reference 3GPP TS 29.272.

The Data field of this AVP has the following ABNF grammar:

```
EPS-Subscribed-QoS-Profile ::= <AVP Header: 1431, Vendor-Id: 10415>
                               {QoS-Class-Identifier}
                               {Allocation-Retention-Priority}
                               *[AVP]
```

5.2.10 VPLMN-Dynamic-Address-Allowed

The VPLMN-Dynamic-Address-Allowed AVP is of type Enumerated defined in 3GPP TS 29.272. It indicates whether the UE is allowed to use a dynamic address allocated in the Visited PLMN (VPLMN). The following values are defined:

Table 7 VPLMN-Dynamic-Address-Allowed AVP

AVP value	Description
0	NOT ALLOWED
1	ALLOWED

5.2.11 3GPP-Charging-Characteristics

The 3GPP-Charging-Characteristics AVP is of type UTF8String. It contains the Charging Characteristics is defined in Reference 3GPP TS 29.061.

The structure of the Charging Characteristics value according to Reference 3GPP TS 32.299 is as follows:



Table 8 3GPP-Charging-Characteristics AVP

8	7	6	5	4	3	2	1	
B4	B3	B2	B1	P3	P2	P1	P0	octet 1
B12	B11	B10	B9	B8	B7	B6	B5	octet 2

Bits P0-P3 refer to the Charging Characteristics Profile Index and B1-B12 may be used by the operator for non-standardised behavior.

Each octet of the Charging Characteristics value is represented via 2 UTF-8 encoded characters in the 3GPP-Charging-Characteristics AVP, defining its hexadecimal representation. For example, if P3 and P1 are set to 1, and all the B bits are set to 0, the value of octet 1 is 10, which hexadecimal representation is 0x0A, and in text form is 0A. Octet 2 is set to 0, represented as 0x00 in hexadecimal and “00” in text, so the 3GPP-Charging-Characteristics value in UTF-8 would be 0A00.

5.2.12 AMBR

The AMBR AVP is of type Grouped defined in 3GPP TS 29.212, and contains AVPs that indicate the aggregate maximum bitrates requested for the uplink and downlink bandwidth.

The Data field of this AVP has the following ABNF grammar:

```
AMBR ::= <AVP Header: 1435, Vendor-Id:10415>
        {Max-Requested-Bandwidth-UL}
        {Max-Requested-Bandwidth-DL}
        *[AVP]
```

5.2.13 Specific-APN-Info

The Specific-APN-Info AVP is of type Grouped defined in 3GPP TS 29.272. It shall only be present in the APN configuration when the APN is a wild card APN. It shall contain the APN which is not present in the subscription context but the UE is authorized to connect to and the identity of the registered PDN-GW and optionally the PLMN Id of the PDN GW.

```
Specific-APN-Info ::= <AVP Header : 1472, Vendor Id: 10415>
                     {Service-Selection}
                     [MIP6-Agent-Info]
                     [Visited-Network-Identifier]
                     *[AVP]
```



5.2.14 QoS-Class-Identifier

The QoS-Class-Identifier AVP is of type Enumerated defined in 3GPP TS 29.212, and it identifies a set of IP-CAN specific QoS parameters that define the authorized QoS, excluding the applicable bitrates for the IP-CAN bearer or service flow.

5.2.15 Allocation-Retention-Priority

The Allocation-Retention-Priority AVP is of type Grouped defined in 3GPP TS 29.212. It indicates Priority of Allocation and Retention for the corresponding Access Point Name (APN) configuration within the Priority-Level AVP. The Data field of this AVP has the following ABNF grammar:

```
Allocation-Retention-Priority ::= <AVP Header: 1034, Vendor-Id:
                                10415>
                                {Priority-Level}
                                *[AVP]
```

5.2.16 Max-Requested-Bandwidth-DL

The Max-Requested-Bandwidth-DL AVP is of type Unsigned32 defined in 3GPP TS 29.124 and it indicates the maximum requested bandwidth in bits per second for a downlink IP flow. The bandwidth contains all the overhead coming from the IP-layer and the layers above, for instance: IP, UDP, RTP and RTP payload.

5.2.17 Max-Requested-Bandwidth-UL

The Max-Requested-Bandwidth-UL AVP is of type Unsigned32 defined in 3GPP TS 29.124, and it indicates the maximum requested bandwidth in bits per second for an uplink IP flow. The bandwidth contains all the overhead coming from the IP-layer and the layers above, for instance: IP, UDP, RTP and RTP payload.

5.2.18 Priority-Level

The Priority-Level AVP is of type Unsigned 32 defined in 3GPP TS 29.212. The priority level defines the relative importance of a resource request. The AVP is used for deciding whether a bearer establishment or modification request can be accepted or needs to be rejected in case of resource limitations. The AVP can also be used to decide which existing bearers to pre-empt during resource limitations. The priority level defines the relative importance of a resource request. Values 1 to 15 are defined, with value 1 as the highest level of priority.

5.2.19 Trace-Info

The Trace-Data AVP is of type Grouped defined in 3GPP TS 29.273. This AVP shall contain the information related to subscriber and equipment trace function and the required action, i.e. activation of deactivation.

AVP format:

```
Trace-Info ::= <AVP header: 1505 10415>
               [Trace-Data]
               [Trace-Reference]
               *[AVP]
```

Either the Trace-Data or the Trace-Reference AVP shall be included. When trace activation is needed, Trace-Data AVP shall be included, while the trace deactivation request shall be signaled by including the Trace-Reference directly under the Trace-Info.

5.2.20 Trace-Data

The Trace-Data AVP is of type Grouped defined 3GPP TS 29.272, while its contents is defined in 3GPP TS 32.422.

This AVP shall contain the information related to trace function.

AVP format:

```
Trace-Data ::= <AVP header: 1458 10415>
               {Trace-Reference}
               {Trace-Depth}
               {Trace-NE-Type-List}
               [Trace-Interface-List]
               {Trace-Event-List}
               [OMC-Id]
               {Trace-Collection-Entity}
               *[AVP]
```

5.2.21 Trace-Reference

The Trace-Reference AVP is of type OctetString defined 3GPP TS 29.272. This AVP shall contain the concatenation of MCC, MNC and Trace ID, where the Trace ID is a 3 byte Octet String. See 3GPP TS 32.422.

5.2.22 Trace-Depth

The Trace-Depth AVP is of type Enumerated defined 3GPP TS 29.272. The possible values are those defined in 3GPP TS 32.422 for Trace Depth.



5.2.23 Trace-NE-Type-List

The Trace-NE-Type-List AVP is of type OctetString defined 3GPP TS 29.272. Octets are coded according to 3GPP TS 32.422.

5.2.24 Trace-Interface-List

The Trace-Interface-List AVP is of type OctetString defined 3GPP TS 29.272. Octets are coded according to 3GPP TS 32.422.

5.2.25 Trace-Event-List

The Trace-Event-List AVP is of type OctetString defined 3GPP TS 29.272. Octets are coded according to 3GPP TS 32.422.

5.2.26 OMC-Id

The OMC-Id AVP is of type OctetString. Octets are coded according to 3GPP TS 29.002.

5.2.27 Trace-Collection-Entity

The Trace-collection-Entity AVP is of type Address and contains the IPv4 or IPv6 address of the Trace Collection Entity, as defined in 3GPP TS 32.422, clause 5.9.

5.2.28 Emergency-Services

The Emergency-Services AVP of type Unsigned32 and it shall contain a bitmask. The PGW shall include this information element, with the Emergency-Indication bit set, during the establishment of an emergency PDN connection.

Note: Bits not defined in this table shall be cleared by the sender and discarded by the receiver.

The meaning of the bits is defined in Table 9:

Table 9 Emergency-Services

Bit	Name	Description
0	Emergency-Indication	This bit, when set, indicates a request to establish a PDN connection for emergency services.





6 Formal Syntax

This interface uses the following syntax:

- Diameter Base Protocol RFC 3588, Reference [4], is used to describe messages and AVPs.





7

Diameter Error Handling

Table 10 Diameter Error Handling

Error Scenario	Return Code
For initial authorization request, Auth-Request-Type is not AUTHORIZE_ONLY, MIP6-Feature-Vector AVP is not PMIP6_SUPPORTED.	Result-Code = DIAMETER_UNABLE_TO_COMPLY
For initial authorization request, user profile exist, STa session is not exist	Result-Code = DIAMETER_AUTHORIZATION_REJECTED
For initial authorization request, user profile and Session are exist, request APN is not included in the APN list from HSS.	Result-Code = DIAMETER_AUTHORIZATION_REJECTED
For initial authorization request, user profile is not exist, AAA server fetch user profile from HSS.	<ul style="list-style-type: none"> For AAA redirection, Result-Code = DIAMETER_REDIRECT_INDICATION For user unknown, Experimental-Result-Code = DIAMETER_ERROR_USER_UNKNOWN Success, Result-Code = DIAMETER_AUTHORIZATION_REJECTED
For initial authorization request, when AAA update the PDN information to HSS, HSS return DIAMETER_ERROR_USER_UNKNOWN.	Experimental-Result-Code = DIAMETER_ERROR_USER_UNKNOWN
For initial authorization request, when AAA update the PDN information to HSS, HSS return DIAMETER_ERROR_IDENTITY_ALREADY_REGISTERED.	Result-Code = DIAMETER_REDIRECT_INDICATION
For initial authorization request, when AAA update the PDN information to HSS, HSS return DIAMETER_ERROR_IDENTITY_NOT_REGISTERED.	Experimental-Result-Code = DIAMETER_ERROR_IDENTITY_NOT_REGISTERED
For initial authorization request, when AAA update the PDN information to HSS, HSS return other errors.	Result-Code = DIAMETER_UNABLE_TO_COMPLY





8 Related Standards

This section states the related standards and explains any deviations from them.

- 3GPP EPS AAA interfaces 3GPP TS 29.273 version 12.5.0/13.6.0
- Diameter Base Protocol RFC 3588
- Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA) RFC 4187
- Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA') RFC 5448
- Extensible Authentication Protocol (EAP) RFC 3748
- Diameter Extensible Authentication Protocol (EAP) Application RFC 4072
- Universal Mobile Telecommunications System (UMTS); LTE; Architecture enhancements for non-3GPP accesses (3GPP TS 23.402 version 9.6.0 Release 9)





Reference List

IPWorks Library Documents

- [1] Glossary of Terms and Acronyms
- [2] Trademark Information
- [3] Typographic Conventions

Standards

- [4] [Diameter Base Protocol RFC 3588](#)
- [5] [Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement \(EAP-AKA\) RFC 4187](#)
- [6] [Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement \(EAP-AKA'\) RFC 5448](#)
- [7] [Extensible Authentication Protocol \(EAP\) RFC 3748](#)
- [8] [Diameter Extensible Authentication Protocol \(EAP\) Application RFC 4072](#)
- [9] [Universal Mobile Telecommunications System \(UMTS\); LTE3GPP EPS AAA interfaces; Evolved Packet System \(EPS\); \(3GPP TS 29.273 version 12.5.0 Release 12/ version 13.6.0 Release 13](#)
- [10] [Universal Mobile Telecommunications System \(UMTS\); LTE; Architecture enhancements for non-3GPP accesses \(3GPP TS 23.402 version 9.6.0 Release 9\)](#)