

Radius STaPlus Interface between IPWorks AAA Server and Non-3GPP Access GW

INTERWORK DESCRIPTION

Copyright

© Ericsson AB 2017. 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 Trademark 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	Authentication/Authorization	5
3.2	Accounting	11
3.3	Disconnect Message	12
4	Information Model	15
4.1	General	15
4.2	RADIUS Message in STa+ Interface	15
4.3	EAP Message in STa+ Interface	18
5	Formal Syntax	23
6	Related Standards	25
7	Appendix	27
7.1	Offload-Indication Attribute	27
7.2	GTP-Tunnel-Data Attribute	27
	Reference List	31





1 Introduction

This document describes the STa+ reference point between the IPWorks AAA Server and trusted non-3GPP Access Network.

This document is focus on the ENIW solution for Wi-Fi AAA.

Scope

The STa+ interface is used by IPWorks AAA server to interact with trusted Non-3GPP Access Network. This interface works between IPWorks AAA server and WMG.

This document covers the following topics:

- Interface Overview
- Procedures
- Information Model
- Related Standards

1.1 Prerequisites

Not applicable.

1.2 Related Information

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

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

The STa+ interface is the customized reference point between WMG and IPWorks AAA in ENIW solution. It supports RADIUS protocol conveyed EAP authentication method and authorization. The related standard can be found in the section References.





EAP-AKA/AKA'	EAP-SIM	EAP-MD5
EAP		
RADIUS		
UDP		

Figure 2 Protocol Stack Used in ENIW Solution



3 Procedures

This section describes the processes implemented for the STa+ interface:

- Authentication and Authorization
- Accounting
- Disconnect Message

3.1 Authentication/Authorization

IPWorks AAA server supports SIM (EAP-SIM/AKA/AKA') authentication methods for trusted non-3GPP access in STa+ reference point. The figures in the following sections show the basic authentication procedures.



3.1.1

EAP-AKA Full Authentication

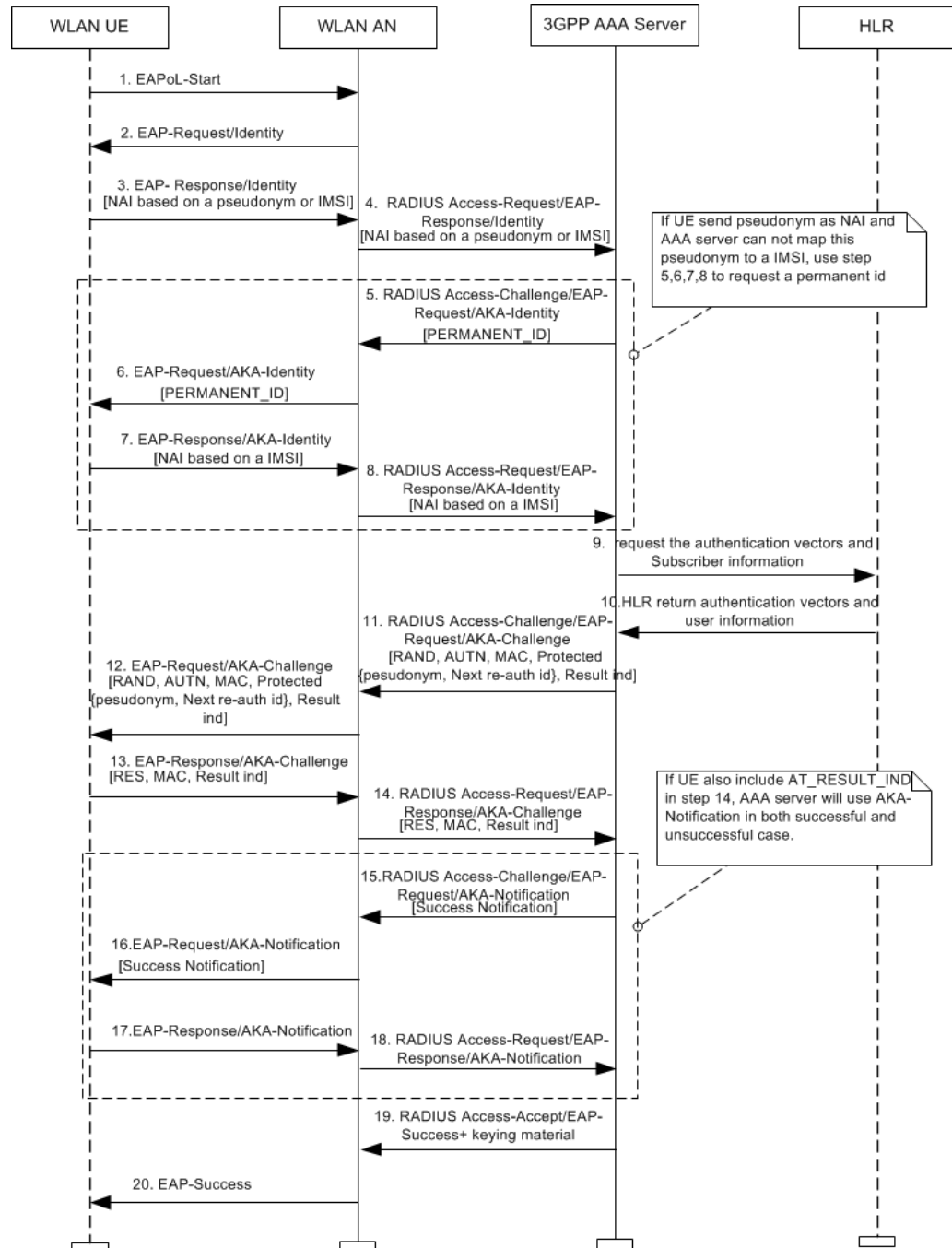


Figure 3 EAP-AKA Full Authentication Flows

3.1.2 EAP-AKA Fast Re-authentication

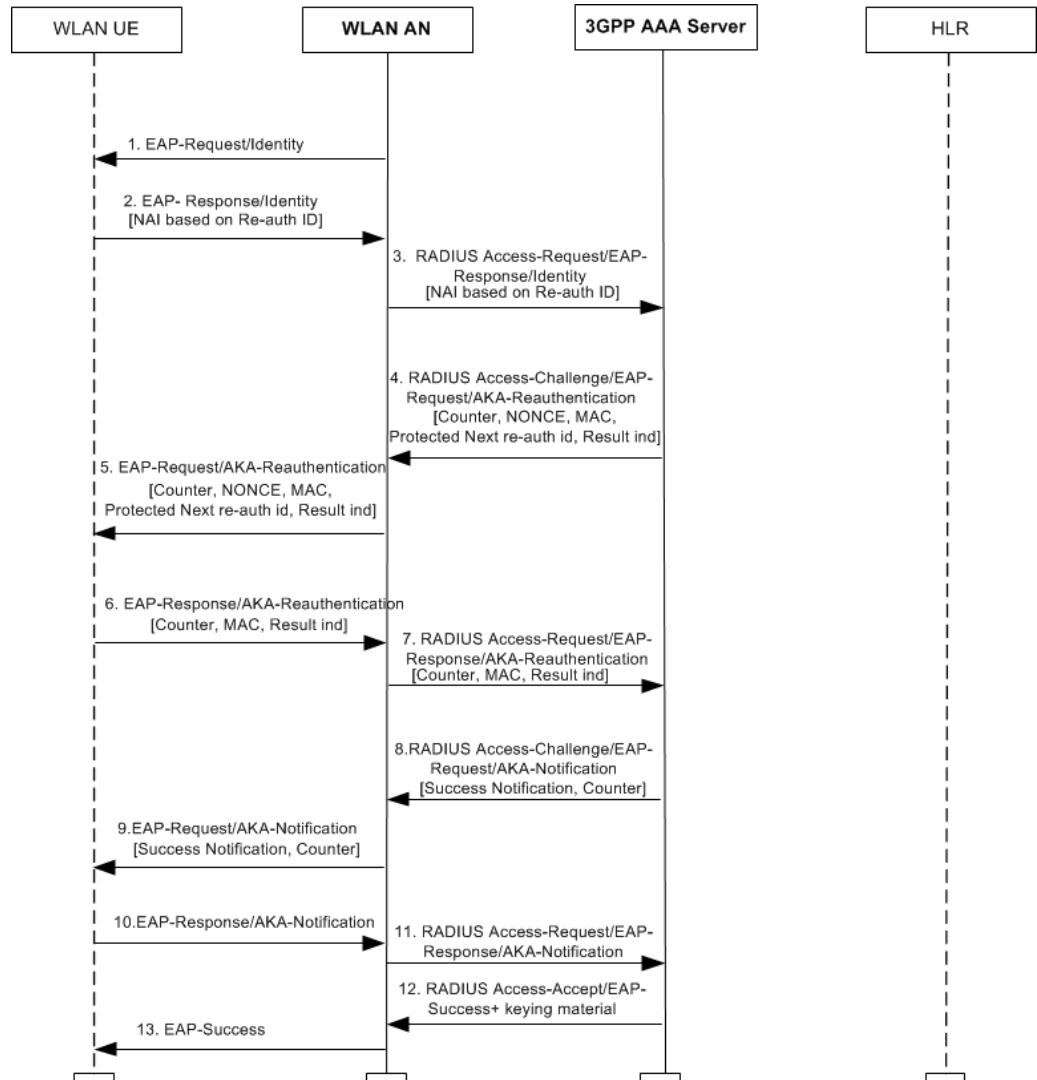


Figure 4 EAP-AKA Fast Re-authentication Flows



3.1.3 EAP-AKA' Full Authentication

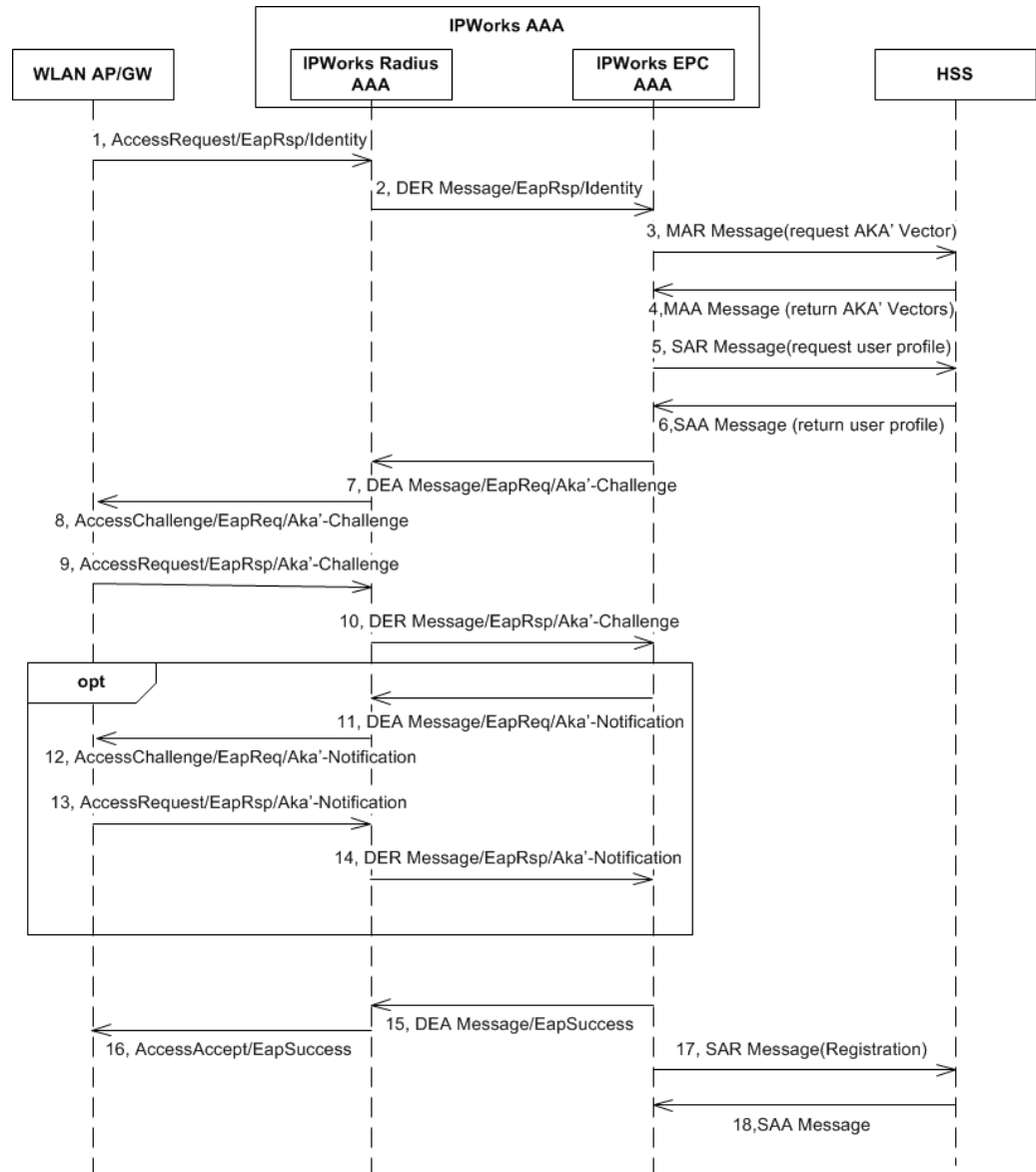


Figure 5 EAP-AKA Prime Full authentication Flows

3.1.4 EAP-AKA' Fast Re-authentication



Figure 6 EAP-AKA Prime Fast Re-authentication Flows



3.1.5

EAP-SIM Full Authentication

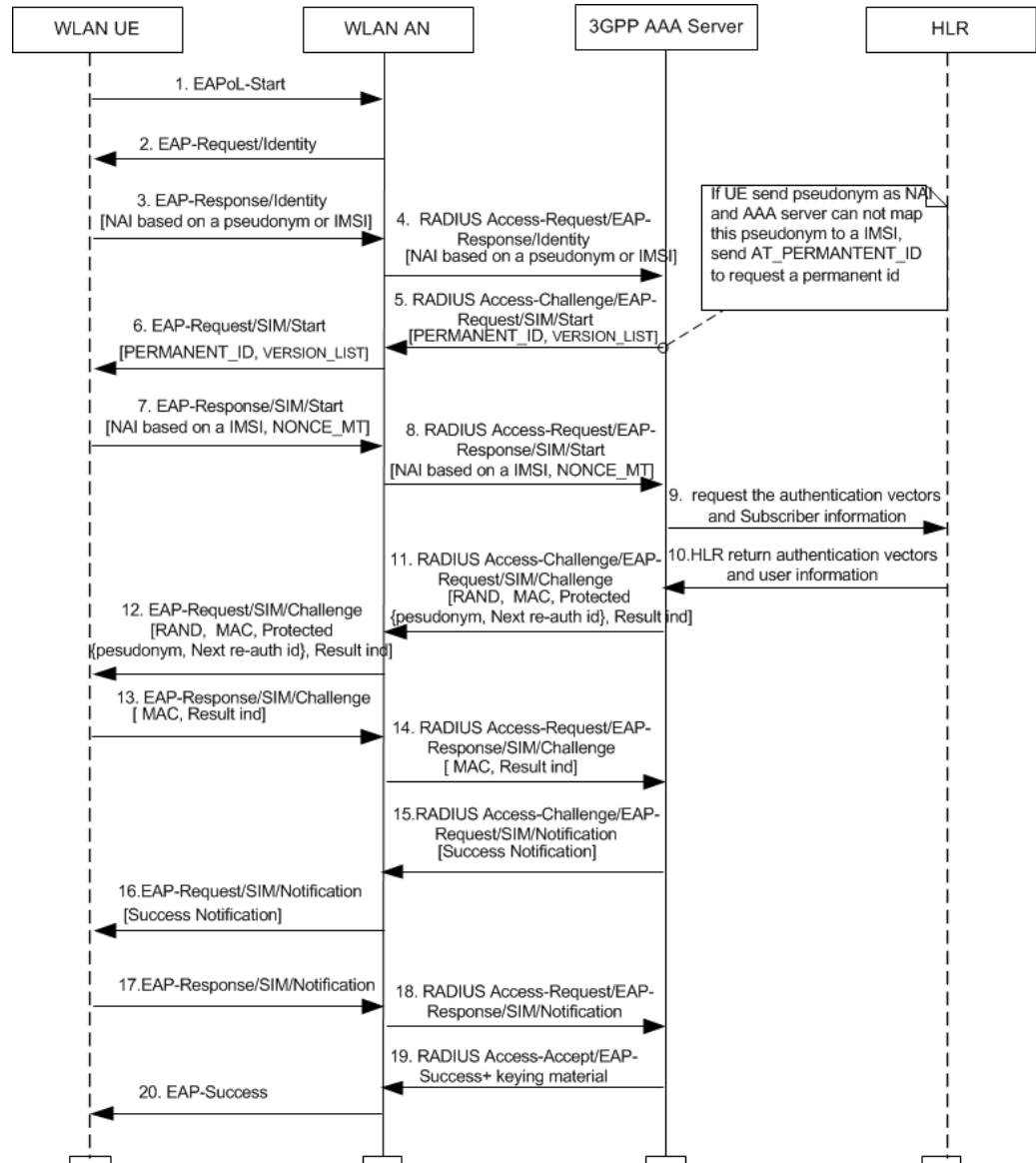


Figure 7 EAP-SIM Full Authentication Flows

3.1.6 EAP-SIM Fast Re-authentication

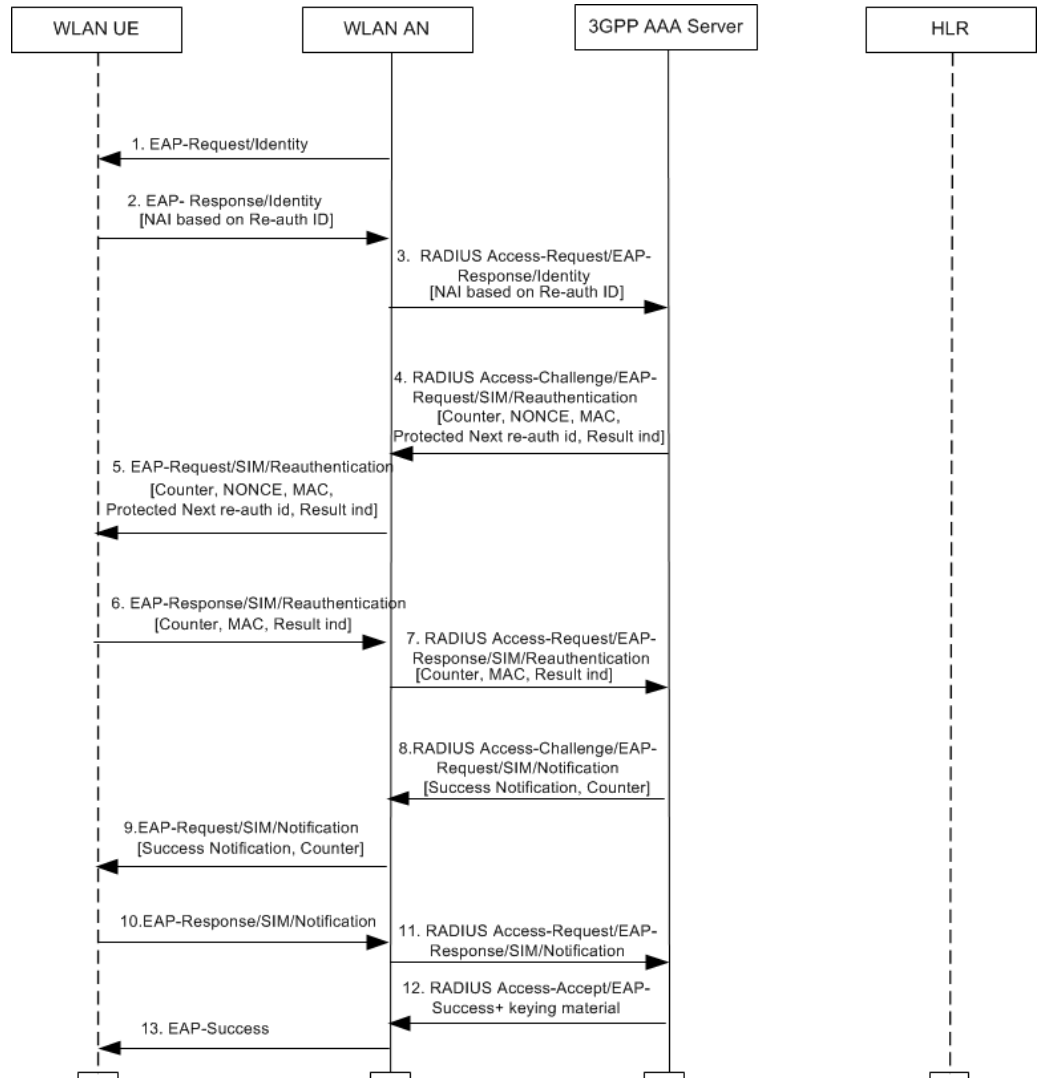


Figure 8 EAP-SIM Fast Re-authentication Flows

3.2 Accounting

Accounting is used to collect the resource usage information for analysis or billing purposes.

- Accounting-Request START message means that a user session has started.
- Accounting-Request Interim-Update is used to update the user session information.
- Accounting-Request STOP means that the user session is terminated.

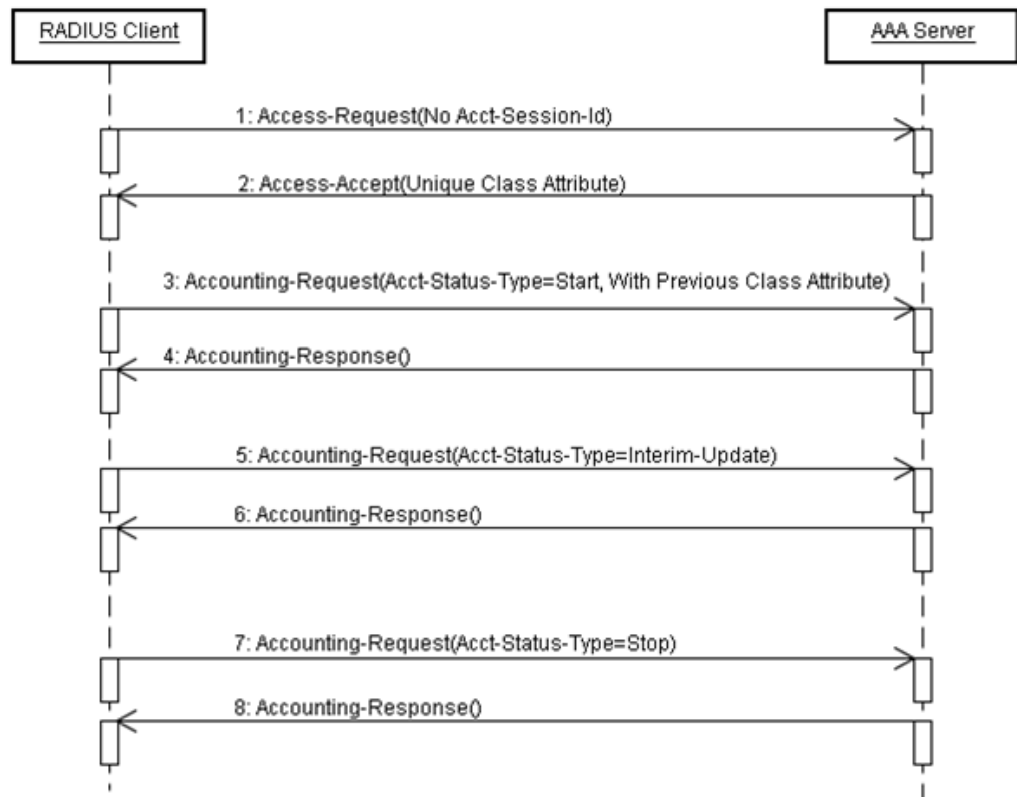


Figure 9 Accounting

3.3 Disconnect Message

The AAA server could receive the status change of related subscribers from HLR and decide whether need to terminate the active session. If the WLAN accessible flag for user has changed or the user logged on from the other server, AAA server may issue the Disconnect-Request messages to notify an NAS about the termination of the accounting sessions.

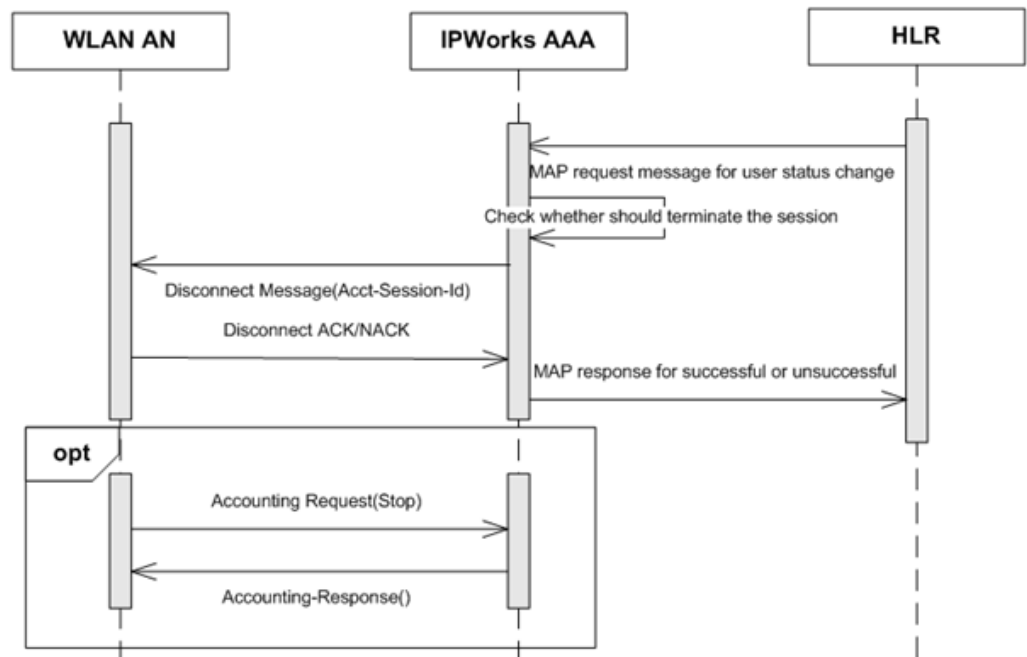


Figure 10 Terminate Session





4 Information Model

This section describes the information model including mandatory and optional parameters of each service operation.

4.1 General

The convention in Table 2 is used to indicate how the attribute is present in a message:

Table 2 Convention

Attribute	Description
0	This attribute MUST NOT be present in message.
0+	Zero or more instances of this attribute MAY be present in message.
0-1	Zero or one instance of this attribute MAY be present in message.
1	Exactly one instance of this attribute MUST be present in message.
0*	The attribute is not included in the message in cases specified in the related RFC, but MAY be included in the future versions of the protocol.

The format <Attr#>/<Vendor-ID>-<Sub-attr#> is used for the vendor-specific subattributes. For example, 26/311-28 is the code of Microsoft vendor-specific RADIUS attribute MS-Primary-DNS-Server.

4.2 RADIUS Message in STa+ Interface

The messages supported by the STa+ interface comply with the RADIUS data format that is defined in RFC 2865, RFC5176, and RFC 2866. They can be divided into the following groups:

- Authentication/Authorization: Access-Request, Access-Accept, Access-Reject, Access-Challenge
- DM: Disconnect-Request, Disconnect-ACK/NAK
- Accounting: Accounting-Request, Accounting-Response

The following sections list the attributes which be used in the messages of STa+ interface. If the messages also include other attributes according to related protocols, AAA server bypasses them.



4.2.1 Authentication/Authorization Message Attributes

Table 3 contains the authentication or authorization message attributes for EAP-AKA/AKA'.

Table 3 Attributes Supported by Authentication/Authorization Message for STa+ Interface

Attr #	Attribute Name	Access-Request	Access-Accept	Access-Reject	Access-Challenge	Description
1	User-Name ⁽¹⁾	1	1	1	1	Section 5.1, RFC 2865
4	NAS-IP-Address	1	0	0	0	Section 5.4, RFC 2865
31	Calling-Station-ID	1	0	0	0	Section 5.31, RFC 2865
30	Called-Station-ID	1	0	0	0	Section 5.30, RFC 2865
32	NAS-Identifier	1	0	0	0	Section 5.32, RFC 2865
87	NAS-Port-Id	1	0	0	0	Section 5.32, RFC 2865
24	State	0-1	0-1	0	1	Section 5.7, RFC 2865 Section 2.1.1, RFC 5080
27	Session-Timeout	0	1	0-1	0	Section 5.27, RFC 2865 Section 3.17, RFC 3580
29	Termination-Action	0	1	0-1	0	Section 5.29, RFC 2865 Section 3.17, RFC 3580
79	EAP-Message	1+	1+	1+	1+	Section 3.1, RFC 3579



Attr #	Attribute Name	Access-Request	Access-Accept	Access-Reject	Access-Challenge	Description
80	Message-Authenticator	1	1	1	1	Section 3.2, RFC 3579
89	Chargeable-User-Identity ⁽²⁾	0-1	1	0	0	Section 2.2, RFC 4372
85	Acct-Interim-Interval ⁽²⁾	0	1	0	0	Section 5.16, RFC 2869
25	class ⁽²⁾	0	0+	0	0	Section 5.25, RFC 2865
26-193-225	Offload-Indication ⁽²⁾⁽³⁾	0	0-1	0	0	See Section 7.1
26-193-226	GTP-Tunnel-Data ⁽²⁾⁽⁴⁾	0	0-1	0	0	See Section 7.2
26-10415-13	3GPP-Charging-Characteristics ⁽²⁾	0	0-1	0	0	3GPP TS 29.061 v9.0.0, Section 16.4.7.2

(1) When the Trusted WiFi Support feature is enabled, the value of User-Name is only set as IMSI; otherwise set as NAI.

(2) This attribute is not available for EAP-MD5.

(3) The AVP Offload-Indication is included in the Access-Accept only when the Trusted Wi-Fi Support feature is enabled.

(4) The AVP GTP-Tunnel-Data is included in the Access-Accept in when the subscriber is authorized as s2a access.

4.2.2

DM Message Attributes

Table 4 Attributes Supported by DM Message for STa+ Interface

Attr #	Attribute Name	Disconnect-Request	Disconnect-ACK	Disconnect-NAK	Description
1	User-Name ⁽¹⁾	1	0	0	Section 5.1, RFC 2865
4	NAS-IP-Address	1	0	0	Section 5.4, RFC 2865
32	NAS-Identifier	1	0	0	Section 5.32, RFC 2865
44	Acct-Session-Id	1	0	0	Section 5.5, RFC 2866
80	Message-Authenticator	1	1	1	Section 3.2, RFC 3579

(1) The value of User-Name attribute is the NAI in the Access-Accept which be sent in the last successful authentication.



4.2.3 Accounting Message Attributes

Table 5 Accounting Message Attributes

Attr #	Attribute Name	Accountin g-Request START	Accountin g-Request STOP	Accounting- Request Inte rim-Update	Description
1	User-Name	1	1	1	Section 5.1, RFC 2865
4	NAS-IP-Addr ess	1	1	1	Section 5.4, RFC 2865
31	Calling-Statio n-ID	1	1	1	Section 5.31, RFC 2865
30	Called-Statio n-ID	0-1	0-1	0-1	Section 5.30, RFC 2865
32	NAS-Identifie r	1	1	1	Section 5.32, RFC 2865
87	NAS-Port-Id	1	1	1	Section 5.17, RFC 2869
40	Acct-Status- Type	1	1	1	Section 5.1, RFC 2866
42	Acct-Input-O ctets	0	1	1	Section 5.3, RFC 2866
43	Acct-Output- Octets	0	1	1	Section 5.4, RFC 2866
44	Acct-Session -Id	1	1	1	Section 5.5, RFC 2866
89	Chargeable- User-Identity	0-1	0-1	0-1	Section 2.2, RFC 4372
46	Acct-Session -Time	0	1	1	Section 5.7, RFC 2866
47	Acct-Input-P ackets	0	1	1	Section 5.8, RFC 2866
48	Acct-Output- Packets	0	1	1	Section 5.9, RFC 2866
52	Acct-Input-Gi gawords	0	1	1	Section 5.1, RFC 2869
53	Acct-Output- Gigawords	0	1	1	Section 5.2, RFC 2869
27	Session-Tim eOut	1	0	0	Section 5.27, RFC 2865
25	class	0+	0+	0+	Section 5.25, RFC 2865
49	Acct-Termina te-Cause	0	1	0	Section 5.10, RFC 2866

4.3 EAP Message in STa+ Interface

In STa+ interface, the following EAP packets are used for authentication:

- Request(1)



- Response(2)
- Success(3)
- Failure(4)

The following EAP types are used in EAP Request/Response exchanges for the STa+ interface.

- EAP-Identity(1)
- EAP-Notification(2)
- EAP-Nak(3)
- EAP-AKA(23)
- EAP-SIM(18)
- EAP-AKA'(50)

4.3.1 EAP-AKA Message in STa+ Interface

The following table provides a guide to which attributes may be found in which kinds of messages, and in what quantity. Messages are denoted with numbers in parentheses as follows:

- EAP-Request/AKA-Identity(1)
- EAP-Response/AKA-Identity(2)
- EAP-Request/AKA-Challenge(3)
- EAP-Response/AKA-Challenge(4)
- EAP-Request/AKA-Notification(5)
- EAP-Response/AKA-Notification(6)
- EAP-Response/AKA-Client-Error(7)
- EAP-Request/AKA-Reauthentication(8)
- EAP-Response/AKA-Reauthentication(9)
- EAP-Response/AKA-Authentication-Reject(10)
- EAP-Response/AKA-Synchronization-Failure(11)

The column denoted with "E" indicates whether the attribute is a nested attribute that **MUST** be included within AT_ENCR_DATA.

**Table 6 EAP-AKA Message in STa+ Interface**

Attribute Name	1	2	3	4	5	6	7	8	9	10	11	E	Description
AT_PERMA NENT_ID_R EQ	0-1	0	0	0	0	0	0	0	0	0	0	No	Section 10.2, RFC 4187
AT_ANY_ID_ REQ	0-1	0	0	0	0	0	0	0	0	0	0	No	Section 10.3, RFC 4187
AT_FULLAU TH_ID_REQ	0-1	0	0	0	0	0	0	0	0	0	0	No	Section 10.4, RFC 4187
AT_IDENTIT Y	0	0-1	0	0	0	0	0	0	0	0	0	No	Section 10.5, RFC 4187
AT_RAND	0	0	1	0	0	0	0	0	0	0	0	No	Section 10.6, RFC 4187
AT_AUTN	0	0	1	0	0	0	0	0	0	0	0	No	Section 10.7, RFC 4187
AT_RES	0	0	0	1	0	0	0	0	0	0	0	No	Section 10.8, RFC 4187
AT_AUTS	0	0	0	0	0	0	0	0	0	0	1	No	Section 10.9, RFC 4187
AT_NEXT_P SEUDONYM	0	0	0-1	0	0	0	0	0	0	0	0	Yes	Section 10.10, RFC 4187
AT_NEXT_R EAUTH_ID	0	0	1	0	0	0	0	0-1	0	0	0	Yes	Section 10.11, RFC 4187
AT_IV	0	0	0-1	0*	0-1	0-1	0	1	1	0	0	No	Section 10.12, RFC 4187
AT_ENCR_D ATA	0	0	0-1	0*	0-1	0-1	0	1	1	0	0	No	Section 10.12, RFC 4187
AT_PADDIN G	0	0	0-1	0*	0-1	0-1	0	0-1	0-1	0	0	Yes	Section 10.12, RFC 4187
AT_CHECK CODE	0	0	0	0	0	0	0	0	0	0	0	No	Section 10.13, RFC 4187
AT_RESULT _IND	0	0	0-1	0-1	0	0	0	0-1	0-1	0	0	No	Section 10.14, RFC 4187
AT_MAC	0	0	1	1	0-1	0-1	0	1	1	0	0	No	Section 10.15, RFC 4187
AT_COUNT ER	0	0	0	0	0-1	0-1	0	1	1	0	0	Yes	Section 10.16, RFC 4187
AT_COUNT ER_TOO_S MALL	0	0	0	0	0	0	0	0	0-1	0	0	Yes	Section 10.17, RFC 4187
AT_NONCE_ S	0	0	0	0	0	0	0	1	0	0	0	Yes	Section 10.18, RFC 4187



Attribute Name	1	2	3	4	5	6	7	8	9	10	11	E	Description
AT_NOTIFICATION	0	0	0	0	1	0	0	0	0	0	0	No	Section 10.19, RFC 4187
AT_CLIENT_ERROR_CODE	0	0	0	0	0	0	1	0	0	0	0	No	Section 10.20, RFC 4187

4.3.2 EAP-AKA' Message in STa+ Interface

The EAP-AKA' is a small revision method of the EAP-AKA message originally defined in RFC4187. It keeps using the same EAP-AKA message types and attribute as described in Section 4.3.1 on page 19 except the attributes in Table 7.

Table 7 EAP-AKAPrime Message in STa+ Interface

Attribute Name	1	2	3	4	5	6	7	8	9	10	11	E	Description
AT_KDF_INPUT	0	0	1	0	0	0	0	0	0	0	0	No	Section 3.1, RFC 5448
AT_KDF	0	0	1	0	0	0	0	0	0	0	0	No	Section 3.2, RFC 5448

4.3.3 EAP-SIM Message in STa+ Interface

Table 8 provides a guide to which attributes may be found in which kinds of messages, and in what quantity. Messages are denoted with numbers in parentheses as follows:

- EAP-Request/SIM/Start(1)
- EAP-Response/SIM/Start(2)
- EAP-Request/SIM/Challenge(3)
- EAP-Response/SIM/Challenge(4)
- EAP-Request/SIM/Notification(5)
- EAP-Response/SIM/Notification(6)
- EAP-Response/SIM/Client-Error(7)
- EAP-Request/SIM/Re-authentication(8)
- EAP-Response/SIM/Re-authentication(9)

**Table 8 EAP-SIM Message in STa+ Interface**

Attribute Name	1	2	3	4	5	6	7	8	9	Encr	Skip	Description
AT_VERSION_LIST	1	0	0	0	0	0	0	0	0	No	No	Section 10.2, RFC 4186
AT_SELECTED_VERSION	0	0-1	0	0	0	0	0	0	0	No	No	Section 10.3, RFC 4186
AT_NONCE_MT	0	0-1	0	0	0	0	0	0	0	No	No	Section 10.4, RFC 4186
AT_PERMANENT_ID_REQ	0-1	0	0	0	0	0	0	0	0	No	No	Section 10.5, RFC 4186
AT_ANY_ID_REQ	0-1	0	0	0	0	0	0	0	0	No	No	Section 10.6, RFC 4186
AT_FULLAUTH_ID_REQ	0-1	0	0	0	0	0	0	0	0	No	No	Section 10.7, RFC 4186
AT_IDENTITY	0	0-1	0	0	0	0	0	0	0	No	No	Section 10.8, RFC 4186
AT_RAND	0	0	1	0	0	0	0	0	0	No	No	Section 10.9, RFC 4186
AT_NEXT_PSEUDONYM	0	0	0-1	0	0	0	0	0	0	Yes	Yes	Section 10.10, RFC 4186
AT_NEXT_REAUTH_ID	0	0	1	0	0	0	0	0-1	0	Yes	Yes	Section 10.11, RFC 4186
AT_IV	0	0	0-1	0*	0-1	0-1	0	1	1	No	Yes	Section 10.12, RFC 4186
AT_ENCR_DATA	0	0	0-1	0*	0-1	0-1	0	1	1	No	Yes	Section 10.12, RFC 4186
AT_PADDING	0	0	0-1	0*	0-1	0-1	0	0-1	0-1	Yes	No	Section 10.12, RFC 4186
AT_RESULT_IND	0	0	1	0-1	0	0	0	0-1	0-1	No	Yes	Section 10.13, RFC 4186
AT_MAC	0	0	1	1	0-1	0-1	0	1	1	No	No	Section 10.14, RFC 4186
AT_COUNTER	0	0	0	0	0-1	0-1	0	1	1	Yes	No	Section 10.15, RFC 4186
AT_COUNTER_TOO_SMALL	0	0	0	0	0	0	0	0	0-1	Yes	No	Section 10.16, RFC 4186
AT_NONCES	0	0	0	0	0	0	0	1	0	Yes	No	Section 10.17, RFC 4186
AT_NOTIFICATION	0	0	0	0	1	0	0	0	0	No	No	Section 10.18, RFC 4186
AT_CLIENT_ERROR_CODE	0	0	0	0	0	0	1	0	0	No	No	Section 10.19, RFC 4186



5 Formal Syntax

Not applicable.





6 Related Standards

The protocols and standards in Table 9 specified the behavior of STa+ interface.

Table 9 Related Standards

Reference Interface	Standard Version
The basic function of Wa interface	3GPP system to WLAN interworking, TS 23.234 V9.0.0
The RADIUS packets exchange process	RFC2865
The RADIUS attributes used in authentication	RFC3579, RFC2869, RFC5080
The RADIUS disconnect message usage	RFC5176
The Accounting message usage	RFC2866
The EAP message usage	RFC3579
The EAP-AKA authentication message exchange	RFC4187
The EAP-AKA' authentication message exchange	RFC5448





7 Appendix

7.1 Offload-Indication Attribute

The Offload-Indication is of type integer (32). Two possible values are provided:

- 0: Indicates that the NSWO (namely the LBO) is applied.
- 1: Indicates that the EPC is applied.

Note: If the Offload-Indication value is set as 1, the GTP-Tunnel-Data attribute is included in the *Access-Accept*. Otherwise the GTP-Tunnel-Data attribute is not included in the *Access-Accept*.

7.2 GTP-Tunnel-Data Attribute

The GTP-Tunnel-Data attribute is of type String. If GTP-Tunnel-Data is received by WiFi-GW, the WiFi-GW tries to establish a GTP tunnel based on the information provided by SAPC.

Table 10 Format of GTP-Tunnel-Data

	Bits								Comment
Octets	8	7	6	5	4	3	2	1	
1	Spare				PDN type				PDN Type
2	Restriction type value								APN restriction
6-Mar	APN-AMBR for uplink								Aggregate Maximum Bit Rate (AMBR)
10-Jul	APN-AMBR for downlink								
11	Spare	PCL	PL				Spare	PVI	
12	Label (QCI)								
13-17	Maximum bit rate for uplink								
18-22	Maximum bit rate for downlink								
23-27	Guaranteed bit rate for uplink								
28-32	Guaranteed bit rate for downlink								
33	Spare								Bearer Quality of Service
34-35	Charging characteristics value								Charging Characteristics
36	Length = a								APN name
37 to (37+a-1)	Access Point Name (APN)								
37+a	Length = b								Primary
38+a to (38+a+b-1)	IPv4 or IPv6 Address								PDN-GW address



	Bits								Comment
Octets	8	7	6	5	4	3	2	1	
38+a+b	Length = c								Secondary PDN-GW address
39+a+b to (39+a +b+c -1)	IPv4 or IPv6 Address								

7.2.1 PDN Type

Set the PDN type value by following rules in Table 11.

Table 11 PDN Type Value

PDN type value (octet 1)			
Bits ⁽¹⁾			
3	2	1	
0	0	1	IPv4
0	1	0	IPv6
0	1	1	IPv4v6

(1) Bits between 4 and 8 of the octet 1 are spare and coded as zero.

7.2.2 APN Restriction

Set the APN restrictions by following rules in Table 12.

Table 12 APN Restriction

Maximum APN Restriction Value	Type of APN	Application Example	APN Restriction Value ⁽¹⁾
0	No Existing Contexts or Restriction		All
1	Public-1	MMS	1, 2, 3
2	Public-2	Internet	1, 2
3	Private-1	Corporate ⁽²⁾	1
4	Private-2	Corporate ⁽³⁾	None

(1) The values are allowed to be established.

(2) For example, the entity who uses MMS.

(3) For example, the entity who does not use MMS.

7.2.3 APN-AMBR Value

APN-AMBR is of type of unsigned 32 binary integer with unit "**kbps**".



Table 13 APN-AMBR Value

Aggregate Maximum Bit Rate (AMBR)	Value
APN-AMBR for uplink	$0 \sim 2^{32} - 1$
APN-AMBR for downlink	$0 \sim 2^{32} - 1$

7.2.4 Bear-QoS Value

Set the Bear-QoS value by following rules in Table 14.

Table 14 Bear-QoS Value

Bearer QoS	Value	Comments
Pre-emption Vulnerability (PVI)	0 or 1	PRE-EMPTION_VULNERABILITY_ENABLED (0)
		PRE-EMPTION_VULNERABILITY_DISABLED (1)
Priority Level(PL)	1 ~ 15	
Pre-emption Capability (PCL)	0 or 1	PRE-EMPTION_CAPABILITY_ENABLED (0)
		PRE-EMPTION_CAPABILITY_DISABLED (1)
Label (QCI)	0 ~ 255	
Maximum bit rate for uplink	0 ~ 10,000,000,000 kbps	1 kbps = 1000 bits per second
Maximum bit rate for downlink	0 ~ 10,000,000,000 kbps	
Guaranteed bit rate for uplink	0 ~ 10,000,000,000 kbps	
Guaranteed bit rate for downlink	0 ~ 10,000,000,000 kbps	

7.2.5 Charging Characteristic Value

For the coding of Charging Characteristics, see 3GPP TS 29.274 v11.3.0 Section 8.30.

7.2.6 APN Name Encoding

The APN name encoding follows the 3GPP TS 23.003 v10.0.0 subclause 9.1. The APN name provided by HLR is used by WiFi-GW to create the GTP tunnel.



7.2.7 Primary or Secondary PDN-GW Address

The primary or secondary PDN-GW address contains the IPv4 or IPv6 address of the PDN-GW. The GTP tunnel is created between the WiFi-GW and PDN-GW.

Table 15 Primary or Secondary PDN-GW Address

PDN-GW Address	Value	Comments
Length	4 or 16	4 means IPv4 address
		16 means IPv6 address
Address Value	IPv4 or IPv6 address	The address is of Hex value, such as 10.1.0.1 is interpreted to equal Hex value 0x0A010001.



Reference List

IPWorks Library Documents

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

Standards

- [4] [3GPP system to Wireless Local Area Network \(WLAN\) interworking, TS 23.234 V9.0.0](#)
- [5] [Common RADIUS Implementation Issues and Suggested Fixes](#)
- [6] [Chargeable User Identity](#)
- [7] [Dynamic Authorization Extensions to Remote Authentication Dial In User Service \(RADIUS\)](#)
- [8] [Extensible Authentication Protocol Method for Global System for Mobile Communications\(GSM\) Subscriber Identity Modules \(EAP-SIM\)](#)
- [9] [Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement \(EAP-AKA\)](#)
- [10] [Extensible Authentication Protocol \(EAP\)](#)
- [11] [IEEE 802.1X RADIUS Usage Guidelines](#)
- [12] [RADIUS Accounting](#)
- [13] [RADIUS Extensions](#)
- [14] [Remote Authentication Dial In User Service \(RADIUS\)](#)
- [15] [Remote Authentication Dial In User Service \(RADIUS\) Support For Extensible Authentication Protocol \(EAP\)](#)