Ruckus Wireless™ SmartZone™ 100 and Virtual SmartZone Essentials

AAA (RADIUS) Interface Reference Guide for SmartZone 3.5.1

Part Number: 800-71509-001 Rev B
Published: 04 September 2017

www.ruckuswireless.com

Contents

Copyright Notice and Proprietary Information

Destination Control Statement

Technical data contained in this publication may be subject to the export control laws of the United States of America. Disclosure to nationals of other countries contrary to United States law is prohibited. It is the reader's responsibility to determine the applicable regulations and to comply with them.

Disclaimer

THIS DOCUMENTATION AND ALL INFORMATION CONTAINED HEREIN ("MATERIAL") IS PROVIDED FOR GENERAL INFORMATION PURPOSES ONLY. RUCKUS AND ITS LICENSORS MAKE NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, WITH REGARD TO THE MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR THAT THE MATERIAL IS ERROR-FREE, ACCURATE OR RELIABLE. RUCKUS RESERVES THE RIGHT TO MAKE CHANGES OR UPDATES TO THE MATERIAL AT ANY TIME.

Limitation of Liability

IN NO EVENT SHALL RUCKUS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR USE, INCURRED BY YOU OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIAL.

Trademarks

Ruckus Wireless, Ruckus, the bark logo, BeamFlex, ChannelFly, Dynamic PSK, FlexMaster, Simply Better Wireless, SmartCell, SmartMesh, SmartZone, Unleashed, ZoneDirector and ZoneFlex are trademarks of Ruckus Wireless, Inc. in the United States and other countries. All other product or company names may be trademarks of their respective owners.

About this Guide

This SmartZone™ SZ100 and Virtual SmartZone Essentials (vSZ-E) AAA (RADIUS) Interface Reference Guide describes the interface between SZ100/vSZ-E (collectively referred to as "the controller" throughout this guide) and the Authentication, Authorization and Accounting (AAA) server. It describes the message flow between the controller and AAA for EAP-based full authentication, authorization, and accounting.

This guide is written for service operators and system administrators who are responsible for managing, configuring, and troubleshooting Ruckus Wireless devices. Consequently, it assumes a basic working knowledge of local area networks, wireless networking, and wireless devices.

NOTE If release notes are shipped with your product and the information there differs from the information in this guide, follow the instructions in the release notes.

Most user guides and release notes are available in Adobe Acrobat Reader Portable Document Format (PDF) or HTML on the Ruckus Wireless Support Web site at https://support.ruckuswireless.com/contact-us.

Document Conventions

Table 1: Text conventions on page 5 and Table 2: Notice conventions on page 5 list the text and notice conventions that are used throughout this guide.

Table 1: Text conventions

Convention	Description	Example
`message phrase`	Represents information as it appears on screen	`[Device Name] >`
`user input`	Represents information that you enter	`[Device Name] > set ipaddr 10.0.0.12`
user interface controls	Keyboard keys, software buttons, and field names	Click **Start** > **All Programs**
screen or page names		Click **Advanced Settings**. The **Advanced Settings** page appears.

Table 2: Notice conventions

Notice type	Description
NOTE	Information that describes important features or instructions

Notice type	Description
CAUTION!	Information that alerts you to potential loss of data or potential damage to an application, system, or device
WARNING!	Information that alerts you to potential personal injury

Terminology

The table lists the terms used in this guide.

Table 3: Terms used in this guide

Terminology	Description
AAA	Authentication, Authorization, and Accounting
CHAP	Challenge Handshake Authentication Protocol
EAP	Extensible Authentication Protocol
EPS	Evolved Packet System
GGSN	Gateway GPRS Support Node
GSN	GPRS Support Node
HLR	Home Location Register
LCS	Location Services
MAP	Mobile Application Part
MTU	Maximum Transmission Unit
MWSG	Metro Wireless Security Gateway
OSU	Online Sign-Up
Passpoint	Hotspot 2.0 certification
PKI	Public Key Infrastructure
PDP	Packet Data Protocol
PPS-MO	Per Provider Subscription Management Object
R-WSG/WSG	Ruckus Wireless Security Gateway
Release1 Device	Hotspot 2.0 Release1 specification compliant device

Terminology	Description
Release 2 Device	Hotspot 2.0 Release 2 passpoint enabled device
RAC	Radio Access Controller
RADIUS	Remote Access Dial In User Service
TEID	Tunnel End Point Identifier
UE	User Equipment
WFA	Wi-Fi Alliance

Legend

The table lists the legends/presence used in this guide.

Table 4: Legends used in this guide

Legend/Presence	Description
M	Mandatory
O	Optional
C	Conditional
U	Indicates that the inclusion of the parameter is the choice of service-user

Definition of Data Types

The table lists the data types used in this guide.

Table 5: Data Types Definition

Data Type	Description
text	Printable, generally UTF-8 encoded (subset of 'string')
string	0-253 octets
ipaddr	4 octets in network byte order
integer	32 bit value in big endian order (high byte first)
date	32 bit value in big endian order - seconds since 00:00:00 GMT, Jan. 1, 1970.

Data Type	Description
ipv6addr	16 octets in network byte order.
ipv6prefix	18 octets in network byte order.
abinary	Ascend's binary filter format.
byte	8 bit unsigned integer.
ether	6 octets of hh:hh:hh:hh:hh:hh where 'h' is hex digits, upper or lowercase.
short	16-bit unsigned integer.
octets	Raw octets, printed and input as hex strings. For example, 0x123456789abcdef.

Related Documentation

For a complete list of documents that accompany this release, refer to the Release Notes.

Online Training Resources

To access a variety of online Ruckus Wireless training modules, including free introductory courses to wireless networking essentials, site surveys, and Ruckus Wireless products, visit the Ruckus Wireless Training Portal at:

https://training.ruckuswireless.com.

References

The table lists the references used in this guide

Table 6: References used in this guide

Serial Number	Reference	Description
1.	3GPP TS 23.234	3GPP system to WLAN inter-working
2.	3GPP TS 33.234	Wireless Local Area Network (WLAN) inter-working security
3.	RFC 2865	Remote authentication dial In user service (RADIUS))
4.	RFC 2866	RADIUS accounting

Serial Number	Reference	Description
5.	RFC 5176	Dynamic authorization extensions to remote authentication dial In user service (RADIUS)
6.	RFC 5580	Carrying Location Objects in RADIUS and Diameter (August 2009)
7.	WFA HS 2-0	WFA HS 2-0 Technical Specification R2 PUBLIC DRAFT v5.00 (Specification for HS 2.0 R2)

EAP Full Authentication Overview 1

This reference guide describes the interface between the controller and the AAA (Authentication, Authorization and Accounting) server. The RADIUS protocol is used for interfacing between Access Points (AP) and controller as well as between the controller and a third party AAA server. The controller acts as a RADIUS proxy for authentication and authorization. This guide also describes the message flow between the controller and AAA for EAP based full authentication, authorization and accounting in the following sections. EAP-SIM is used as EAP message payload type but can be replaced with EAP-AKA without affecting call flows and RADIUS attributes except EAP-Message (79).

The controller supports two different call flows for authentication and authorization:

- A 3GPP standard based solution, where authentication and service authorization are performed separately.
- A proprietary solution where authentication and authorization are combined. This guide lists all the interface messages and RADIUS VSAs used between the controller and AAA.

NOTE This guide does not provide design details of either the AAA server or the controller to handle interface requirements.

NOTE Refer to AP Roaming Scenarios appendix for various scenario cases.

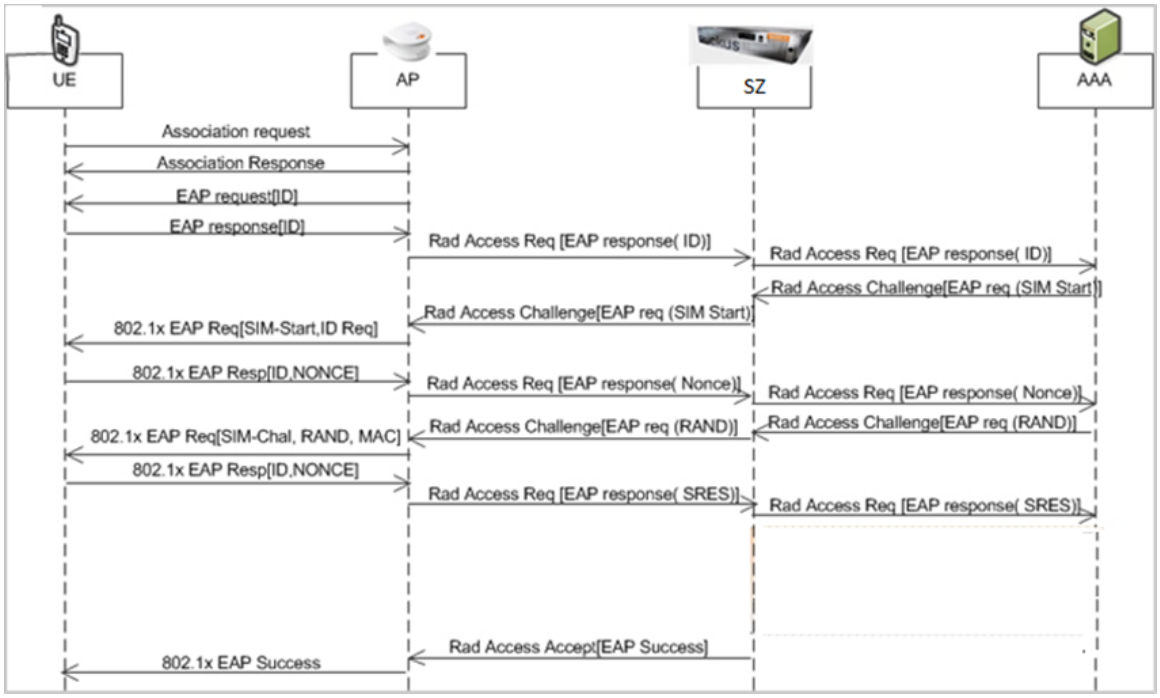
NOTE Refer to the appendix Use Cases for flow details on NAS IP, accounting session identifier and filter identifier.

EAP Full Authentication

This is authentication and authorization combined together.

In this call flow, the controller acts as an AAA proxy server. It does not initiate a separate access request message to perform service authorization. Parameters needed by the controller (TTG) to establish the GTP tunnel (QoS, Charging Characteristics, MSISDN) are expected in the access accept message from AAA. The figure shows the detailed call flow.

Figure 1: Combined authentication sequence diagram



This section covers:

- RADIUS Access Request [ID]
- RADIUS Access Challenge [EAP Request (SIM Start)]
- RADIUS Access Request [EAP Response (NONCE_MT)]
- RADIUS Access Challenge [EAP Request (RAND, MAC)]
- RADIUS Access Request [EAP Response (SRES)]
- RADIUS Access Accept [EAP Success (MSK)]

RADIUS Access Request [ID]

The table lists the attribute details for the first message sent by the controller to the AAA server.

NOTE When RFC 5580 is enabled for a WLAN, and the AAA server supports RFC 5580, location-related information is not conveyed in access requests. Instead, the exchange of location-related information is negotiated between the controller and the AAA server as stipulated in RFC 5580.

Table 7: RADIUS access request attributes

Attribute	Attribute ID	Presence	Type	Description
User-Name	1	M	String	Indicates the name of the user to be authenticated.
NAS-IP-Address	4	C	Integer	This attribute is the IP address of the AP which is serving the station or controller's control IP address, controller's management IP address and user defined value.
NAS-Port	5	O	Integer	This attribute indicates the physical port number of the NAS which authenticates the user. The controller uses the association ID for the STA in the AP to represent this.
Service-Type	6	O	Integer	Indicates the type of service based on the user request or the type of service to be provided.
Framed MTU	12	O	Integer	Indicates the Maximum Transmission Unit (MTU) to be configured for the user, when it is not negotiated by some other means.
Vendor-Specific	26	C	Integer	Vendor ID: Ruckus:25053 VSA: Ruckus-WLan-ID (4) VSA Length: 6 Reports the associated WLANs ID. Ruckus VSAs are received from Ruckus APs only. It is optional for 3rd party APs.

Attribute	Attribute ID	Presence	Type	Description
Vendor-Specific	26	C	Integer	Vendor ID: Ruckus:25053 VSA: Ruckus-SCG-CBLADE-IP (7) VSA Length: 6 Reports the control plane IP address. Ruckus VSAs are received from Ruckus APs only. It is optional for 3rd party APs.
Vendor-Specific	26	C	Integer	Vendor ID:Ruckus:25053 VSA: Ruckus-SCG-DBLADE-IP (8) VSA Length: 6 Reports the control plane IP address. Ruckus VSAs are received from Ruckus APs only. It is optional for 3rd party APs.
Vendor-Specific	26	C	String	Vendor ID: Ruckus:25053 VSA: Ruckus-SSID (3) VSA Length: Variable Reports the associated WLANs SSID in access request and accounting packet. Ruckus VSAs are received from Ruckus APs only. It is optional for 3rd party APs.

Attribute	Attribute ID	Presence	Type	Description
Vendor-Specific	26	C	String	Vendor ID: Ruckus:25053 VSA: Ruckus-Location (5) VSA Length: Variable Reports the device location for this AP. This is a configurable value in the device location setting. Ruckus VSA is received only from Ruckus AP. It is optional for 3rd party APs.
Called Station ID	30	O	String	This attribute allows NAS to send the ID (BSSID), which is called by the user. It is MAC of the AP. It supports 2 types of values, namely BSSID:SSID, where BSSID is the MAC address of the WLAN on AP. The second value is AP-MAC:SSID, where AP-MAC is the MAC address of the AP.The letters in the MAC address are in uppercase.For example: 11-22-33-AA-BB-CC:SSID.
Calling Station ID	31	M	String	Allows NAS to send the ID (UE MAC), which indicates as to who is calling this server.
NAS-Identifier	32	C	Integer	NAS-IP-Address or NAS-Identifier attribute is mandatory in received messages. It supports 3 types of values, namely BSSID (MAC address of the WLAN on AP), AP-MAC (MAC address of AP) and user defined address (maximum length of 62).

Attribute	Attribute ID	Presence	Type	Description
Proxy-State	33	O	Octets	This attribute is available to be sent by a proxy server (controller) to another server (AAA server) when forwarding an access request, accounting request (start, stop or interim) and must be returned unmodified in the access accept, access reject, access challenge and accounting response.
Acct-Session-ID	44	M	Integer	This attribute is a unique accounting identity to facilitate easy matching of start, interim and stop records in a log file. The start, interim and stop records for a given session must have the same Acct-Session-ID.
NAS-Port-Type	61	M	Integer	Indicates the physical port type of NAS, which authenticates the user.
Connect-Info	77	O	String	This attribute is sent from the NAS to indicate the nature of the user's connection.
EAP Message	79	M	Octets	This attribute encapsulates Extensible Authentication Protocol (EAP) packets, which allows NAS to authenticate dial-in users via EAP, without having to understand the EAP protocol (EAP payload, EAP-SIM or EAP-AKA).

Attribute	Attribute ID	Presence	Type	Description
Message Authenticator	80	M	Octets	This attribute is used in signing access requests for preventing spoofing of access requests using CHAP, ARAP or EAP authentication methods. It authenticates this whole RADIUS packet - HMAC-MD5 (Type| Identifier | Length | Request Authenticator | Attributes).
Chargeable User ID	89	M	String	This attribute sends a null value during authentication.
Operator-Name	126	C	String	The attribute identifies the owner of the access network by the AAA server. It is encoded as per RFC 5580. **NOTE** This attribute is included only if the location delivery method is Out of Band as specified in RFC 5580
Location-Information	127	C	Octets	This is a composite attribute, which provides meta data about the location information. It is encoded as per RFC 5580. **NOTE** This attribute is included only if the location delivery method is Out of Band as specified in RFC 5580.

Attribute	Attribute ID	Presence	Type	Description
Location-Data	128	M	String	This attribute contains the actual location information. It is encoded as per RFC 5580. **NOTE** This attribute is included only if the location delivery method is Out of Band as specified in RFC 5580.
Basic-Location-Policy-Rules	129	C	Octets	This attribute provides the basic privacy policy associated to the location information. It is encoded as per RFC 5580. **NOTE** This attribute is included only if the location delivery method is Out of Band as specified in RFC 5580.
Extended-Location-Policy-Rules	130	C	Octets	This attribute provides the extended privacy policy for the target whose location is specified.This attribute is sent with the above attribute (basic location policy). It is encoded as per RFC 5580. **NOTE** This attribute is included only if the location delivery method is Out of Band as specified in RFC 5580.

Attribute	Attribute ID	Presence	Type	Description
Location-Capable	131	C	Integer	This attribute is sent in RADIUS access request during the authentication phase to indicate the AP's capability for providing the location. Encoded as per RFC 5580. **NOTE** This attribute is included only if location delivery method is not Out of Band.

RADIUS Access Challenge [EAP Request (SIM Start)]

The table lists the attribute details of the first message sent by the AAA to the controller, which is forwarded to the RADIUS client (access point).

Table 8: RADIUS access challenge attributes

Attribute	Attribute ID	Presence	Type	Description
State	24	O	Octets	This attribute is sent by the server to the client in an access-challenge message and must be sent unmodified from the client to the server in the new access request message - a reply to that challenge, if any.
Proxy-State	33	C	Octets	This attribute is available to be sent by a proxy server (controller) to another server (AAA server) when forwarding an access request, accounting request (start, stop or interim) and must be returned unmodified in the access accept, access reject, access-challenge and accounting response.

Attribute	Attribute ID	Presence	Type	Description
EAP Message	79	M	Octets	This attribute encapsulates Extensible Authentication Protocol (EAP) packets, which allows NAS to authenticate dial-in users via EAP, without having to understand the EAP protocol (EAP payload, EAP-SIM or EAP-AKA).
Message Authenticator	80	M	Octets	This attribute is used in signing access requests for preventing spoofing of access requests using CHAP, ARAP or EAP authentication methods. It authenticates this whole RADIUS packet - HMAC-MD5 (Type| Identifier | Length | Request Authenticator | Attributes).
Chargeable User ID	89	M	String	This attribute sends a null value during authentication.
Basic-Location-Policy-Rules	129	C	Octets	This attribute provides the basic privacy policy associated to the location information. It is encoded as per RFC 5580. **NOTE** This attribute is expected from the AAA server in the initial request location delivery method mentioned in RFC 5580.
Extended-Location-Policy-Rules	130	C	Octets	This attribute provides the extended privacy policy for the target whose location is specified.This attribute is sent with the above attribute (basic location policy). It is encoded as per RFC 5580. **NOTE** This attribute is expected from the AAA server in the initial request location delivery method mentioned in RFC 5580.

Attribute	Attribute ID	Presence	Type	Description
Requested-Location-Info	132	M	Integer	This attribute is only used in messages sent by the AAA server towards the AP. Using this attribute the AAA server indicates its request for location information. Encoded as per RFC 5580. **NOTE** This attribute is expected from the AAA server in the initial request location delivery method mentioned in RFC 5580.

RADIUS Access Request [EAP Response (NONCE_MT)]

The table lists the attribute details of messages sent by the controller to the AAA server and responses received from the UEs.

Table 9: RADIUS access request attributes

Attribute	Attribute ID	Presence	Type	Description
User-Name	1	M	String	Indicates the name of the user to be authenticated.
User-Password	2	C	String	This attribute indicates the password of the user to be authenticated. It is mandatory for PAP authentication.
CHAP-Password	3	C	String	This attribute indicates the value provided by a CHAP user in response to the access-challenge. It is mandatory for CHAP authentication.
NAS-IP-Address	4	C	Integer	This attribute is the IP address of the AP which is serving the station or controller's control IP address, controller's management IP address and user defined value.
NAS-Port	5	O	Integer	This attribute indicates the physical port number of the NAS which authenticates the user. The controller uses the association ID for the STA in the AP to represent this.

Attribute	Attribute ID	Presence	Type	Description
Service-Type	6	O	Integer	Indicates the type of service based on the user request or the type of service to be provided.
Framed MTU	12	O	Integer	Indicates the Maximum Transmission Unit (MTU) to be configured for the user, when it is not negotiated by some other means.
State	24	O	Octets	This attribute is sent by the server to the client in an access-challenge message and must be sent unmodified from the client to the server in the new access request message - a reply to that challenge, if any.
Vendor-Specific	26	C	Integer	Vendor ID: Ruckus:25053 VSA: Ruckus-SCG-CBLADE-IP (7) VSA Length: 6 Reports the control plane IP address. Ruckus VSAs are received from Ruckus APs only. It is optional for 3rd party APs.
Vendor-Specific	26	C	Integer	Vendor ID: Ruckus:25053 VSA: Ruckus-SCG-DBLADE-IP (8) VSA Length: 6 Reports the data plane IP address. Ruckus VSAs are received from Ruckus APs only. It is optional for 3rd party APs.
Vendor-Specific	26	C	String	Vendor ID: Ruckus:25053 VSA: Ruckus-SSID (3) VSA Length: Variable Reports the associated WLANs SSID in access request and accounting packet. Ruckus VSAs are received from Ruckus APs only. It is optional for 3rd party APs.

Attribute	Attribute ID	Presence	Type	Description
Vendor-Specific	26	C	String	Vendor ID: Ruckus:25053 VSA: Ruckus-Location (5) VSA Length: Variable Reports the device location for this AP. This is a configurable value in the device location setting. Ruckus VSA is received only from Ruckus AP. It is optional for 3rd party APs.
Called Station ID	30	O	String	This attribute allows NAS to send the ID (BSSID), which is called by the user. It is MAC of the AP. It supports 2 types of values, namely BSSID:SSID, where BSSID is the MAC address of the WLAN on AP. The second value is AP-MAC:SSID, where AP-MAC is the MAC address of the AP.The letters in the MAC address are in uppercase.For example: 11-22-33-AA-BB-CC:SSID.
Calling Station ID	31	M	String	Allows NAS to send the ID (UE MAC), which indicates as to who is calling this server.
NAS-Identifier	32	C	Integer	NAS-IP-Address or NAS-Identifier attribute is mandatory in received messages. It supports 3 types of values, namely BSSID (MAC address of the WLAN on AP), AP-MAC (MAC address of AP) and user defined address (maximum length of 62).
Proxy-State	33	O	Octets	This attribute is available to be sent by a proxy server (controller) to another server (AAA server) when forwarding an access request, accounting request (start, stop or interim) and must be returned unmodified in the access accept, access reject, access challenge and accounting response.

Attribute	Attribute ID	Presence	Type	Description
Acct-Session-ID	44	M	Integer	This attribute is a unique accounting identity to facilitate easy matching of start, interim and stop records in a log file. The start, interim and stop records for a given session must have the same Acct-Session-ID.
NAS-Port-Type	61	M	Integer	Indicates the physical port type of NAS, which authenticates the user.
Connect-Info	77	O	String	This attribute is sent from the NAS to indicate the nature of the user's connection.
EAP Message	79	M	Octets	This attribute encapsulates Extensible Authentication Protocol (EAP) packets, which allows NAS to authenticate dial-in users via EAP, without having to understand the EAP protocol (EAP payload, EAP-SIM or EAP-AKA).
Message Authenticator	80	M	Octets	This attribute is used in signing access requests for preventing spoofing of access requests using CHAP, ARAP or EAP authentication methods. It authenticates this whole RADIUS packet - HMAC-MD5 (Type| Identifier | Length | Request Authenticator | Attributes).
Chargeable User ID	89	M	String	This attribute sends a null value during authentication.
Operator-Name	126	C	String	The attribute identifies the owner of the access network by the AAA server. It is encoded as per RFC 5580. **NOTE** This attribute is included only if the location delivery method is Out of Band as specified in RFC 5580.

Attribute	Attribute ID	Presence	Type	Description
Location-Information	127	C	Octets	This is a composite attribute, which provides meta data about the location information. It is encoded as per RFC 5580. **NOTE** This attribute is included only if the location delivery method is Out of Band as specified in RFC 5580.
Location-Data	128	M	String	This attribute contains the actual location information. It is encoded as per RFC 5580. **NOTE** This attribute is included only if the location delivery method is the initial request as specified in RFC 5580.
Basic-Location-Policy-Rules	129	C	Octets	This attribute provides the basic privacy policy associated to the location information. It is encoded as per RFC 5580. **NOTE** This attribute is included only if the location delivery method is the initial request as specified in RFC 5580.
Extended-Location-Policy-Rules	130	C	Octets	This attribute provides the extended privacy policy for the target whose location is specified.This attribute is sent with the above attribute (basic location policy). It is encoded as per RFC 5580. **NOTE** This attribute is included only if the location delivery method is the initial request as specified in RFC 5580.

Attribute	Attribute ID	Presence	Type	Description
Location-Capable	131	C	Integer	This attribute is sent in RADIUS access request during the authentication phase to indicate the AP's capability for providing the location. Encoded as per RFC 5580. **NOTE** This attribute is included only if the location delivery method is the initial request as specified in RFC 5580.

RADIUS Access Challenge [EAP Request (RAND, MAC)]

The table lists the attribute details of messages sent by the AAA to the controller, which are forwarded to the RADIUS client (access point).

Table 10: RADIUS access challenge attributes

Attribute	Attribute ID	Presence	Type	Description
State	24	O	Octets	This attribute is sent by the server to the client in an access-challenge message and must be sent unmodified from the client to the server in the new access request message - a reply to that challenge, if any.
Proxy-State	33	C	Octets	This attribute is available to be sent by a proxy server (controller) to another server (AAA server) when forwarding an access request, accounting request (start, stop or interim) and must be returned unmodified in the access accept, access reject, access challenge and accounting response.
EAP Message	79	M	Octets	This attribute encapsulates Extensible Authentication Protocol (EAP) packets, which allows NAS to authenticate dial-in users via EAP, without having to understand the EAP protocol (EAP payload, EAP-SIM or EAP-AKA).

Attribute	Attribute ID	Presence	Type	Description
Message Authenticator	80	M	Octets	This attribute is used in signing access requests for preventing spoofing of access requests using CHAP, ARAP or EAP authentication methods. It authenticates this whole RADIUS packet - HMAC-MD5 (Type| Identifier | Length | Request Authenticator | Attributes).
Chargeable User ID	89	M	String	This attribute sends a null value during authentication.

RADIUS Access Request [EAP Response (SRES)]

The table lists the attribute details of messages sent by the controller to the AAA server.

Table 11: RADIUS access request attributes

Attribute	Attribute ID	Presence	Type	Description
User-Name	1	M	String	Indicates the name of the user to be authenticated.
User-Password	2	C	String	This attribute indicates the password of the user to be authenticated. It is mandatory for PAP authentication.
CHAP-Password	3	C	String	This attribute indicates the value provided by a CHAP user in response to the access-challenge. It is mandatory for CHAP authentication.
NAS-IP-Address	4	C	Integer	This attribute is the IP address of the AP which is serving the station or controller's control IP address, controller's management IP address and user defined value.
NAS-Port	5	O	Integer	This attribute indicates the physical port number of the NAS which authenticates the user. The controller uses the association ID for the STA in the AP to represent this.
Service-Type	6	O	Integer	Indicates the type of service based on the user request or the type of service to be provided.

Attribute	Attribute ID	Presence	Type	Description
Framed MTU	12	O	Integer	Indicates the Maximum Transmission Unit (MTU) to be configured for the user, when it is not negotiated by some other means.
State	24	O	Octets	This attribute is sent by the server to the client in an access-challenge message and must be sent unmodified from the client to the server in the new access request message - a reply to that challenge, if any.
Vendor-Specific	26	C	Integer	Vendor ID: Ruckus:25053 VSA: Ruckus-WLan-ID (4) VSA Length: 6 Reports the associated WLANs ID. Ruckus VSA is received only from Ruckus AP. It is optional for 3rd party APs.
Vendor-Specific	26	C	Integer	Vendor ID: Ruckus:25053 VSA: Ruckus-SCG-CBLADE-IP (7) VSA Length: 6 Reports the control plane IP address. Ruckus VSAs are received from Ruckus APs only. It is optional for 3rd party APs.
Vendor-Specific	26	C	Integer	Vendor ID:Ruckus:25053 VSA: Ruckus-SCG-DBLADE-IP (8) VSA Length: 6 Reports the data plane IP address. Ruckus VSAs are received from Ruckus APs only. It is optional for 3rd party APs.
Vendor-Specific	26	C	String	Vendor ID: Ruckus:25053 VSA: Ruckus-SSID (3) VSA Length: Variable Reports the associated WLANs SSID in access request and accounting packet. Ruckus VSAs are received from Ruckus APs only. It is optional for 3rd party APs.

Attribute	Attribute ID	Presence	Type	Description
Vendor-Specific	26	C	String	Vendor ID: Ruckus:25053 VSA: Ruckus-Location (5) VSA Length: Variable Reports the device location for this AP. This is a configurable value in the device location setting. Ruckus VSA is received only from Ruckus AP. It is optional for 3rd party APs.
Called Station ID	30	O	String	This attribute allows NAS to send the ID (BSSID), which is called by the user. It is MAC of the AP. It supports 2 types of values, namely BSSID:SSID, where BSSID is the MAC address of the WLAN on AP. The second value is AP-MAC:SSID, where AP-MAC is the MAC address of the AP.The letters in the MAC address are in uppercase.For example: 11-22-33-AA-BB-CC:SSID.
Calling Station ID	31	M	String	This attribute allows NAS to send the ID (UE MAC), which indicates as to who is calling this server. The value supported is STA's MAC address where the letters in the MAC address are in uppercase.For example: 11-22-33-AA-BB-CC.
NAS-Identifier	32	C	Integer	NAS-IP-Address or NAS-Identifier attribute is mandatory in received messages. It supports 3 types of values, namely BSSID (MAC address of the WLAN on AP), AP-MAC (MAC address f AP) and user defined address (maximum length of 62).
Proxy-State	33	O	Octets	This attribute is available to be sent by a proxy server (controller) to another server (AAA server) when forwarding an access request, accounting request (start, stop or interim) and must be returned unmodified in the access accept, access reject, access challenge and accounting response.

Attribute	Attribute ID	Presence	Type	Description
Acct-Session-ID	44	M	Integer	This attribute is a unique accounting identity to facilitate easy matching of start, interim and stop records in a log file. The start, interim and stop records for a given session must have the same Acct-Session-ID.
NAS-Port-Type	61	M	Integer	Indicates the physical port type of NAS, which authenticates the user.
Connect-Info	77	O	String	This attribute is sent from the NAS to indicate the nature of the user's connection.
EAP Message	79	M	Octets	This attribute encapsulates Extensible Authentication Protocol (EAP) packets, which allows NAS to authenticate dial-in users via EAP, without having to understand the EAP protocol (EAP payload, EAP-SIM or EAP-AKA).
Message Authenticator	80	M	Octets	This attribute is used in signing access requests for preventing spoofing of access requests using CHAP, ARAP or EAP authentication methods. It authenticates this whole RADIUS packet - HMAC-MD5 (Type| Identifier | Length | Request Authenticator | Attributes).
Chargeable User ID	89	M	String	This attribute sends a null value during authentication.

RADIUS Access Accept [EAP Success (MSK)]

The table lists the attribute details of messages sent by AAA to the controller, which is forwarded to the RADIUS client (access point) upon successful service authorization (see the next two messages).

NAS calculates MSK using the MS-MPP-Send and MS-MPP-Recv attributes.

Table 12: RADIUS access accept attributes

Attribute	Attribute ID	Presence	Type	Description
User-Name	1	O	String	Indicates the name of the user to be authenticated

Attribute	Attribute ID	Presence	Type	Description
Filter-Id	11	O	String	Represents the User Role name sent by AAA. This is used by SCG to map the received Group Role Name to the UTP profile and forward the corresponding ACL/rate limiting parameters to NAS. NAS enforces the UTP for the given user. Filter-Id might be included in access accept irrespective of a WISPr, 802.1x or HS 2.0 call.
Class	25	O	Integer	This attribute is sent by the server in access accept and client should include this attribute in accounting request without modification.
ChargeableUser ID	89	C	Integer	This attribute is MSISDN or any chargeable user identity returned by the AAA server. This attribute is mandatory for TTG sessions only.
Vendor-Specific	26	O	String	Vendor ID: 3GPP: 10415 VSA: 3GPP-GPRS-Negotiated-QoS-Profile (5) VSA Length: Variable This attribute carries the QoS value from AAA server. QoS from AAA is received from Ruckus defined VSA or from 3GPP defined VSA (3GPP-GPRS-Negotiated-QoS Profile).
Vendor-Specific	26	O	Integer	Vendor ID: WISPr: 14122 VSA: WISPr-Bandwidth-Max-UP (7) VSA Length: Variable The attribute contains the maximum uplink value in bits per second.

Attribute	Attribute ID	Presence	Type	Description
Vendor-Specific	26	O	Integer	Vendor ID: WISPr: 14122 VSA: WISPr-Bandwidth-Max-DOWN (8) VSA Length: Variable The attribute contains the maximum downlink value in bits per second.
Vendor-Specific	26	C	Charging characteristics	Vendor ID:Ruckus:25053 VSA: Ruckus-Charging-Charac (118) VSA Length: 4 Charging characteristics value, Octets are encoded according to TS 3GPP 32.215. This attribute carries the charging characteristics value, which is received from the AAA server.
Vendor-Specific	26	C	String	Vendor ID:Ruckus:25053 VSA: Ruckus-IMSI (102) VSA Length: Variable BCD encoded IMSI of the subscriber.
Session-Timeout	27	O	Integer	This attribute sets the maximum number of seconds of service to be provided to the user before session termination.
Idle-Timeout	28	O	Integer	It sets the maximum number of consecutive seconds of idle connection allowed to the user, before the session gets terminated.
Termination-Action	29	O	Integer	This attribute indicates the action that NAS will take when the specified service completes.

Attribute	Attribute ID	Presence	Type	Description
Proxy-State	33	M	Octets	This attribute is available to be sent by a proxy server (controller) to another server (AAA server) when forwarding an access request, accounting request (start, stop or interim) and must be returned unmodified in the access accept, access reject, access challenge and accounting response.
Tunnel-Type	64	C	Integer	This attribute indicates the tunnel type for the access point. For example, tunnel type 13 is for VLAN.
Tunnel-Medium-Type	65	C	Integer	This attribute indicates the tunnel medium type for the access point. For example, tunnel type 06 is for IEEE_802.
EAP Message	79	M	Octets	This attribute encapsulates Extensible Authentication Protocol (EAP) packets, which allows NAS to authenticate dial-in users via EAP, without having to understand the EAP protocol (EAP payload, EAP-SIM or EAP-AKA).
Message Authenticator	80	M	Octets	This attribute is used in signing access requests for preventing spoofing of access requests using CHAP, ARAP or EAP authentication methods. It authenticates this whole RADIUS packet - HMAC-MD5 (Type| Identifier | Length | Request Authenticator | Attributes).
Tunnel-Private-Group-ID	81	C	String	This attribute contains the dynamic VLAN ID as configured in the authentication profile.

Attribute	Attribute ID	Presence	Type	Description
Accounting-Interim-Interval	85	O	Integer	Indicates the number of seconds between each interim update for this specific session. If the value is blank, the configured default value is used as the accounting interim interval.
Chargeable User ID	89	M	String	This attribute sends a null value during authentication.
Vendor-Specific	26	C	Integer	Vendor ID:Ruckus:25053 VSA: Ruckus-Acct-Status (126) VSA Length: 4 Acct Stat is true(1) or false(0). The controller sever uses this attribute on the access accept to indicate if the authenticator needs to send the accounting start for the current/specified client.
Vendor-Specific	26	O	Integer	Vendor ID: Microsoft: 311 VSA: MS-MPPE-Send-Key (16) VSA Length: Variable This attribute contains a session key used by Microsoft Point-to-Point Encryption Protocol (MPPE).
Vendor-Specific	26	O	Integer	Vendor ID: Microsoft: 311 VSA: MS-MPPE-Recv-Key (17) VSA Length: Variable This attribute contains a session key used by the Microsoft Point-to-Point Encryption Protocol (MPPE).

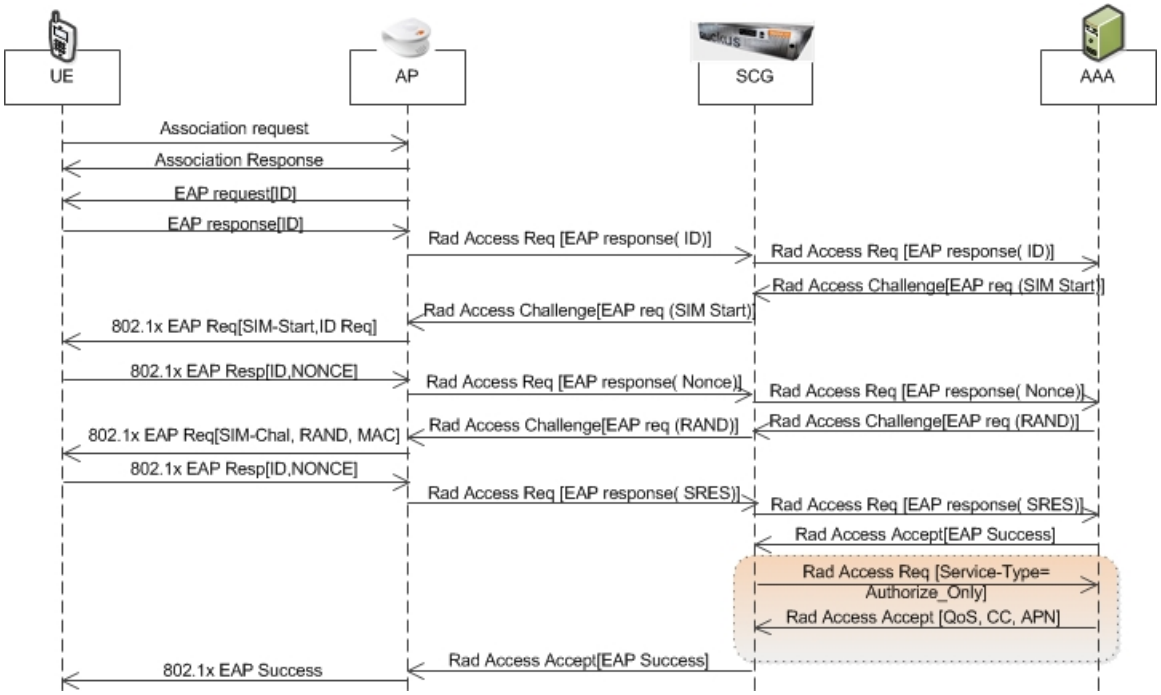
Attribute	Attribute ID	Presence	Type	Description
Vendor-Specific	26	C	Octets	Vendor ID: Ruckus:25053 VSA: Ruckus-APN-NI (104) VSA Length: Variable This attribute carries the APN subscribed by the user. It contains only the network identifier (NI), which is part of the APN. The operator identifier part is stored separately in Ruckus-APN-OI.
Vendor-Specific	26	C	Integer	Vendor ID: Ruckus:25053 VSA: Ruckus-Session-Type(125) VSA Length: 6 Session type - TTG (2), Local-Breakout(3), Local-Breakout-AP(4), L3GRE (5), L2GRE (6), QinQL3 (7), PMIP (8). The controller server uses this attribute on the access -accept to indicate the forward policy of the specific UE.
Basic-Location-Policy-Rules	129	C	Octets	This attribute provides the basic privacy policy associated to the location information. It is encoded as per RFC 5580. **NOTE** This attribute is expected from the AAA server in the initial request location delivery method as mentioned in RFC 5580.

Attribute	Attribute ID	Presence	Type	Description
Extended-Location-Policy-Rules	130	C	Octets	This attribute provides the extended privacy policy for the target whose location is specified.This attribute is sent with the above attribute (basic location policy). It is encoded as per RFC 5580. **NOTE** This attribute is expected from the AAA server in the initial request location delivery method as mentioned in RFC 5580.
Requested-Location-Info	132	M	Integer	This attribute is only used in messages sent by the AAA server towards the AP. Using this attribute the AAA server indicates its request for location information. Encoded as per RFC 5580. **NOTE** This attribute is expected from the AAA server in the initial request location delivery method as mentioned in RFC 5580.

EAP - Full Authentication – 3GPP Solution

In this call flow, EAP-SIM authentication is performed first. When the controller (acting as an AAA proxy) receives access accept from the AAA server, a separate access request is sent back to the AAA server to process a service authorization. The figure shows the detailed call flow.

Figure 2: 3GPP based solution sequence diagram



- RADIUS Access Request [ID]
- RADIUS Access Challenge [EAP Request (SIM Start)]
- RADIUS Access Request [EAP Response (NONCE_MT)]
- RADIUS Access Challenge [EAP Request (RAND, MAC)]
- RADIUS Access Request [EAP Response (SRES)]
- RADIUS Access Accept [EAP Success (MSK)]
- Authorization Access Request
- Authorization Access Accept

RADIUS Access Request [ID]

The table lists the attribute details of the first message sent by the controller to AAA.

NOTE When RFC 5580 is enabled for a WLAN, and the AAA server supports RFC 5580, location-related information is not conveyed in access requests. Instead, the exchange of location-related information is negotiated between the controller and the AAA server as stipulated in RFC 5580.

Table 13: RADIUS access request attributes

Attribute	Attribute ID	Presence	Type	Description
User-Name	1	M	String	Indicates the name of the user for authentication.
NAS-IP-Address	4	C	Integer	This attribute is the IP address of the AP which is serving the station or controller's control IP address, controller's management IP address and user defined value.
NAS-Port	5	O	Integer	This attribute indicates the physical port number of the NAS which authenticates the user. The controller uses the association ID for the STA in the AP to represent this.
Service-Type	6	O	Integer	Indicates the type of service based on the user request or the type of service to be provided.
Framed MTU	12	O	Integer	Indicates the Maximum Transmission Unit (MTU) to be configured for the user, when it is not negotiated by some other means.
Vendor-Specific	26	C	Integer	Vendor ID: Ruckus:25053 VSA: Ruckus-WLan-ID (4) VSA Length: 6 Reports the associated WLANs ID. Ruckus VSAs are received only from Ruckus APs. It is optional for 3rd party APs.
Vendor-Specific	26	C	Integer	Vendor ID: Ruckus:25053 VSA: Ruckus-SCG-CBLADE-IP (7) VSA Length: 6 Reports the control plane IP address. Ruckus VSAs are received from Ruckus APs only. It is optional for 3rd party APs.

Attribute	Attribute ID	Presence	Type	Description
Vendor-Specific	26	C	Integer	Vendor ID: Ruckus:25053 VSA: Ruckus-SCG-DBLADE-IP (8) VSA Length: 6 Reports the data plane IP address. Ruckus VSAs are received from Ruckus APs only. It is optional for 3rd party APs.
Vendor-Specific	26	C	String	Vendor ID: Ruckus:25053 VSA: Ruckus-SSID (3) VSA Length: Variable. Reports the associated WLANs SSID in access request and accounting packet. Ruckus VSAs are received from Ruckus APs only. It is optional for 3rd party APs.
Vendor-Specific	26	C	String	Vendor ID: Ruckus:25053 VSA: Ruckus-Location (5) VSA Length: Variable. Reports the device location for this AP. This is a configurable value in the device location setting. Ruckus VSAs are received from Ruckus APs only. It is optional for 3rd party APs.
Called Station ID	30	O	String	This attribute allows NAS to send the ID (BSSID), which is called by the user. It is the MAC of the AP. It supports 2 types of values, namely BSSID:SSID, where BSSID is the MAC address of the WLAN on AP. The second value is AP-MAC:SSID, where AP-MAC is the MAC address of the AP.The letters in the MAC address are in uppercase.For example: 11-22-33-AA-BB-CC:SSID.
Calling Station ID	31	M	String	Allows NAS to send the ID (UE MAC), which indicates as to who is calling this server.

Attribute	Attribute ID	Presence	Type	Description
NAS-Identifier	32	C	String	NAS-IP-Address or NAS-Identifier attribute is mandatory in received messages. It supports 3 types of values, namely BSSID (MAC address of the WLAN on AP), AP-MAC (MAC address of AP) and user defined address (maximum length of 62).
Proxy-State	33	O	Octets	This attribute is available to be sent by a proxy server (controller) to another server (AAA server) when forwarding an access request, accounting request (start, stop or interim) and must be returned unmodified in the access accept, access-reject, access-challenge and accounting response.
Acct-Session-ID	44	M	String	This attribute is a unique accounting identity to facilitate easy matching of start, interim and stop records in a log file. The start, interim and stop records for a given session must have the same *Acct-Session-ID*.
NAS-Port-Type	61	M	Integer	Indicates the physical port type of NAS, which authenticates the user.
Connect-Info	77	O	String	This attribute is sent from the NAS to indicate the nature of the user's connection.
EAP Message	79	M	Octets	This attribute encapsulates Extensible Authentication Protocol (EAP) packets, which allows NAS to authenticate dial-in users via EAP, without having to understand the EAP protocol (EAP payload, EAP-SIM or EAP-AKA).
Message Authenticator	80	M	Octets	This attribute is used in signing access requests for preventing spoofing of access requests using CHAP, ARAP or EAP authentication methods. It authenticates the whole RADIUS packet - HMAC-MD5 (Type| Identifier | Length | Request Authenticator | Attributes).

Attribute	Attribute ID	Presence	Type	Description
Chargeable User ID	89	M	String	This attribute sends a null value during authentication.
Operator-Name	126	C	String	The attribute identifies the owner of the access network by the AAA server. It is encoded as per RFC 5580. Note: This attribute is included only if the location delivery method is Out of Band as specified in RFC 5580.
Location-Information	127	C	Octets	This is a composite attribute, which provides meta data about the location information. It is encoded as per RFC 5580. Note: This attribute is included only if the location delivery method is Out of Band as specified in RFC 5580.
Location-Data	128	M	String	This attribute contains the actual location information. It is encoded as per RFC 5580. Note: This attribute is included only if the location delivery method is the initial request as specified in RFC 5580.
Basic-Location-Policy-Rules	129	C	Octets	This attribute provides the basic privacy policy associated to the location information. It is encoded as per RFC 5580. Note: This attribute is included only if the location delivery method is the initial request as specified in RFC 5580.
Extended-Location-Policy-Rules	130	C	Octets	This attribute provides the extended privacy policy for the target whose location is specified. This attribute is sent with the above attribute (basic location policy). It is encoded as per RFC 5580. Note: This attribute is included only if the location delivery method is the initial request as specified in RFC 5580.

Attribute	Attribute ID	Presence	Type	Description
Location-Capable	131	C	Integer	This attribute is sent in RADIUS access request during the authentication phase to indicate the AP's capability for providing the location. Encoded as per RFC 5580. Note: This attribute is included only if the location delivery method is not Out of Band as specified in RFC 5580.

RADIUS Access Challenge [EAP Request (SIM Start)]

The table lists the attribute details of the messages sent by the AAA server to the controller and forwarded to the RADIUS client (NAS).

Table 14: RADIUS access challenge attributes

Attribute	Attribute ID	Presence	Type	Description
State	24	O	Octets	This attribute is sent by the server to the client in an access-challenge message and must be sent unmodified from the client to the server in the new access request message - a reply to that challenge, if any.
Proxy-State	33	O	Octets	This attribute is available to be sent by a proxy server (controller) to another server (AAA server) when forwarding an access request, accounting request (start, stop or interim) and must be returned unmodified in the access accept, access-reject, access-challenge and accounting response.
EAP Message	79	M	Octets	This attribute encapsulates Extensible Authentication Protocol (EAP) packets, which allows NAS to authenticate dial-in users via EAP, without having to understand the EAP protocol (EAP payload, EAP-SIM or EAP-AKA).

Attribute	Attribute ID	Presence	Type	Description
Message Authenticator	80	M	Octets	This attribute is used for signing access request for preventing spoofing of access request using CHAP, ARAP or EAP authentication methods. It authenticates this whole RADIUS packet - HMAC-MD5 (Type| Identifier | Length | Request Authenticator | Attributes).
Chargeable User ID	89	M	String	This attribute sends a null value during authentication.
Basic-Location-Policy-Rules	129	C	Octets	This attribute provides the basic privacy policy associated to the location information. It is encoded as per RFC 5580. Note: This attribute is expected from the AAA server in the initial request location delivery method as mentioned in RFC 5580.
Extended-Location-Policy-Rules	130	C	Octets	This attribute provides the extended privacy policy for the target whose location is specified.This attribute is sent with the above attribute (basic location policy). It is encoded as per RFC 5580. Note: This attribute is expected from the AAA server in the initial request location delivery method as mentioned in RFC 5580.
Requested-Location-Info	132	M	Integer	This attribute is only used in messages sent by the AAA server towards the AP. Using this attribute the AAA server indicates its request for location information. Encoded as per RFC 5580. Note: This attribute is expected from the AAA server in the initial request location delivery method mentioned in RFC 5580.

RADIUS Access Request [EAP Response (NONCE_MT)

The table lists the attribute details for messages sent by the controller to the AAA server (response received from UE).

Table 15: RADIUS access request attributes

Attribute	Attribute ID	Presence	Type	Description
User-Name	1	M	String	Indicates the name of the user for authentication.
User-Password	2	C	String	This attribute indicates the password of the user to be authenticated. It is mandatory for PAP authentication.
CHAP-Password	3	C	String	This attribute indicates the value provided by a CHAP user in response to the access-challenge. It is mandatory for CHAP authentication.
NAS-IP-Address	4	C	Integer	This attribute is the IP address of the AP which is serving the station or controller's control IP address, controller's management IP address and user defined value.
NAS-Port	5	O	Integer	This attribute indicates the physical port number of the NAS which authenticates the user. The controller uses the association ID for the STA in the AP to represent this.
Service-Type	6	O	Integer	Indicates the type of service based on the user request or the type of service to be provided.
Framed MTU	12	O	Integer	Indicates the Maximum Transmission Unit (MTU) to be configured for the user, when it is not negotiated by some other means.

Attribute	Attribute ID	Presence	Type	Description
State	24	O	Octets	This attribute is sent by the server to the client in an access-challenge message and must be sent unmodified from the client to the server in the new access request message - a reply to that challenge, if any.
Vendor-Specific	26	C	Integer	Vendor ID: Ruckus:25053 VSA: Ruckus-WLan-ID (4) VSA Length: 6 Reports the associated WLANs ID. Ruckus VSA is received only from Ruckus AP. It is optional for 3rd party APs.
Vendor-Specific	26	C	Integer	Vendor ID: Ruckus:25053 VSA: Ruckus-SCG-CBLADE-IP (7) VSA Length: 6 Reports the control plane IP address. Ruckus VSAs are received from Ruckus APs only. It is optional for 3rd party APs.
Vendor-Specific	26	C	Integer	Vendor ID: Ruckus:25053 VSA: Ruckus-SCG-DBLADE-IP (8) VSA Length: 6 Reports the data plane IP address. Ruckus VSAs are received from Ruckus APs only. It is optional for 3rd party APs.

Attribute	Attribute ID	Presence	Type	Description
Vendor-Specific	26	C	String	Vendor ID: Ruckus:25053 VSA: Ruckus-Location(5) VSA Length: Variable Reports the device location for this AP. This is a configurable value in the device location setting. Ruckus VSA is received only from Ruckus AP. It is optional for 3rd party APs.
Vendor-Specific	26	C	String	Vendor ID: Ruckus:25053 VSA: Ruckus-SSID (3) VSA Length: Variable Reports the associated WLANs SSID in access request and accounting packet. Ruckus VSAs are received from Ruckus APs only. It is optional for 3rd party APs.
Called Station ID	30	O	String	This attribute allows NAS to send the ID (BSSID), which is called by the user. It is MAC of the AP. It supports 2 types of values, namely BSSID:SSID, where BSSID is the MAC address of the WLAN on AP. The second value is APMAC:SSID, where APMAC is the MAC address of the AP.The letters in the MAC address are in uppercase.For example: 11-22-33-AA-BB-CC:SSID.
Calling Station ID	31	M	String	Allows NAS to send the ID (UE MAC), which indicates as to who is calling this server.

Attribute	Attribute ID	Presence	Type	Description
NAS-Identifier	32	C	String	NAS-IP-Address or NAS-Identifier attribute is mandatory in received messages. It supports 3 types of values, namely BSSID (MAC address of the WLAN on AP), APMAC (MAC address of AP) and user defined address (maximum length of 62).
Proxy-State	33	O	Octets	This attribute is available to be sent by a proxy server (controller) to another server (AAA server) when forwarding an access request, accounting request (start, stop or interim) and must be returned unmodified in the access accept, access-reject, access-challenge and accounting response.
Acct-Session-ID	44	M	String	This attribute is a unique accounting identity to facilitate easy matching of start, interim and stop records in a log file. The start, interim and stop records for a given session must have the same Acct-Session-ID.
NAS-Port-Type	61	M	Integer	Indicates the physical port type of NAS, which authenticates the user.
Connect-Info	77	O	String	This attribute is sent from the NAS to indicate the nature of the user's connection.
EAP Message	79	M	Octets	This attribute encapsulates Extensible Authentication Protocol (EAP) packets, which allows NAS to authenticate dial-in users via EAP, without having to understand the EAP protocol (EAP payload, EAP-SIM or EAP-AKA).

Attribute	Attribute ID	Presence	Type	Description
Message Authenticator	80	M	Octets	This attribute is used in signing access requests for preventing spoofing of access requests using CHAP, ARAP or EAP authentication methods. It authenticates this whole RADIUS packet - HMAC-MD5 (Type| Identifier | Length | Request Authenticator | Attributes).
Chargeable User ID	89	M	String	This attribute sends a null value during authentication.
Operator-Name	126	C	String	The attribute identifies the owner of the access network by the AAA server. It is encoded as per RFC 5580. **NOTE** This attribute is included only if the location delivery method is Out of Band as specified in RFC 5580.
Location-Information	127	C	Octets	This is a composite attribute, which provides meta data about the location information. It is encoded as per RFC 5580. **NOTE** This attribute is included only if the location delivery method is Out of Band as specified in RFC 5580.
Location-Data	128	M	String	This attribute contains the actual location information. It is encoded as per RFC 5580. **NOTE** This attribute is included only if the location delivery method is the initial request as specified in RFC 5580.

Attribute	Attribute ID	Presence	Type	Description
Basic-Location-Policy-Rules	129	C	Octets	This attribute provides the basic privacy policy associated to the location information. It is encoded as per RFC 5580. **NOTE** This attribute is included only if the location delivery method is the initial request as specified in RFC 5580.
Extended-Location-Poby-Rules	130	C	Octets	This attribute provides the extended privacy policy for the target whose location is specified.This attribute is sent with the above attribute (basic location policy). It is encoded as per RFC 5580. **NOTE** This attribute is included only if the location delivery method is the initial request as specified in RFC 5580.

RADIUS Access Challenge [EAP Request (RAND, MAC)]

The table lists the attribute details for messages sent by the AAA server to the controller and forwarded to the RADIUS client NAS.

Attribute	Attribute ID	Presence	Type	Description
State	24	O	Octets	This attribute is sent by the server to the client in an access-challenge message and must be sent unmodified from the client to the server in the new access request message - a reply to that challenge, if any.
Proxy-State	33	O	Octets	This attribute is available to be sent by a proxy server (controller) to another server (AAA server) when forwarding an access request, accounting request (start, stop or interim) and must be returned unmodified in the access accept, access-reject, access-challenge and accounting response.

Attribute	Attribute ID	Presence	Type	Description
EAP Message	79	M	Octets	This attribute encapsulates Extensible Authentication Protocol (EAP) packets, which allows NAS to authenticate dial-in users via EAP, without having to understand the EAP protocol (EAP payload, EAP-SIM or EAP-AKA).
Message Authenticator	80	M	Octets	This attribute is used in signing access requests for preventing spoofing of access requests using CHAP, ARAP or EAP authentication methods. It authenticates this whole RADIUS packet - HMAC-MD5 (Type| Identifier | Length | Request Authenticator | Attributes).
Chargeable User ID	89	M	String	This attribute sends a null value during authentication.

RADIUS Access Request [EAP Response (SRES)]

The table lists the attribute details for messages sent by controller to AAA.

Table 16: RADIUS access accept messages

Attribute	Attribute ID	Presence	Type	Description
User-Name	1	M	String	Indicates the name of the user for authentication.
User-Password	2	C	String	This attribute indicates the password of the user to be authenticated. It is mandatory for PAP authentication.
CHAP-Password	3	C	String	This attribute indicates the value provided by a CHAP user in response to the access-challenge. It is mandatory for CHAP authentication.
NAS-IP-Address	4	C	Integer	This attribute is the IP address of the AP which is serving the station or controller's control IP address, controller's management IP address and user defined value.

Attribute	Attribute ID	Presence	Type	Description
NAS-Port	5	O	Integer	This attribute indicates the physical port number of the NAS which authenticates the user. The controller uses the association ID for the STA in the AP to represent this.
Service-Type	6	O	Integer	Indicates the type of service based on the user request or the type of service to be provided.
Framed MTU	12	O	Integer	Indicates the Maximum Transmission Unit (MTU) to be configured for the user, when it is not negotiated by some other means.
State	24	O	Octets	This attribute is sent by the server to the client in an access-challenge message and must be sent unmodified from the client to the server in the new access request message - a reply to that challenge, if any.
Vendor-Specific	26	C	Integer	Vendor ID: Ruckus:25053. VSA: Ruckus-WLan-ID (4) VSA Length: 6 Reports the associated WLANs ID. Ruckus VSA is received only from Ruckus AP. It is optional for 3rd party APs.
Vendor-Specific	26	C	Integer	Vendor ID: Ruckus:25053. VSA: Ruckus-SCG-CBLADE-IP (7) VSA Length: 6 Reports the control plane IP address. Ruckus VSAs are received from Ruckus APs only. It is optional for 3rd party APs.

Attribute	Attribute ID	Presence	Type	Description
Vendor-Specific	26	C	Integer	Vendor ID: Ruckus:25053. VSA: Ruckus-SCG-DBLADE-IP (8) VSA Length: 6 Reports the data plane IP address. Note: Ruckus VSAs are received from Ruckus APs only. It is optional for 3rd party APs.
Vendor-Specific	26	C	String	Vendor ID: Ruckus:25053. VSA: Ruckus-Location (5) VSA Length: Variable. Reports the device location for this AP. This is a configurable value in the device location setting. Ruckus VSA is received only from Ruckus AP. It is optional for 3rd party APs.
Vendor-Specific(	26	C	String	Vendor ID: Ruckus:25053. VSA: Ruckus-SSID (3) VSA Length: Variable. Reports the associated WLANs SSID in access request and accounting packet. Note: Ruckus VSAs are received from Ruckus APs only. It is optional for 3rd party APs.
Calling Station ID	30	O	String	Allows NAS to send the ID (BSSID), which is called by the user. It is MAC of the AP.
Calling Station ID	31	M	IString	Allows NAS to send the ID (UE MAC), which indicates as to who is calling this server.
NAS-Identifier	32	C	String	NAS-IP-Address or NAS-Identifier attribute is mandatory in received messages. It supports 3 types of values, namely BSSID (MAC address of the WLAN on AP), AP-MAC (MAC address of AP) and user defined address (maximum length of 62).

Attribute	Attribute ID	Presence	Type	Description
Proxy-State	33	O	Octets	This attribute is available to be sent by a proxy server (controller) to another server (AAA server) when forwarding an access request, accounting request (start, stop or interim) and must be returned unmodified in the access accept, access-reject, access-challenge and accounting response.
Acct-Session-ID	44	M	String	This attribute is a unique accounting identity to facilitate easy matching of start, interim and stop records in a log file. The start, interim and stop records for a given session must have the same Acct-Session-ID.
NAS-Port-Type	61	M	Integer	Indicates the physical port type of NAS, which authenticates the user.
Connect-Info	77	O	String	This attribute is sent from the NAS to indicate the nature of the user's connection.
EAP Message	79	M	Octets	This attribute encapsulates Extensible Authentication Protocol (EAP) packets, which allows NAS to authenticate dial-in users via EAP, without having to understand the EAP protocol (EAP payload, EAP-SIM or EAP-AKA).
Message Authenticator	80	M	Octets	This attribute is used in signing access requests for preventing spoofing of access requests using CHAP, ARAP or EAP authentication methods. It authenticates this whole RADIUS packet - HMAC-MD5 (Type| Identifier | Length | Request Authenticator | Attributes).
Chargeable User ID	89	M	String	This attribute sends a null value during authentication.

RADIUS Access Accept [EAP Success (MSK)]

The table lists the attribute details for message sent by the AAA to the controller, which are forwarded to the RADIUS client (access point) upon successful service authorization (see the next two messages).

Table 17: RADIUS access request messages

Attribute	Attribute ID	Presence	Type	Description
User-Name	1	M	String	Indicates the name of the user for authentication.
Filter-Id	11	O	String	Represents the User Role name sent by AAA. This is used by SCG to map the received Group Role Name to the UTP profile and forward the corresponding ACL/rate limiting parameters to NAS. NAS enforces the UTP for the given user. Filter-Id might be included in access accept irrespective of a WISPr, 802.1x or HS 2.0 call.
Class	25	O	String	This attribute is sent by the server in access accept and the client should include this attribute in the accounting request without modification.
Vendor-Specific	26	O	Integer	Vendor ID: WISPr: 14122. VSA: WISPr-Bandwidth-Max-UP (7) VSA Length: Variable. The attribute contains the maximum uplink value in bits per second.
Vendor-Specific	26	O	Integer	Vendor ID: WISPr: 14122. VSA: WISPr-Bandwidth-Max-DOWN (8). VSA Length: Variable. The attribute contains the maximum downlink value in bits per second.

Attribute	Attribute ID	Presence	Type	Description
Vendor-Specific	26	M	Integer	Vendor ID: Microsoft 311. VSA: MS-MPPE-Send-Key (16). VSA Length: Variable. This attribute contains a session key used by Microsoft Point-to-Point Encryption Protocol (MPPE).
Vendor-Specific	26	M	Integer	Vendor ID: Microsoft 311. VSA: MS-MPPE-Recv-Key (17). VSA Length: Variable. This attribute contains a session key used by the Microsoft Point-to-Point Encryption Protocol (MPPE).
Vendor-Specific	26	C	String	Vendor ID: Ruckus:25053. VSA: Ruckus-IMSI (102). VSA Length: Variable. BCD encoded IMSI of the subscriber.
Vendor-Specific	26	C	Integer	Vendor ID: Ruckus:25053. VSA: Ruckus-Session-Type (125). VSA Length: 6. Session Type - TTG (2), Local-Breakout(3), Local-Breakout-AP(4), L3oGRE (5), L2oGRE (6), QinQL3 (7), PMIP (8). The controller server uses this attribute on the access -accept to indicate the forward policy of the specific UE.

Attribute	Attribute ID	Presence	Type	Description
Vendor-Specific	26	C	Integer	Vendor ID: Ruckus:25053. VSA: Ruckus-Acct-Status (126). VSA Length: 6. Acct Stat is true(1) or false(0). The controller server uses this attribute on the access accept to indicate if the authenticator needs to send the accounting start for the current/specified client.
Session-Timeout	27	O	Integer	This attribute sets the maximum number of seconds of service to be provided to the user before termination of the session.
Idle-Timeout	28	O	Integer	It sets the maximum number of consecutive seconds of idle connection allowed to the user before termination of the session.
Termination-Action	29	O	Integer	Indicates the action that NAS will take when the specified service is completed.
Proxy-State	33	O	Octets	This attribute is available to be sent by a proxy server (controller) to another server (AAA server) when forwarding an access request, accounting request (start, stop or interim) and must be returned unmodified in the access accept, access reject, access challenge and accounting response.
Tunnel-Type	64	C	Integer	This attribute indicates the tunnel type for the access point. For example, tunnel type 13 is for VLAN.
Tunnel-Medium-Type	65	C	Integer	This attribute indicates the tunnel medium type for the access point. For example, tunnel type 06 is for IEEE_802.

Attribute	Attribute ID	Presence	Type	Description
EAP Message	79	M	Octets	This attribute encapsulates Extensible Authentication Protocol (EAP) packets, which allows NAS to authenticate dial-in users via EAP, without having to understand the EAP protocol (EAP payload, EAP-SIM or EAP-AKA).
Message Authenticator	80	M	String	This attribute is used in signing access requests for preventing spoofing of access requests using CHAP, ARAP or EAP authentication methods. It authenticates this whole RADIUS packet - HMAC-MD5 (Type| Identifier | Length | Request Authenticator | Attributes).
Tunnel-Private-Group-ID	81	C	String	This attribute contains the dynamic VLAN ID as configured in the authentication profile.
Accounting-Interim-Interval	85	O	Integer	Indicates the number of seconds between each interim update for this specific session. If the value is blank, the configured default value is used as the accounting interim interval.
Basic-Location-Policy-Rules	129	C	Octets	This attribute provides the basic privacy policy associated to the location information. It is encoded as per RFC 5580. **NOTE** This attribute is expected from the AAA server if the location delivery method is accounting request as specified in RFC 5580.

Attribute	Attribute ID	Presence	Type	Description
Extended-Location-Policy-Rules	130	C	Octets	This attribute provides the extended privacy policy for the target whose location is specified.This attribute is sent with the above attribute (basic location policy). It is encoded as per RFC 5580. **NOTE** This attribute is expected from the AAA server if the location delivery method is accounting request as specified in RFC 5580.
Requested-Location-Info	132	M	Integer	This attribute is only used in messages sent by the AAA server towards the AP. Using this attribute the AAA server indicates its request for location information. Encoded as per RFC 5580. **NOTE** This attribute is expected from the AAA server if the location delivery method is accounting request as specified in RFC 5580.

Authorization Access Request

The authorization procedure starts after successful authentication only. Messages are initiated from the controller. The table lists the attribute details for messages sent by the controller to the AAA server.

Table 18: Authorisation Access request attributes

Attribute	Attribute ID	Presence	Type	Description
User-Name	1	M	String	Indicates the name of the user to be authenticated.

Attribute	Attribute ID	Presence	Type	Description
Vendor-Specific	26	C	Integer	Vendor ID: Ruckus VSA: 25053 VSA: Ruckus-SGSN-Number(124) VSA Length: Variable. AAA uses this attribute to populate the MAP update GPRS location. E.164 address of SGSN (controller). Ruckus VSAs are received from Ruckus APs only. It is optional for 3rd party APs.
Vendor-Specific	26	C	String	Vendor ID: Ruckus: 25053 VSA: Ruckus-SSID (3) VSA Length: Variable. Reports the associated WLANs SSID in access request and accounting packet. Ruckus VSAs are received from Ruckus APs only. It is optional for 3rd party APs.
Vendor-Specific	26	C	String	Vendor ID: Ruckus: 25053 VSA: Ruckus-Location (5) VSA Length: Variable. Reports the device location for this AP. This is a configurable value in the device location setting. Ruckus VSA is received only from Ruckus AP. It is optional for 3rd party APs.
NAS-Identifier	32	C	Integer	NAS-IP-Address or NAS-Identifier attribute is mandatory in received messages. It supports 3 types of values, namely BSSID (MAC address of the WLAN on AP), AP-MAC (MAC address of AP) and user defined address (maximum length of 62).
Proxy-State	33	O	Octets	This attribute is available to be sent by a proxy server (controller) to another server (AAA server) when forwarding an access request, accounting request (start, stop or interim) and must be returned unmodified in the access accept, access reject, access challenge and accounting response.
Chargeable User ID	89	M	String	This attribute sends a null value during authentication.

Authorization Access Accept

The authorization procedure starts only after successful authorization, where messages are sent by AAA to the controller. Information received from AAA is used in setting the GTP tunnel towards the GGSN (APN, QoS and Charging Characteristics).

The table lists the attribute details for messages sent by the AAA server to the controller.

Table 19: Authorization access accept attributes

Attribute	Attribute ID	Presence	Type	Description
User-Name	1	O	String	Indicates the name of the user for authentication.
Filter-Id	11	O	String	Represents the User Role name sent by AAA. This is used by the controller to map the received Group Role Name to the UTP profile and forward the corresponding ACL/rate limiting parameters to NAS. NAS enforces the UTP for the given user. Filter-Id might be included in access accept irrespective of a WISPr, 802.1x or HS 2.0 call.
Vendor-Specific	26	O	Integer	Vendor ID: WISPr: 14122 VSA: WISPr-Bandwidth-Max-UP (7) VSA Length: Variable. The attribute contains the maximum uplink value in bits per second.
Vendor-Specific	26	O	Integer	Vendor ID: WISPr: 14122 VSA: WISPr-Bandwidth-Max-DOWN (8) VSA Length: Variable. The attribute contains the maximum downlink value in bits per second.
Vendor-Specific	26	O	Octets	Vendor ID: Ruckus: 25053 VSA: Ruckus-APN-NI(104) VSA Length: Variable. This attribute carries the APN subscribed by the user. It contains only the network identifier (NI), which is part of the APN. The operator identifier part is stored separately in Ruckus-APN-OI.

Attribute	Attribute ID	Presence	Type	Description
Vendor-Specific	26	O	String	Vendor ID: 3GPP: 10415 VSA:3GPP-GPRS-Negotiated-QoS-Profile (5) VSA Length: Variable. This attribute carries the QoS value from AAA server. QoS from AAA is received from Ruckus defined VSA or from 3GPP defined VSA (3GPP-GPRS-Negotiated-QoS Profile).
Vendor-Specific	26	O	Charging characteristics	Vendor ID: Ruckus: 25053 VSA: Ruckus-Charging-Charac (118) VSA Length: 4 Charging characteristics value, octets are encoded according to TS 3GPP 32.215. This attribute carries the charging characteristics value, which is received from the AAA server.
Session-Timeout	27	O	Integer	This attribute de-authenticates the UE when the session time expires.
Proxy-State	33	O	Octets	This attribute is available to be sent by a proxy server (controller) to another server (AAA server) when forwarding an access request, accounting request (start, stop or interim) and must be returned unmodified in the access accept, access reject, access challenge and accounting response.
Acct-Interim-Interval	85	O	Integer	Indicates the number of seconds between each interim update for this specific session. If the value is blank, the configured default value is used as the accounting interim interval.
Chargeable User ID	89	M	String	This attribute sends a null value during authentication.

RADIUS Access Reject

The table lists the attribute details of access reject messages (failure scenarios) sent by the AAA in case of unsuccessful authentication or authorization. The controller can also initiate access reject towards NAS, based on certain use cases.

Table 20: RADIUS access reject attributes

Attribute	Attribute ID	Presence	Type	Description
Reply-Message	18	O	Integer	Indicates the text, which could be displayed to the user.
EAP Message	79	C	Octets	This attribute encapsulates Extensible Authentication Protocol (EAP) packets, which allows NAS to authenticate dial-in users via EAP, without having to understand the EAP protocol (EAP payload, EAP-SIM or EAP-AKA).
Message Authenticator	80	C	Octets	This attribute is used for signing access requests for preventing spoofing of access requests using CHAP, ARAP or EAP authentication methods. It authenticates this whole RADIUS packet - HMAC-MD5 (Type| Identifier | Length | Request Authenticator | Attributes). This attribute is available only for EAP failures.

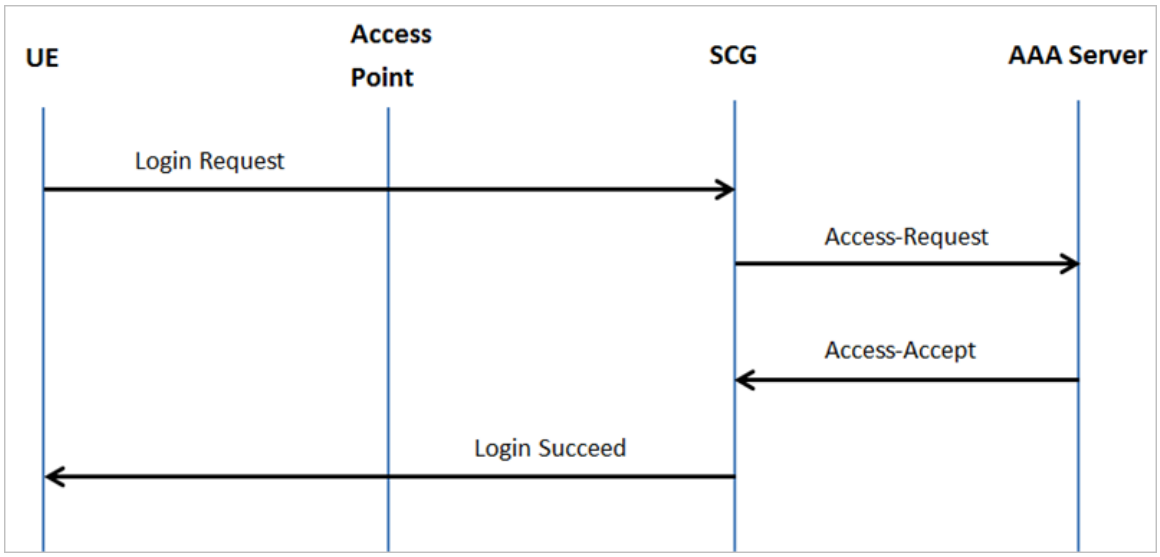
Hotspot (WISPr) Authentication and Accounting Overview

2

Hotspot (WISPr) authentication starts after a user has entered his or her logon credentials (user name and password) on the subscriber portal logon page. After this, the northbound portal interface initiates an *access request* message to process a service authorization.

Additional parameters can be provided by the AAA server in the access accept message. These parameters define the limitations and behavior of a specific user, such as session timeout, grace period and idle timeout.The figure shows the detailed call flow.

Figure 3: Hotspot (WISPr) call flow



This section covers:

- Hotspot (WISPr) Authentication Request
- Hotspot (WISPr) Authentication Response
- Hotspot (WISPr) Accounting Request [Start]

Hotspot (WISPr) Authentication Request

The table lists the attribute details of messages sent by the controller to Hotspot (WISPr).

NOTE These attributes are sent in the *Access-Request* only if *Client Fingerprinting* is enabled. To enable this option in the controller web interface navigate to **Access Points** > **Zone Tab** > **WLANs** > **Advanced Options** > **Select Enable Client Fingerprinting**.

Figure 4: Enable Client Fingerprinting

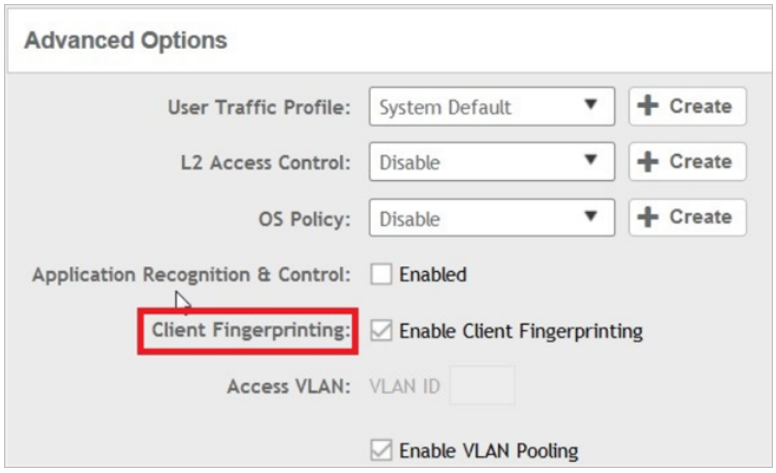


Table 21: Hotspot (WISPr) authentication request attributes

Attribute	Attribute ID	Presence	Type	Description
User-Name	1	M	String	This attribute is the logon user name.
User-Password	2	C	String	This attribute indicates the password of the user to be authenticated. This attribute is mandatory for PAP authentication.
CHAP-Password	3	M	String	Indicates the value provided by a CHAP user in response to the access-challenge. It is mandatory for CHAP authentication.
NAS-IP-Address	4	C	IP Address	This attribute contains the controller management IP address.
Service-Type	6	O	Integer	This attribute has the value 1 (login).
Framed-IP-Address	8	O	IP Address	This attribute is STA's IP address.

Attribute	Attribute ID	Presence	Type	Description
Framed MTU	12	O	Integer	Indicates the Maximum Transmission Unit (MTU) to be configured for the user, when it is not negotiated by some other means. **NOTE** The attribute will not be available if the MTU size is set to auto in the WLAN configuration page of the controller Web interface.
Vendor-Specific	26	O	Integer	Vendor ID: WISPr: 14122 Vendor Type: 1 VSA: WISPr-Location-ID VSA Length: Variable This attribute is a configurable value in the hotspot (WISPr) user interface.
Vendor-Specific	26	O	Integer	Vendor ID: WISPr: 14122 Vendor Type: 2 VSA: WISPr-Location-Name VSA Length: Variable This attribute is a configurable value in the hotspot (WISPr) user interface.
Vendor-Specific	26	O	Integer	Vendor ID: WISPr: 14122 Vendor Type: 3 VSA: WISPr-Logoff-URL VSA Length: Variable This attribute indicates the hotspot (WISPr) service logout URL.
Vendor-Specific	26	O	String	Vendor ID: Ruckus Vendor Type: 3 VSA: Ruckus-Client-Host-name VSA Length: 138 This attribute reports the configured client host name

Attribute	Attribute ID	Presence	Type	Description
Vendor-Specific	26	O	String	Vendor ID: Ruckus Vendor Type: 3 VSA: Ruckus-Client-Os-Type VSA Length: 139 This attribute reports the Client OS Type.
Vendor-Specific	26	O	String	Vendor ID: Ruckus Vendor Type: 3 VSA:Ruckus-Client-Os-Class VSA Length: Variable This attribute reports the client OS class
Vendor-Specific	26	O	String	Vendor ID: WISPr: 25053 Vendor Type: 3 VSA: Ruckus-SSID (3) VSA Length: Variable Reports the associated WLANs SSID in the access request and accounting packet, Ruckus VSA is received only from Ruckus AP.
Vendor-Specific	26	C	Integer	Vendor ID: Ruckus:25053 VSA: Ruckus-Zone-ID (127) VSA Length: 6 Reports the zone ID to which the 3rd party AP is associated. This VSA is received only for 3rd party APs.
Called Station ID	30	M	Integer	This attribute allows NAS to send the ID (BSSID), which is called by the user. It is MAC of the AP. It supports 2 types of values, namely BSSID:SSID, where BSSID is the MAC address of the WLAN on AP. The second value is AP-MAC:SSID, where AP-MAC is the MAC address of the AP. The letters in the MAC address are in uppercase. For example: 11-22-33-AA-BB-CC:SSID.

Attribute	Attribute ID	Presence	Type	Description
Calling Station ID	31	M	String	STA's MAC address where the letters in the MAC address are in uppercase. For example, 11-22-33-AA-BB-CC.
NAS-Identifier	32	C	Integer	This attribute contains a string identifying the NAS originating the access request. It supports 3 types of values for BSSID (MAC address of the WLAN on AP). AP-MAC (MAC address of AP) is a user defined attribute where the maximum length is 62. This attribute can also be configured as per the configuration specified on the WLAN configuration page of the controller web interface. This attribute can also be configured as per the configuration specified on the WLAN configuration page of the controller web interface.
Chap-Challenge	60	M	String	This attribute contains the chap challenge sent by NAS to a PPP CHAP user.
NAS-Port-Type	61	O	Integer	This attribute indicates the physical port type of the NAS, which authenticates the user.
Vendor-Specific	26	C	Integer	Vendor ID: Ruckus: 2503 Vendor Type: 9 VSA: VLAN-ID VSA Length: Variable This attribute value is as per the configuration specified on the WLAN configuration page of the controller web interface.
Operator-Name	126	C	String	The attribute identifies the owner of the access network by the AAA server. It is encoded as per RFC 5580. **NOTE** This attribute is included in the first access request when the location delivery method is Out of Band. If the location delivery method is the initial request then the subsequent access request is included in this parameter - as specified in RFC 5580.

Attribute	Attribute ID	Presence	Type	Description
Location-Information	127	C	Octets	This is a composite attribute, which provides meta data about the location information. It is encoded as per RFC 5580. **NOTE** This attribute is included in the first access request when the location delivery method is Out of Band. If the location delivery method is the initial request then the subsequent access request is included in this parameter - as specified in RFC 5580.
Location-Data	128	M	String	This attribute contains the actual location information. It is encoded as per RFC 5580. **NOTE** This attribute is included in the first access request when the location delivery method is Out of Band. If the location delivery method is the initial request then the subsequent access request is included in this parameter - as specified in RFC 5580.
Basic-Location-Policy-Rules	129	M	String	This attribute provides the basic privacy policy associated to the location information. It is encoded as per RFC 5580. **NOTE** This attribute is included in the first access request when the location delivery method is Out of Band. If the location delivery method is the initial request then the subsequent access request is included in this parameter - as specified in RFC 5580.
Extended-Location-Policy-Rules	130	C	Octets	This attribute provides the extended privacy policy for the target whose location is specified.This attribute is sent with the above attribute (*basic location policy*). It is encoded as per RFC 5580. **NOTE** This attribute is included in the first access request when the location delivery method is Out of Band. If the location delivery method is the initial request then the subsequent access request is included in this parameter - as specified in RFC 5580.

Attribute	Attribute ID	Presence	Type	Description
Location-Capable	131	C	Integer	This attribute is sent in RADIUS access request during the authentication phase to indicate the AP's capability for providing the location. Encoded as per RFC 5580. **NOTE** This attribute is included only if the location delivery method is the initial request or accounting request as specified in RFC 5580.

NOTE Acct-Session-Id shall be optionally included in the WISPr Access Request by Ruckus AP if Accounting is disabled in the UI.

Hotspot (WISPr) Authentication Response

The table lists the attribute details of messages sent by the Hotspot (WISPr) module to the controller.

Table 22: Hotspot (WISPr) authentication request attributes

Attribute	Attribute ID	Presence	Type	Description
Filter-Id	11	O	String	Represents the User Role name sent by AAA. This is used by SCG to map the received Group Role Name to the UTP profile and forward the corresponding ACL/rate limiting parameters to NAS. NAS enforces the UTP for the given user. Filter-Id might be included in access accept irrespective of a WISPr, 802.1x or HS 2.0 call.
Class	25	O	Integer	This attribute is sent by the server in access accept and the client should include this attribute in the accounting request without any modification.
Vendor-Specific	26	O	Integer	Vendor ID: WISPr: 14122 VSA: WISPr-Bandwidth-Max-UP (7) VSA Length: Variable The attribute contains the maximum uplink value in bits per second.

Attribute	Attribute ID	Presence	Type	Description
Vendor-Specific	26	O	Integer	Vendor ID: WISPr: 14122 VSA: WISPr-Bandwidth-Max-DOWN (8) VSA Length: Variable The attribute contains the maximum downlink value in bits per second.
Vendor-Specific	26	O	Integer	Vendor ID: Ruckus: 25053 Vendor Type: 7 VSA: Ruckus-Grace-Period VSA Length: Variable This attribute is the grace period in hotspot (WISPr) WLANs.
Session-Timeout	27	O	Integer	This attribute de-authenticates the UE when the session time expires.
Idle-Timeout	28	O	Integer	This attribute sets the maximum number of consecutive seconds of idle connection allowed to the user before termination of the session.
Accounting-Interim-Interval	85	O	Integer	Indicates the number of seconds between each interim update for this specific session. If the value is blank, the configured default value is used as the accounting interim interval.
Basic-Location-Policy-Rules	129	M	String	This attribute provides the basic privacy policy associated to the location information. It is encoded as per RFC 5580. **NOTE** This attribute is expected from the AAA server in the initial request location delivery method as mentioned in RFC 5580.
Extended-Location-Policy-Rules	130	C	Octets	This attribute provides the extended privacy policy for the target whose location is specified.This attribute is sent with the above attribute (*basic location policy*). It is encoded as per RFC 5580. **NOTE** This attribute is expected from the AAA server in the initial request location delivery method as mentioned in RFC 5580.

Attribute	Attribute ID	Presence	Type	Description
RequestedLocationInfo	132	M	Integer	This attribute is only used in messages sent by the AAA server towards the AP. Using this attribute the AAA server indicates its request for location information. Encoded as per RFC 5580. **NOTE** This attribute is expected from the AAA server in the initial request location delivery method as mentioned in RFC 5580.

Hotspot (WISPr) Accounting Request [Start]

The table lists the attribute details of messages sent by the controller to the Hotspot (WISPr) module.

Table 23: Hotspot (WISPr) accounting request (start) attributes

Attribute	Attribute ID	Presence	Type	Description
User-Name	1	M	String	This attribute is the logon user name.
NAS-IP-Address	4	C	IP Address	This attribute is the IP address of the AP which is serving the station or controller's control IP address, controller's management IP address and user defined value.
NAS-Port	5	O	Integer	This attribute is the AID value.
FramedIP-Address	8	O	IP Address	This attribute is STA's IP address.
Class	25	O	Integer	This attribute is sent by the server in access accept and the client should include this attribute in the accounting request without modification.
Vendor-Specific	26	O	Integer	Vendor ID: WISPr: 14122 Vendor Type: 1 VSA: WISPr-Location-ID VSA Length: Variable This attribute is a configurable value in the hotspot (WISPr) user interface.

Attribute	Attribute ID	Presence	Type	Description
Vendor-Specific	26	O	Integer	Vendor ID: WISPr: 14122 Vendor Type: 2 VSA: WISPr-Location-Name VSA Length: Variable This attribute is a configurable value in the hotspot (WISPr) user interface.
Vendor-Specific	26	O	Integer	Vendor ID: Ruckus: 25053 Vendor Type: 2 VSA: Ruckus-STA-RSSI (2) VSA Length: Variable This attribute can only be present with Acct-Status-Type = Interim or Stop.
Vendor-Specific	26	O	String	Vendor ID: Ruckus: 25053 Vendor Type: 3 VSA: Ruckus-SSID (3) VSA Length: Variable Reports the associated WLANs SSID in the access request and accounting packet, Ruckus VSA is received only from Ruckus AP.
Vendor-Specific	26	O	String	Vendor ID: Ruckus: 25053 Vendor Type: 5 VSA: Ruckus-Location VSA Length: Variable Reports the device location for this AP. This is a configurable value in the device location setting. Ruckus VSA is received only from Ruckus AP. It is optional for 3rd party APs.

Attribute	Attribute ID	Presence	Type	Description
Vendor-Specific	26	O	Integer	Vendor ID: Ruckus: 25053 Vendor Type: 7 VSA: Ruckus-SCG-CBLADE-IP VSA VSA Length: 6 This attribute indicate the control plane IP address that is being used.
Vendor-Specific	26	O	Integer	Vendor ID: Ruckus: 25053 Vendor Type: 8 VSA: Ruckus-SCG-DBLADE-IP VSA VSA Length: 6 This attribute value is observed by NBI, when the GRE tunnel is set up.
Called Station ID	30	M	Integer	This attribute allows NAS to send the ID (BSSID), which is called by the user. It is MAC of the AP. It supports 2 types of values, namely BSSID:SSID, where BSSID is the MAC address of the WLAN on AP. The second value is AP-MAC:SSID, where AP-MAC is the MAC address of the AP.The letters in the MAC address are in uppercase.For example: 11-22-33-AA-BB-CC:SSID
Calling Station ID	31	M	String	STA's MAC address the letters in the MAC address are in uppercase. For example, 11-22-33-AA-BB-CC.
NAS-Identifier	32	C	Integer	This attribute contains a string identifying the NAS originating the access request. It supports 3 types of values for BSSID (MAC address of the WLAN on AP). AP-MAC (MAC address of AP) is a user defined attribute where the maximum length is 62. This attribute can also be configured as per the configuration specified on the WLAN configuration page of the controller web interface.

Attribute	Attribute ID	Presence	Type	Description
Proxy-State	33	O	Octets	This attribute is available to be sent by a proxy server (controller) to another server (AAA server) when forwarding an access request, accounting request (start, stop or interim) and must be returned unmodified in the access accept, access reject, access challenge and accounting response.
Acct-Status-Type	40	M	Integer	This attribute has the following values where 1 is Start, 2 is Stop, 3 is Interim, 7 are On and 8 are Off.
Acct-Delay-Time	41	C	Integer	This attribute can only be seen in accounting retry packets. This is a configurable option and by default this attribute is disabled.
Acct-Session-ID	44	M	Integer	This attribute is a unique accounting identity to facilitate easy matching of start, interim and stop records in a log file. The start, interim and stop records for a given session must have the same *Acct-Session-ID.*
Acct-Authentic	45	M	Integer	This attribute value in EAP 802.1X-Auth and hotspot (WISPr) is: 1 for RADIUS-Auth and 2 for MAC-Auth local.
Acct-Session-Time	46	M	Integer	This attribute can only be present with *Acct-Status-Type = Interim, Stop.*
Acct-Terminate-Cause	49	M	Integer	This attribute can only be present with *Acct-Status-Type = Stop.*
Acct-Mul-Session-ID	50	O	Integer	This attribute is hand-off between APs, which triggers new accounting session (stop followed by start) with different session identifiers. Acct-Multi-Session-ID retains the same ID to tie multiple sessions.
Acct-Link-Count	51	O	Integer	Count of links in a multi-link session, when an accounting record is generated.
Event-Timestamp	55	O	Integer	This attribute is included in the Accounting-Request packet to record the time that this event occurred on NAS. For example, in seconds since January 1, 2013 00:00 UTC.
NAS-Port-Type	61	O	Integer	This attribute indicates the physical port type of the NAS, which authenticates the user.

Attribute	Attribute ID	Presence	Type	Description
Connect-Info	77	O	String	This attribute is sent from the NAS to indicate the nature of the user's connection.
Location-Information	127	C	Octets	This is a composite attribute, which provides meta data about the location information. It is encoded as per RFC 5580.
Location-Data	128	M	String	This attribute contains the actual location information. It is encoded as per RFC 5580. **NOTE** This attribute is included only if the location delivery method is the accounting request as specified in RFC 5580.
Basic-Location-Policy-Rules	129	M	String	This attribute provides the basic privacy policy associated to the location information. It is encoded as per RFC 5580. **NOTE** This attribute is included only if the location delivery method is the accounting request as specified in RFC 5580.
Extended-Location-Policy-Rules	130	C	Octets	This attribute provides the extended privacy policy for the target whose location is specified.This attribute is sent with the above attribute (*basic location policy*). It is encoded as per RFC 5580. **NOTE** This attribute is included only if the location delivery method is the accounting request as specified in RFC 5580.

Hotspot (WISPr) Accounting Request [Stop/Interim]

The table lists the attribute details of messages sent by the controller to the Hotspot (WISPr) module.

Table 24: Hotspot (WISPr) accounting request (stop/interim) attributes

Attribute	Attribute ID	Presence	Type	Description
User-Name	1	M	String	This attribute is the logon user name.

Attribute	Attribute ID	Presence	Type	Description
NAS-IP-Address	4	C	Integer	This attribute is the IP address of the AP which is serving the station or controller's control IP address, controller's management IP address and user defined value.
NAS-Port	5	O	Integer	This attribute is the AID value.
Framed-IP-Address	8	O	IP Address	This attribute is STA's IP address.
Class	25	O	Integer	This attribute is sent by the server in access accept and the client should include this attribute in the accounting request without modification.
Vendor-Specific	26	O	Integer	Vendor ID: WISPr: 14122 Vendor Type: 1 VSA: WISPr-Location-ID VSA Length: Variable This attribute is a configurable value in the hotspot (WISPr) user interface.
Vendor-Specific	26	O	Integer	Vendor ID: WISPr: 14122 Vendor Type: 2 VSA: WISPr-Location-Name VSA Length: Variable This attribute is a configurable value in the hotspot (WISPr) user interface.
Vendor-Specific	26	O	Integer	Vendor ID: Ruckus: 25053 Vendor Type: 2 VSA: Ruckus-STA-RSSI (2) VSA Length: Variable This attribute can only be present with Acct-Status-Type = Interim or Stop.

Attribute	Attribute ID	Presence	Type	Description
Vendor-Specific	26	O	String	Vendor ID: Ruckus: 25053 Vendor Type: 3 VSA: Ruckus-SSID (3) VSA Length: Variable Reports the associated WLANs SSID in the access request and accounting packet, Ruckus VSA is received only from Ruckus AP.
Vendor-Specific	26	O	String	Vendor ID: Ruckus: 25053 Vendor Type: 5 VSA: Ruckus-Location VSA Length: Variable Reports the device location for this AP. This is a configurable value in the device location setting. Ruckus VSA is received only from Ruckus AP. It is optional for 3rd party APs.
Vendor-Specific	26	O	Integer	Vendor ID: Ruckus: 25053 Vendor Type: 7 VSA: Ruckus-SCG-CBLADE-IP VSA VSA Length: Variable This attribute indicate the control plane IP address that is being used.
Vendor-Specific	26	O	Integer	Vendor ID: Ruckus: 25053 Vendor Type: 8 VSA: Ruckus-SCG-DBLADE-IP VSA VSA Length: Variable This attribute value is observed by NBI, when the GRE tunnel is set up.

Attribute	Attribute ID	Presence	Type	Description
Called Station ID	30	M	Integer	This attribute allows NAS to send the ID (BSSID), which is called by the user. It is MAC of the AP. It supports 2 types of values, namely BSSID:SSID, where BSSID is the MAC address of the WLAN on AP. The second value is AP-MAC:SSID, where AP-MAC is the MAC address of the AP. The letters in the MAC address are in uppercase.For example: 11-22-33-AA-BB-CC:SSID
Calling Station ID	31	M	String	STA's MAC address the letters in the MAC address are in uppercase. For example, 11-22-33-AA-BB-CC.
NAS-Identifier	32	C	Integer	This attribute contains a string identifying the NAS originating the access request. It supports 3 types of values for BSSID (MAC address of the WLAN on AP). AP-MAC (MAC address of AP) is a user defined attribute where the maximum length is 62. This attribute can also be configured as per the configuration specified on the WLAN configuration page of the controller web interface.
Proxy-State	33	O	Octets	This attribute is available to be sent by a proxy server (controller) to another server (AAA server) when forwarding an access request, accounting request (start, stop or interim) and must be returned unmodified in the access accept, access reject, access challenge and accounting response.
Acct-Status-Type	40	M	Integer	This attribute has the following values where 1 is Start, 2 is Stop, 3 is Interim, 7 are On and 8 are Off.
Acct-Delay-Time	41	C	Integer	This attribute can only be seen in accounting retry packets. This is a configurable option and by default this attribute is disabled.
Acct-Input-Octets	42	M	Integer	This attribute indicates the number of octets received from the port over the course of this service provided.

Attribute	Attribute ID	Presence	Type	Description
Acct-Output-Octets	43	M	Integer	This attribute indicates the number of octets sent to the port in the course of delivering this service.
Acct-Session-ID	44	M	Integer	This attribute is a unique accounting identity to facilitate easy matching of start, interim and stop records in a log file. The start, interim and stop records for a given session must have the same *Acct-Session-ID.*
Acct-Authentic	45	M	Integer	This attribute value in EAP 802.1X-Auth and hotspot (WISPr) is: 1 for RADIUS-Auth and 2 for MAC-Auth local.
Acct-Terminate-Cause	49	M	Integer	This attribute can only be present with *Acct-Status-Type = Stop.*
Acct-Multi-Session-ID	50	O	Integer	This attribute is hand-off between APs, which triggers new accounting session (stop followed by start) with different session identifiers. Acct-Multi-Session-ID retains the same ID to tie multiple sessions.
Acct-Link-Count	51	O	Integer	Count of links in a multi-link session, when an accounting record is generated.
Acct-Input-Gigawords	52	M	Integer	This attribute can only be present with *Acct-Status-Type = Interim, Stop.*
Acct-Output-Gigawords	53	M	Integer	This attribute can only be present with *Acct-Status-Type = Interim, Stop.*
Event-Timestamp	55	O	Integer	This attribute is included in the Accounting-Request packet to record the time that this event occurred on NAS. For example, in seconds since January 1, 2013 00:00 UTC.
NAS-Port-Type	61	O	Integer	This attribute indicates the physical port type of the NAS, which authenticates the user.
Connect-Info	77	O	String	This attribute is sent from the NAS to indicate the nature of the user's connection.

Attribute	Attribute ID	Presence	Type	Description
Location-Information	127	C	Octets	This is a composite attribute, which provides meta data about the location information. It is encoded as per RFC 5580. **NOTE** This attribute is included only if the location delivery method is accounting request as specified in RFC 5580.
Location-Data	128	M	String	This attribute contains the actual location information. It is encoded as per RFC 5580. **NOTE** This attribute is included only if the location delivery method is accounting request as specified in RFC 5580.
Basic-Location-Policy-Rules	129	M	String	This attribute provides the basic privacy policy associated to the location information. It is encoded as per RFC 5580. **NOTE** This attribute is included only if the location delivery method is accounting request as specified in RFC 5580.
Extended-Location-Policy-Rules	130	C	Octets	This attribute provides the extended privacy policy for the target whose location is specified.This attribute is sent with the above attribute (*basic location policy*). It is encoded as per RFC 5580. **NOTE** This attribute is included only if the location delivery method is accounting request as specified in RFC 5580.

Hotspot (WISPr) Accounting Response

The table lists the attribute details of messages received by the controller to the Hotspot (WISPr) module.

Table 25: Hotspot (WISPr) accounting response attributes

Attribute	Presence	Type	Description
Response Authenticator	M	Integer	MD5(Code|ID|Length|RequestAuth|RequestAuth|RequestAuth|Attributes|Secret)

Hotspot 2.0 Authentication 3

Hotspot 2.0 WLAN supports 802.1x authentication and passpoint technology. Passpoint enabled devices (R2 devices) connect to the network automatically based on their PPS-MO and facilitates seamless roaming for users on Wi-Fi network.

WLAN supports Hotspot 2.0 Online SignUp (OSU) procedure and passpoint enabled devices, which connect to the network and are provisioned with PPS-MO. R2 users can onboard PPS-MO through authentication procedure using RADIUS credentials. Non SIM based authentication (EAP-TTLS) is supported as per the WFA RFC mandate for Hotspot 2.0 R2 devices. SIM based authentication (EAP SIM and EAP AKA) is supported as per the WFA RFC mandate for Hotspot 2.0 R1 devices.

SIM based authentication is similar to EAP - Full Authentication – 3GPP Solution except that RADIUS message include Hotspot 2.0 specific attributes. SIM based authentication is also applicable for R1 devices associated with Hotspot 2.0 WLAN and RADIUS messages are proxied to the external AAA server.

R2 devices are associated with Hotspot 2.0 WLAN on receiving the PPS-MO from the controller. Alternatively R2 devices can also get PPS-MO from remote OSU server and RADIUS request is proxied to external AAA server during access.

NOTE For this release, TTLS RADIUS authentication is supported. There is no support for EAP-SIM.

SIM Based Authentication - Access Request

SIM based authentication for Hotspot 2.0 devices is similar to EAP - Full Authentication – 3GPP Solution. In addition to the parameters mentioned in each of the following RADIUS access-accept. The table lists the attributes specific to Hotspot 2.0.

- RADIUS Access Request [ID]
- RADIUS Access Request [EAP Response (NONCE_MT)]
- RADIUS Access Request [EAP Response (SRES)]

Table 26: Hotspot 2.0 RADIUS access request attributes

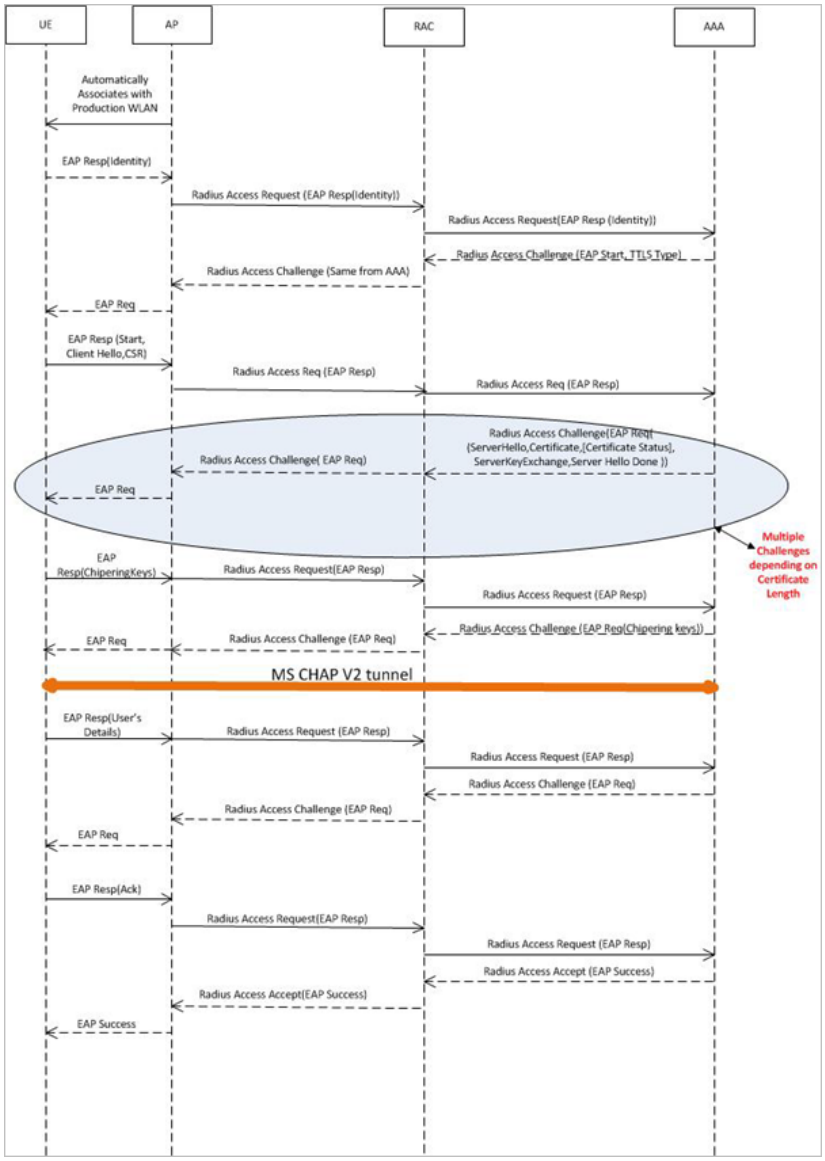
Attribute	Attribute ID	Presence	Type	Description
Vendor-Specific	26	C	String	Vendor ID: 40808 Vendor Type: 2 VSA: AP Version VSA Length: Variable This attribute indicates version 0 as R1 compliant AP and version 1as R2 compliant AP.
Vendor-Specific	26	C	String	Vendor ID: 40808 Vendor Type: 3 VSA: Mobile Device Version VSA Length: Variable This attribute indicates version 0 as R1 compliant AP and version 1 as R2 compliant AP. Version 1 also includes the update identifier details.

R2 Device Access Authentication

In the R2 device authentication where PPS-MO is provisioned by an external OSU, RADIUS access request is always proxied to the remote AAA server when the device connects to the Hotspot 2.0 WLAN. RAC proxies the request to the AAA server based on the realm configuration defined in **Services&Profiles > Hotspot 2.0** of the controller web interface.

The figure shows the call flow for R2 devices when PPS-MO is received from external OSU. RAC does not decode the EAP payload and certificate details. It merely proxy's the request based on the RADIUS user name attribute used in the request.

Figure 5: R2 device access authentication


UE
AP
RAC
AAA
Automatically Associates with Production WLAN
EAP Resp(Identity)
Radius Access Request (EAP Resp(Identity))
Radius Access Request(EAP Resp (Identity))
Radius Access Challenge (EAP Start, TTLS Type)
Radius Access Challenge (Same from AAA)
EAP Req
EAP Resp (Start, Client Hello,CSR)
Radius Access Req (EAP Resp)
Radius Access Req (EAP Resp)
Radius Access Challenge(EAP Req((ServerHello,Certificate,[Certificate Status], ServerKeyExchange,Server Hello Done))
Radius Access Challenge(EAP Req)
EAP Req
Multiple Challenges depending on Certificate Length
EAP Resp(ChiperingKeys)
Radius Access Request(EAP Resp)
Radius Access Request (EAP Resp)
Radius Access Challenge (EAP Req(Chipering keys))
EAP Req
Radius Access Challenge (EAP Req)
MS CHAP V2 tunnel
EAP Resp(User's Details)
Radius Access Request (EAP Resp)
Radius Access Request (EAP Resp)
Radius Access Challenge (EAP Req)
Radius Access Challenge (EAP Req)
EAP Req
EAP Resp(Ack)
Radius Access Request(EAP Resp)
Radius Access Request (EAP Resp)
Radius Access Accept (EAP Success)
Radius Access Accept(EAP Success)
EAP Success

Access Request

The table lists the attributes specific to Hotspot 2.0.

Table 27: Hotspot 2.0 RADIUS access request attributes

Attribute	Attribute ID	Presence	Type	Description
Vendor-Specific	26	C	String	Vendor ID: 40808 Vendor Type: 2 VSA: AP Version VSA Length: Variable This attribute indicates version 0 as R1 compliant AP and version 1as R2 compliant AP.
Vendor-Specific	26	C	String	Vendor ID: 40808 Vendor Type: 3 VSA: Mobile Device Version VSA Length: Variable This attribute indicates version 0 as R1 compliant AP and version 1 as R2 compliant AP. Version 1 also includes the update identifier details.

NOTE R2 access requests will have similar attributes as captured in EAP Full Authentication with a few exceptions:

- The Username in the access request will have the value 'anonymous@realm.com'. 'Realm.com' will vary depending on the NAI realm configured in the PPS-MO.
- The EAP message will carry an EAP-TTLS payload. It will be used to exchange certificate details and MSCHAPv2 credentials unlike EAP carrying EAP SIM credentials such as RAND, SRES, and Kc in EAP-SIM.

Access Response

The table lists the attributes specific to Hotspot 2.0.

An HS 2.0 R2 call will have RADIUS responses such as multiple access challenges and Access Accept as captured or EAP SIM full authentication. See the note at the end of the table.

Table 28: Hotspot 2.0 RADIUS access response attributes

Attribute	Attribute ID	Presence	Type	Description
Vendor-Specific	26	C	String	Vendor ID: 40808 Vendor Type: 1 VSA: Subscription Remediation Needed VSA Length: Variable This attribute provides the remediation URL.
Vendor-Specific	26	C	String	Vendor ID: 40808 Vendor Type: 4 VSA: De-authentication Request VSA Length: Variable This attribute is applicable only for R2 devices. It gives the de-authenticated URL and the re-authentication delay.

Attribute	Attribute ID	Presence	Type	Description
Vendor-Specific	26	C	String	Vendor ID: 40808 Vendor Type: 5 VSA: Session Information URL VSA Length: Variable This attribute provides the URL details seen before session termination.

NOTE The EAP message for the HS 2.0 R2 call will have TLS and MSCHAPv2 credentials instead of SIM.

NOTE Attributes such as Client Hello, Server Hello are standard TLS 1.0 specific attributes and are embedded within EAP. For details refer to RFC 2246.

R2 Device Onboarding

The UE can onboard with a controller using AAA credentials, where the controller proxys the onboarding requests to AAA.

Onboarding Access Request

The details in the access request are as follows:

Table 29: Onboarding Access Request

Attribute	Attribute ID	Presence	Type	Description
NAS-Port-Type	61	M	Integer	Indicates the physical port type of NAS, which authenticates the user.
NAS-Port	5	O	Integer	This attribute indicates the physical port number of the NAS which authenticates the user. The controller uses the association ID for the STA in the AP to represent this.

Attribute	Attribute ID	Presence	Type	Description
User-Name	1	M	String	Indicates the name of the user for authentication.
User-Password	2	C	String	This attribute indicates the password of the user to be authenticated. It is mandatory for PAP authentication.
Calling Station ID	31	O	String	This attribute will contain the Calling Station ID as received from NAS during authentication or the accounting procedure
Message Authenticator	80	O	Octets	This attribute is used to sign *access requests* to prevent spoofing access requests using CHAP, ARAP or EAP authentication methods. It authenticates this whole RADIUS packet - HMAC-MD5 (Type| Identifier | Length | Request Authenticator | Attributes).
NAS-IP-address	4	C	IP Address	This attribute is the IP address of the AP which is serving the station or controller's control IP address, controller's management IP address and user defined value.
Proxy-State	33	O	Octets	This attribute is available to be sent by a proxy server to another server.

Onboarding Access Response

The details in the access response are as follows:

Table 30: Onboarding Access Response

Attribute	Attribute ID	Presence	Type	Description
Proxy-State	33	O	Octets	This attribute is available to be sent by a proxy server to another server.
Filter-Id	11	O	String	Represents the User Role name sent by AAA. This is used by SCG to map the received Group Role Name to the UTP profile and forward the corresponding ACL/rate limiting parameters to NAS. NAS enforces the UTP for the given user. Filter-Id might be included in access accept irrespective of a WISPr, 802.1x or HS 2.0 call.

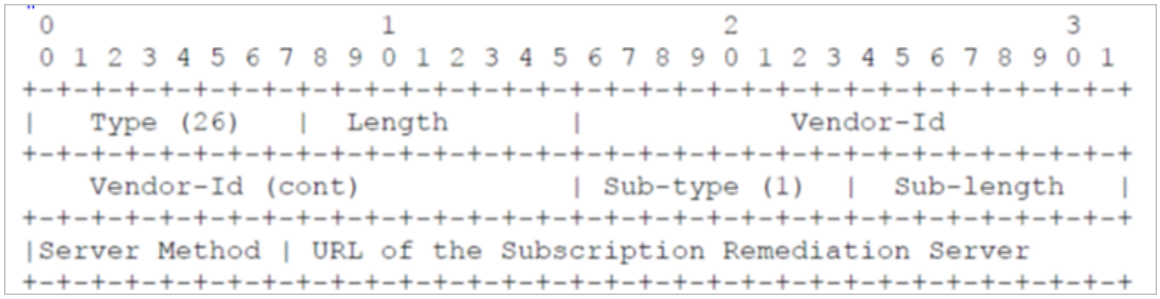
Attribute	Attribute ID	Presence	Type	Description
WISPr uplink	26	O	Integer	Vendor ID: WISPr: 14122 VSA: WISPr-Bandwidth-Max-UP (7) VSA Length: Variable The attribute contains the maximum uplink value in bits per second.
WISPr downlink	26	O	Integer	Vendor ID: WISPr: 14122 VSA: WISPr-Bandwidth-Max-DOWN (8) VSA Length: Variable The attribute contains the maximum downlink value in bits per second.

Hotspot 2.0 VSAs

There are vendor specific attributes for Hotspot 2.0 as mandated by WFA Hotspot 2.0 specifications along with the regular RADIUS message attributes (as per RFC 2865).

The figure indicates the VSA fields in a hotspot 2.0 subscription remediation flow.

Figure 6: Hotspot 2.0 VSA fields

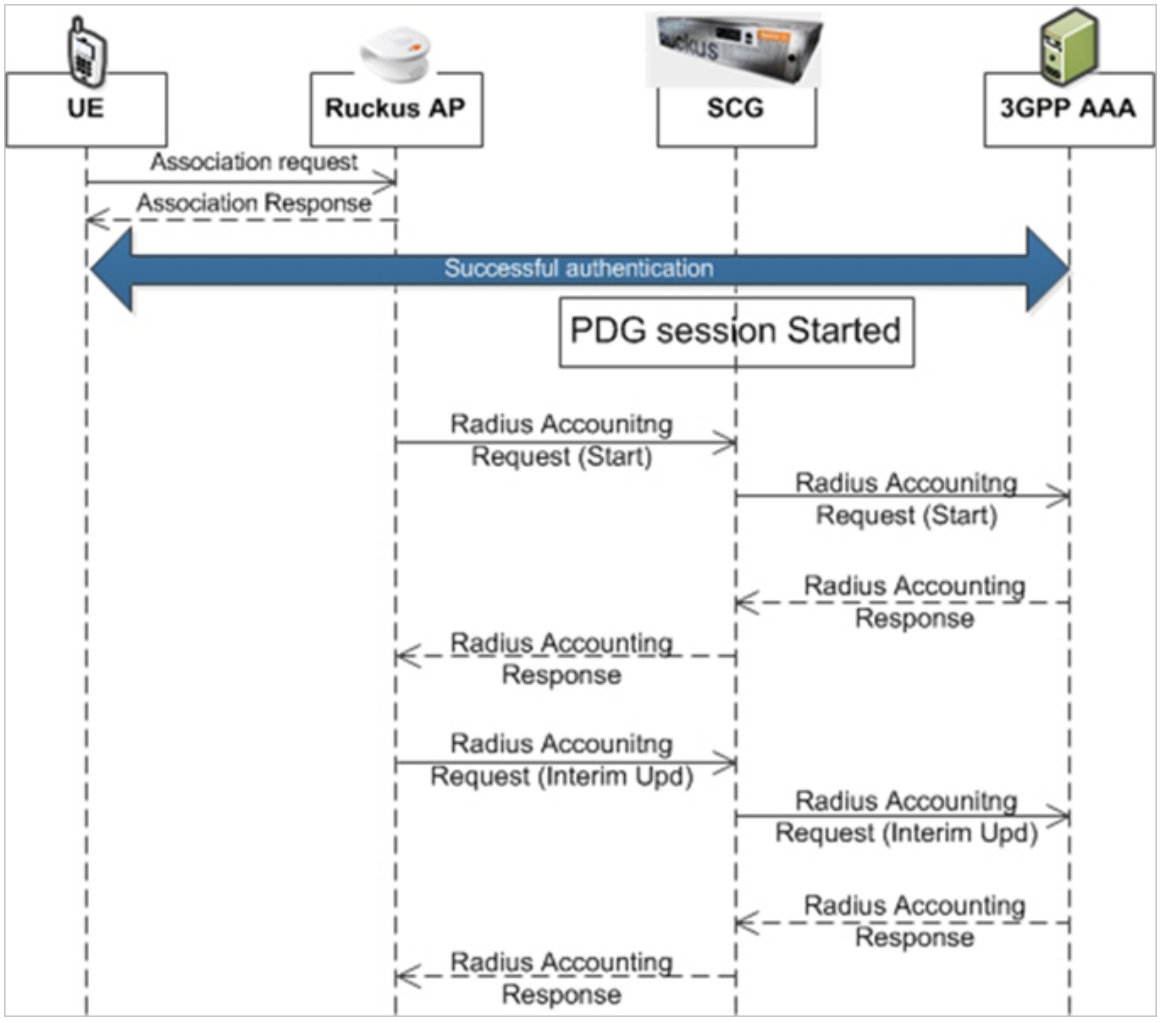


AP Initiated Accounting Messages (PDG/LBO Sessions) 4

The controller honors RADIUS accounting messages received from AP, for both Ruckus AP and 3rd Party AP. For accounting messages from AP, controller generates W-AN-CDR/S-CDR/W-CDR as configured in the controller UI (non-proxy mode), or proxy accounting messages received from AP to configured external AAA server (proxy mode).

The figure shows the controller proxy accounting messages from NAS to external AAA server.

Figure 7: AP initiated accounting messages



This section covers:

Accounting Start Messages

The table lists the attribute details of messages sent by the controller to the AAA server.

Table 31: Accounting start message attributes

Attribute	Attribute ID	Presence	Type	Description
User-Name	1	M	String	The username of the given accounting session.
NAS-IP-Address	4	C	IP Address	This attribute is the IP address of the AP which is serving the station or user equipment, controller's control IP address, controller's management IP address and user defined value.

Attribute	Attribute ID	Presence	Type	Description
NAS-Port	5	O	Integer	This attribute indicates the physical port number of the NAS which authenticates the user. The controller uses the association ID for the STA in the AP to represent this.
Framed-IP-Address	8	O	IP Address	This attribute indicates the address to be configured for the user.
Vendor-Specific	26	C	String	Vendor ID: Ruckus:25053 VSA: Ruckus-SSID (3) VSA Length: Variable Reports the associated WLANs SSID in access request and accounting packet. Ruckus VSAs are received from Ruckus APs only. It is optional for 3rd party APs.

Attribute	Attribute ID	Presence	Type	Description
Vendor-Specific	26	C	String	Vendor ID: Ruckus:25053 VSA: Ruckus-Location (5) VSA Length: Variable Reports the device location for this AP. This is a configurable value in the device location setting. Ruckus VSA is received only from Ruckus AP. It is optional for 3rd party APs.
Vendor-Specific	26	C	Integer	Vendor ID: Ruckus:25053 VSA: Ruckus- SCG-CBLADE- IP (7) VSA Length: 6 Reports the control plane IP address. Ruckus VSAs are received from Ruckus APs only. It is optional for 3rd party APs.

Attribute	Attribute ID	Presence	Type	Description
Vendor-Specific	26	C	Integer	Vendor ID: Ruckus:25053 VSA: Ruckus-SCG- DBLADE- IP (8) VSA Length: 6 Reports the data plane IP address. Ruckus VSA is received only from Ruckus AP. It is optional for 3rd party APs.
Called Station ID	30	O	Integer	This attribute supports two kinds of formats, namely, BSSID:SSID, which is the MAC address of the WLAN on AP and AP-MAC:SSID which is the MAC address of AP. The letters in the MAC address are in uppercase. For example: 112233AABBCCSSID.

Attribute	Attribute ID	Presence	Type	Description
Calling Station ID	31	O	String	Allows NAS to send the ID (UE MAC), which indicates as to who is calling the STA's MAC address. The letters in the MAC address are in uppercase. For example: 11-22-33-AA-BB-CC.
NAS-Identifier	32	C	Integer	NAS-IP-Address or NAS-Identifier attribute is mandatory in received messages. It supports 3 types of values, namely BSSID (MAC address of the WLAN on AP), AP-MAC (MAC address of AP) and user defined address (maximum length of 62).

Attribute	Attribute ID	Presence	Type	Description
Proxy-State	33	C	Octets	This attribute is available to be sent by a proxy server (controller) to another server (AAA server) when forwarding an access request, accounting request (start, stop or interim) and must be returned unmodified in the access accept, access reject, access challenge and accounting response.
Acct-Status-Type	40	M	Integer	This attribute indicates whether the *Accounting-Request* attribute marks the beginning of the user service (Start). Start value is 1.

Attribute	Attribute ID	Presence	Type	Description
Acct-Delay-Time	41	C	Integer	This is a configurable option and by default this attribute is disabled.In case the accounting message gets retransmitted, this attribute contains the time stamp of the consecutive retransmitted message.
Acct-Session-ID	44	M	Integer	This attribute is a unique accounting identity to facilitate easy matching of start, interim and stop records in a log file. The start, interim and stop records for a given session must have the same *Acct-Session-ID.*
Acct-Authentic	45	M	Integer	This attribute indicates whether the user was authenticated through RADIUS server or NAS or remote authentication protocol.

Attribute	Attribute ID	Presence	Type	Description
Acct-Multi-Session-ID	50	O	Integer	This attribute is a unique Accounting ID, to link multiple related sessions in a log file
Acct-Link-Count	51	O	Integer	Count of links in a multi-link session, when an accounting record is generated.
Event-Timestamp	55	O	Integer	This attribute is included in the accounting-request packet for recording the time in seconds that the event occurred on NAS. For example, January 1, 2013 00:00 UTC.
NAS-Port-Type	61	O	Integer	Indicates the physical port type of NAS, which authenticates the user.
Connect-Info	77	O	String	This attribute is sent from the NAS to indicate the nature of the user's connection.
Chargeable User ID	89	C	String	This attribute is MSISDN or any chargeable user identity returned by the AAA server.

Attribute	Attribute ID	Presence	Type	Description
Location-Information	127	C	Octets	This is a composite attribute, which provides meta data about the location information. It is encoded as per RFC 5580. **NOTE** This attribute is included only when the expected location delivery method is accounting request as specified in RFC 5580.
Location-Data	128	M	String	This attribute contains the actual location information. It is encoded as per RFC 5580. **NOTE** This attribute is included only when the expected location delivery method is accounting request as specified in RFC 5580.

Attribute	Attribute ID	Presence	Type	Description
Basic-Location -Policy-Rules	129	C	Octets	This attribute provides the basic privacy policy associated to the location information. It is encoded as per RFC 5580. **NOTE** This attribute is included only when the expected location delivery method is accounting request as specified in RFC 5580.

Attribute	Attribute ID	Presence	Type	Description
Extended-Location -Policy-Rules	130	C	Octets	This attribute provides the extended privacy policy for the target whose location is specified.This attribute is sent with the above attribute (*basic location policy*). It is encoded as per RFC 5580. **NOTE** This attribute is included only when the expected location delivery method is accounting request as specified in RFC 5580.

Accounting Interim Update and Stop Messages

The table lists the attribute details of messages sent by the controller to AAA.

Table 32: Accounting interim update and stop message attributes

Attribute	Attribute ID	Presence	Type	Description
User-Name	1	M	String	The username of the given accounting session.

Attribute	Attribute ID	Presence	Type	Description
NAS-IP-Address	4	C	IP Address	This attribute is the IP address of the AP which is serving the station or controller's control IP address, controller's management IP address and user defined value.
NAS-Port	5	O	Integer	This attribute indicates the physical port number of the NAS which authenticates the user. The controller uses the association ID for the STA in the AP to represent this.
Framed-IP-Address	8	O	IP Address	This attribute indicates the address to be configured for the user.

Attribute	Attribute ID	Presence	Type	Description
Vendor-Specific	26	C	Integer	Vendor ID: Ruckus:25053 VSA: Ruckus-STA-RSSI (2) VSA Length: 6 UE reports the current RSSI value in the accounting packet. Ruckus VSA is received only from Ruckus AP.
Vendor-Specific	26	C	String	Vendor ID: Ruckus:25053 VSA: Ruckus-SSID (3) VSA Length: Variable Reports the associated WLANs SSID in the access request and accounting packet. Ruckus VSA is received only from Ruckus AP. It is optional for 3rd party APs.

Attribute	Attribute ID	Presence	Type	Description
Vendor-Specific	26	C	String	Vendor ID: Ruckus:25053 VSA: Ruckus-Location (5) VSA Length: Variable Reports the device location for this AP. This is a configurable value in the device location setting. Ruckus VSA is received only from Ruckus AP. It is optional for 3rd party APs.
Vendor-Specific	26	C	Integer	Vendor D: Ruckus:25053 VSA: RuckusSCGCBLADEIP (7) VSA Length: 6 Reports the control plane IP address. Ruckus VSA is received only from Ruckus AP. It is optional for 3rd party APs.

Attribute	Attribute ID	Presence	Type	Description
Vendor-Specific	26	C	Integer	Vendor ID: Ruckus:25053 VSA: RuckusSCGDPBLADEIP (8) VSA Length: 6 Reports the data plane address. Ruckus VSA is received only from Ruckus AP. It is optional for 3rd party APs.
Called Station ID	30	O	Integer	This attribute allows NAS to send the ID (BSSID), which is called by the user. It is MAC of the AP. It supports 2 types of values, namely BSSID:SSID, where BSSID is the MAC address of the WLAN on AP. The second value is AP-MAC:SSID, where AP-MAC is the MAC address of the AP. The letters in the MAC address are in uppercase.For example: 11:22:33:AA:BB:CC:SSID

Attribute	Attribute ID	Presence	Type	Description
Calling Station ID	31	O	String	Allows NAS to send the ID (UE MAC), which indicates as to who is calling this server.
NAS-Identifier	32	C	Integer	NAS-IP-Address or NAS-Identifier attribute is mandatory in received messages. It supports 3 types of values, namely BSSID (MAC address of the WLAN on AP), AP-MAC (MAC address of AP) and user defined address (maximum length of 62).
Proxy-State	33	O	Octets	This attribute is available to be sent by a proxy server (controller) to another server (AAA server) when forwarding an access request, accounting request (start, stop or interim) and must be returned unmodified in the access accept, access reject, access challenge and accounting response.

Attribute	Attribute ID	Presence	Type	Description
Acct-Status-Type	40	M	Integer	Value differs based on message type. Attribute *interim update* has the value 3 and *stop* has the value 2.
Acct-Delay-Time	41	C	Integer	This is a configurable option and by default this attribute is disabled. In case the accounting message gets retransmitted, this attribute contains the time stamp of the consecutive retransmitted message.
Acct-Input-Octets	42	M	Integer	This attribute indicates the number of octets received from the port over the course of the service provided. This attribute is present in *Acct-Status-Type = Interim Stop*
Acct-Output-Octets	43	M	Integer	This attribute indicates the number of octets sent to the port in the course of delivering this service.

Attribute	Attribute ID	Presence	Type	Description
Acct-Session-ID	44	M	Integer	This attribute is a unique accounting identity to facilitate easy matching of start, interim and stop records in a log file. The start, interim and stop records for a given session must have the same *Acct-Session-ID.*
Acct-Authentic	45	M	Integer	This attribute indicates whether the user was authenticated through RADIUS server or NAS or remote authentication protocol.
Acct-Session-Time	46	M	Integer	This attribute indicates the number of seconds for receiving the service.
Acct-Input-Packets	47	M	Integer	This attribute indicates the number of packets received from the port over the course of the service provided to a framed user.

Attribute	Attribute ID	Presence	Type	Description
Acct-Output-Packets	48	M	Integer	This attribute indicates the number of packets sent from the port over the course of the service provided to a framed user.
Acct-Terminate-Cause	49	M	Integer	This attribute indicates how the session was terminated. This attribute can only be present in accounting request records where the Acct-Status-Type is set to Stop.
Acct-Multi-Session-ID	50	O	Integer	This attribute is a unique Accounting ID, linking multiple related sessions in a log file.
Acct-Link--Count	51	O	Integer	Count of links in a multi-link session, when an accounting record is generated.
Acct-Input--Gigawords	52	M	Integer	This attribute indicates the number of times that the *Acct-Input-Octets* counter wraps around 2^32 over the course of this provided service.

Attribute	Attribute ID	Presence	Type	Description
Acct-Output--Gigawords	53	M	Integer	This attribute indicates the number of times the *Acct-Output-Octets* counter is wrapped around 2^32 in the course of delivering this service.
Event-Timestamp	55	O	Integer	This attribute is included in the accounting request packet to record the time (in seconds) that this event occurred on NAS. For example, January 1, 2013 00:00 UTC.
NAS-Port-Type	61	O	Integer	Indicates the physical port type of NAS, which authenticates the user.
Connect-Info	77	O	String	This attribute is sent from the NAS to indicate the nature of the user's connection.
Chargeable User ID	89	C	String	AP includes Chargeable User ID attribute along with the values received from the AAA server.

Attribute	Attribute ID	Presence	Type	Description
Location-Information	127	C	Octets	This is a composite attribute, which provides meta data about the location information. It is encoded as per RFC 5580. Note: This attribute is included only when the expected location delivery method is accounting request as specified in RFC 5580.
Location-Data	128	M	String	This attribute contains the actual location information. It is encoded as per RFC 5580. **NOTE** This attribute is included only when the expected location delivery method is accounting request as specified in RFC 5580.

Attribute	Attribute ID	Presence	Type	Description
Basic-Location--Policy-Rules	129	C	Octets	This attribute provides the basic privacy policy associated to the location information. It is encoded as per RFC 5580. **NOTE** This attribute is included only when the expected location delivery method is accounting request as specified in RFC 5580.

Attribute	Attribute ID	Presence	Type	Description
Extended-Location -Policy-Rules	130	C	Octets	This attribute provides the extended privacy policy for the target whose location is specified.This attribute is sent with the above attribute (*basic location policy*). It is encoded as per RFC 5580. **NOTE** This attribute is included only when the expected location delivery method is accounting request as specified in RFC 5580.

Accounting On Messages

The table lists the attribute details of messages sent by the controller to the AAA server.

Table 33: Accounting on message attributes

Attribute	Attribute ID	Presence	Type	Description
User-Name	1	M	String	The username of the given accounting session.

Attribute	Attribute ID	Presence	Type	Description
NAS-IP-Address	4	C	IP Address	This attribute is the IP address of the AP which is serving the station or controller's control IP address, controller's management IP address and user defined value.
Vendor-Specific	26	C	String	Vendor ID: Ruckus:25053 VSA: Ruckus-SSID (3) VSA Length: - Variable Reports the associated WLANs SSID in the access request and accounting packet, Ruckus VSA is received only from Ruckus AP. It is optional for 3rd party APs.

Attribute	Attribute ID	Presence	Type	Description
Vendor-Specific	26	C	String	Vendor ID: Ruckus:25053 VSA: Ruckus-Location (5) VSA Length: Variable Reports the device location for this AP. This is a configurable value in the device location setting. Ruckus VSA is received only from Ruckus AP. It is optional for 3rd party APs.
Vendor-Specific	26	C	Integer	Vendor ID: Ruckus:25053 VSA: Ruckus-SCG- CBLADE-IP (7) VSA Length: 6 Reports the control plane IP address. Ruckus VSA is received only from Ruckus AP. It is optional for 3rd party APs.

Attribute	Attribute ID	Presence	Type	Description
Vendor-Specific	26	C	Integer	Vendor ID: Ruckus:25053 VSA: Ruckus-SCG -DBLADE-IP (8) VSA Length: 6 Reports the data plane IP address. Ruckus VSA is received only from Ruckus AP. It is optional for 3rd party APs.

Attribute	Attribute ID	Presence	Type	Description
Called Station ID	30	O	Integer	This attribute allows NAS to send the ID (BSSID), which is called by the user. It is MAC of the AP. It supports 2 types of values, namely BSSID:SSID, where BSSID is the MAC address of the WLAN on AP. The second value is AP-MAC:SSID, where AP-MAC is the MAC address of the AP. The letters in the MAC address are in uppercase.For example: 11- 22-33- AA-BB-CC:SSID

Attribute	Attribute ID	Presence	Type	Description
NAS-Identifier	32	C	Integer	NAS-IP-Address or NAS-Identifier attribute is mandatory in received messages. It supports 3 types of values, namely BSSID (MAC address of the WLAN on AP), AP-MAC (MAC address of AP) and user defined address (maximum length of 62).
Proxy-State	33	O	Octets	This attribute is available to be sent by a proxy server (controller) to another server (AAA server) when forwarding an access request, accounting request (start, stop or interim) and must be returned unmodified in the access accept, access reject, access challenge and accounting response.

Attribute	Attribute ID	Presence	Type	Description
Acct-Status-Type	40	M	Integer	This attribute indicates whether the Accounting-Request attribute marks it as Accounting-On (7) and Accounting-Off (8).
Acct-Delay-Time	41	C	Integer	In case the accounting message gets retransmitted, this attribute contains the time stamp of the consecutive retransmitted message.
Acct-Authentic	45	M	Integer	This attribute indicates whether the user was authenticated through RADIUS server or NAS or remote authentication protocol.

Accounting Off Messages

The table lists the attribute details of messages sent by the controller to the AAA server.

Table 34: Accounting off message attributes

Attribute	Attribute ID	Presence	Type	Description
User-Name	1	M	String	The username of the given accounting session.

Attribute	Attribute ID	Presence	Type	Description
NAS-IP-Address	4	C	IP Address	This attribute is the IP address of the AP which is serving the station or controller's control IP address, controller's management IP address and user defined value.
Vendor-Specific	26	C	String	Vendor ID: Ruckus:25053 VSA: Ruckus-SSID (3) VSA Length: Variable Reports the associated WLANs SSID in access request and accounting packet. Ruckus VSAs are received from Ruckus APs only. It is optional for 3rd party APs.

Attribute	Attribute ID	Presence	Type	Description
Vendor-Specific	26	C	String	Vendor ID: Ruckus:25053 VSA: Ruckus-Location (5) VSA Length: Variable Reports the device location for this AP. This is a configurable value in the device location setting. Ruckus VSA is received only from Ruckus AP. It is optional for 3rd party APs.
Vendor-Specific	26	C	Integer	Vendor ID: Ruckus:25053 VSA: Ruckus-SCG- CBLADE-IP (7) VSA Length: 6 Reports the control plane IP address. Ruckus VSAs are received from Ruckus APs only. It is optional for 3rd party APs.

Attribute	Attribute ID	Presence	Type	Description
Vendor-Specific	26	C	Integer	Vendor ID: Ruckus:25053 VSA: Ruckus-SCG -DBLADE-IP (8) VSA Length: 6 Reports the data plane IP address. Ruckus VSA is received only from Ruckus AP. It is optional for 3rd party APs.

Attribute	Attribute ID	Presence	Type	Description
Called Station ID	30	O	Integer	This attribute allows NAS to send the ID (BSSID), which is called by the user. It is MAC of the AP. It supports 2 types of values, namely BSSID:SSID, where BSSID is the MAC address of the WLAN on AP. The second value is AP-MAC:SSID, where AP-MAC is the MAC address of the AP. The letters in the MAC address are in uppercase.For example: 11 -22-33- AA-BB-CC:SSID.

Attribute	Attribute ID	Presence	Type	Description
NAS-Identifier	32	C	Integer	NAS-IP-Address or NAS-Identifier attribute is mandatory in received messages. It supports 3 types of values, namely BSSID (MAC address of the WLAN on AP), AP-MAC (MAC address of AP) and user defined address (maximum length of 62).
Proxy-State	33	O	Octets	This attribute is available to be sent by a proxy server (controller) to another server (AAA server) when forwarding an access request, accounting request (start, stop or interim) and must be returned unmodified in the access accept, access reject, access challenge and accounting response.

Attribute	Attribute ID	Presence	Type	Description
Acct-Status-Type	40	M	Integer	This attribute indicates whether the Accounting-Request attribute marks it as Accounting-Off (8) Accounting-On (7).
Acct-Delay-Time	41	C	Integer	In case the accounting message gets retransmitted, this attribute contains the time stamp of the consecutive retransmitted message.
Acct-Authentic	45	M	Integer	This attribute indicates whether the user was authenticated through RADIUS server or NAS or remote authentication protocol.

Dynamic Authorization and List of Vendor Specific Attributes - AAA Server

5

The AAA server initiates messages to the controller signaling an authorization change, as described in *RFC 5176, Dynamic Authorization Extensions to RADIUS*. This occurs when modifications are made to the subscriber GPRS profile at the HLR (via OAM). Reference *TS 29.234* describes these procedures on the Wm reference point using the diameter protocol.

The following sections list the message flow attributes utilized for RADIUS Dynamic Authorization Extension. Change of Authorization (CoA) and Disconnect Message (DM) messages can have any of the following attributes as a session identifier.

- User name
- CUI with MSISDN
- Acct-Sess-Id (Session identification attribute)

Service Authorisation

A change in service authorization is initiated at the AAA server.

For example, when the AAA server receives a *MAP-InsertSubscriberData* from the HLR along with the modified GPRS profile information (QoS) or is modified for any other reason the controller AAA proxy intercepts the CoA request. It checks if the CoA message contains a session identification attribute (such as user name) as well as attributes indicating the authorization changes (new QoS). Depending on these attributes the call flows could vary.

If the CoA request contains a session identification and the attribute - *service-type (6)* is set to *authorize-only* the controller responds with *CoA NAK* since the controller does not support CoA with service-type as authorize-only.

If the CoA request does not contain the *service-type (6)* attribute, the message must contain a session identification attributes as well as authorization attributes (QoS).

The controller supports RADIUS CoA (Change-of-Authorization) in limited form. RADIUS CoA is supported only for modifying QoS profile when subscriber traffic is tunneled to the core network (Gn and S2a) interface. It is also supported when traffic originates from Ruckus Wireless or from 3rd Party APs.

This section covers:

NOTE Refer to the Authentication and Authorization section for this procedure.

Change of Authorization (CoA) Messages - Not Set to Authorize Only

The table lists the attribute details of CoA messages where the service type *AVP* is not set.is not set. CoA can have any of the following attributes as session identifier:

- User name
- CUI with MSISDN
- Acct-Sess-Id
- NAS-Port
- Framed-IP-Address
- Called-Station-Id
- Acct-Multi-Session-Id
- Framed-Interface-Id
- Framed-IPv6-Prefix
- NAS-IPv6-Address

Table 35: Change of Authorization (CoA) messages - Authorize-Only is not set

Attribute	Attribute ID	Presence	Type/Description
Message Code		M	43
User-Name	1	C	Identifies the username of the UE/subscriber to be disconnected. Username is received from NAS during authentication or accounting session.

Attribute	Attribute ID	Presence	Type/Description
NAS-IP-Address	4	C	This attribute is the IP address of the AP which is serving the station or user equipment, controller's control IP address, controller's management IP address and user defined value.
NAS-Port	5	O	Indicates the physical NAS port number, which authenticates the user or the port on which a session is terminated. If present should match the session context table.
3GPP VSA (Negotiated-QoS-Profile)	5	O	This attribute carries the new QoS value and can be either be Ruckus defined VSA or 3GPP defined VSA. **NOTE** The controller uses this attribute for updating the QoS from the AAA server, whichever is present. If both are present priority is for 3GPP-QoS attribute.
Service-Type	6	O	This attribute indicates the type of service the user has requested, or the type of service to be provided. CoA request should be processed if present. **NOTE** Changes do not get applied on the UE session. It ignores the parameter.

Attribute	Attribute ID	Presence	Type/Description
Framed-IP-Address	8	O	The IPv4 address associated with a session. This is the IP address, which gets assigned to UE after successfull call establishment. If present should match the session context table.
Filter-Id	11	O	Represents the user role name sent by AAA. This is used by SCG to map the received Group Role Name to the UTP profile and forward the corresponding ACL/rate limiting parameters to NAS. NAS enforces the UTP for the given user.
Vendor-Specific	26	O	Vendor ID: WISPr: 14122 VSA: WISPr-Bandwidth-Max-UP (7) VSA Length: Variable The attribute contains the maximum uplink value in bits per second.
Vendor-Specific	26	O	Vendor ID: WISPr: 14122 VSA: WISPr-Bandwidth-Max-DOWN (8) VSA Length: Variable The attribute contains the maximum downlink value in bits per second.

Attribute	Attribute ID	Presence	Type/Description
Session-Timeout	27	O	This attribute sets the maximum number of seconds of service to be provided to the user before termination of the session
Idle-Timeout	28	O	It sets the maximum number of consecutive seconds of idle connection allowed to the user before termination of the session.
Called Station ID	30	O	This attribute will contain the Called Station ID as received from NAS during authentication or the accounting procedure.
Calling Station ID	31	O	This attribute will contain the Calling Station ID as received from NAS during authentication or the accounting procedure
NAS-Identifier	32	C	If present, it should match with the value in the controller session table.
Acct-Session-ID	44	C	This attribute should have the same value as sent by NAS during the accounting procedure.
State	45	O	This attribute is copied as is if it is received in a request from the AAA server. **NOTE** Changes do not get applied on the UE session. It ignores the parameter.

Attribute	Attribute ID	Presence	Type/Description
Acct-Multi-Session-Id	50	O	Thus attribute uniquely identifyies related sessions. It should have the same value received in authentication or accouting request. If present should match the session context table.
Accounting-Interim-Interval	85	O	Indicates the number of seconds between each interim update for this specific session. If the value is blank, the configured default value is used as the accounting interim interval.
Chargeable User ID	89	C	This attribute is MSISDN or any chargeable user identity returned by the AAA server.
NAS-IPv6-Address	95	O	This attribute is the IPv6 address of the AP which is serving the station or controller's control IP address, controller's management IP address and user defined value
Framed-Interface-Id	96	O	The IPv6 interface identifier associated with a session, which is always sent with framed-IPv6 prefix. If present should match the session context.
Framed-IPv6-Prefix	97	O	The IPv6 prefix associated with a session, which is always sent with framed interface identifier. If present should match the session context.

Change of Authorization Acknowledge Messages (CoA Ack)

The table lists the attributes of CoA messages being acknowledged by the controller to DAC.

Table 36: Change of Authorization (CoA) messages - Acknowledge

Attribute	Attribute ID	Presence	Type/Description
Message Code		M	44
State	24	C	This attribute is copied without any modification or only if it is sent in the CoA request.

Change of Authorization Negative Acknowledge Messages (CoA NAK)

The table lists the attributes of CoA messages that are not acknowledged by the controller to the DAC.

Table 37: Change of Authorization (CoA) messages - Negative Acknowledge

Attribute	Attribute ID	Presence	Type/Description
Message Code		M	45
Service-Type	6	C	Indicates the type of service based on the user request or the type of service to be provided. It is included only if the *Service-Type* attribute is present in CoA request, is set to *authorize only*.
State	24	C	This attribute is copied without any modification or only if it is sent in the CoA request.

Attribute	Attribute ID	Presence	Type/Description
Error-Cause	101	C	Included only if the *Service-Type* attribute is present in CoA request is set to *authorize only*. It is included only if the *Error-Cause* attribute is set to *request initiated*. **NOTE** For other scenarios, the attribute *Error-Cause* will have the value as mentioned in TS.

Disconnect Messages

The table lists the attributes of disconnect messages, which are initiated by the controller.

Table 38: Disconnected messages

Attribute	Attribute ID	Presence	Type/Description
Message Code		M	40
User-Name	1	M	Identifies the user name of the UE/subscriber to be disconnect. User name received from NAS during authentication or accounting session.
NAS-IP-Address	4	C	If present, it should match with the value in the controller session table.
NAS-Port	5	O	Indicates the physical NAS port number, which authenticates the user or the port on which a session is terminated. If present should match the session context table.

Attribute	Attribute ID	Presence	Type/Description
Service-Type	6	O	This attribute indicates the type of service the user has requested, or the type of service to be provided. DM request should be processed if present. **NOTE** Changes do not get applied on the UE session. It ignores the parameter.
Framed-IP-Address	8	O	The IPv4 address associated with a session. This is the IP address, which gets assigned to UE after successfull call establishment. If present should match the session context table.
Acct-Terminate-Cause	24	O	This attribute has a value 6 for admin reset.
Calling Station ID	31	C	This attribute will contain the Calling Station ID as received from NAS during authentication or the accounting procedure.

Attribute	Attribute ID	Presence	Type/Description
NAS-Identifier	32	C	It supports 3 types of values, namely BSSID (MAC address of the WLAN on AP), AP-MAC (MAC address of AP) and user defined address (maximum length of 62).
Acct-Session-ID	44	C	This attribute should have the same value as sent by NAS during accounting procedure.
State	45	O	This attribute is copied as is if it is received in a request from the AAA server.
Acct-Terminate-Cause	49	M	This attribute indicates how the session was terminated. Value 6 is for admin reset.
Acct-Multi-Session-Id	50	O	Thus attribute uniquely identifyies related sessions. It should have the same value received in authentication or accouting request. If present should match the session context table.

Attribute	Attribute ID	Presence	Type/Description
Message Authenticator	80	O	This attribute is used to sign *access requests* to prevent spoofing access requests using CHAP, ARAP or EAP authentication methods. It authenticates this whole RADIUS packet - HMAC-MD5 (Type| Identifier | Length | Request Authenticator | Attributes).
NAS-Port-Id	87	O	String identifying the port based on the session and should match the session context if present in request.
Chargeable User ID	89	C	This attribute is MSISDN or any chargeable user identity returned by the AAA server.
NAS-IPv6-Address	95	O	This attribute is the IPv6 address of the AP which is serving the station or controller's control IP address, controller's management IP address and user defined value

Attribute	Attribute ID	Presence	Type/Description
Framed-Interface-Id	96	O	The IPv6 interface identifier associated with a session, which is always sent with framed-IPv6 prefix. If present should match the session context.
Framed-IPv6-Prefix	97	O	The IPv6 prefix associated with a session, which is always sent with framed interface identifier. If present should match the session context.

Acknowledgment of Disconnect Messages (DM Ack)

The table lists the attributes of disconnect messages, which are acknowledged.

Table 39: Acknowledgment of disconnect messages

Attribute	Attribute ID	Presence	Type/Description
Message Code		M	41
Acct-Terminate-Cause	49	O	This attribute indicates how the session was terminated. Value for *Admin-Reset* is set to 6.

Negative Acknowledge of Disconnect Messages (DM NAK)

The table lists the attributes of disconnect messages, which are not acknowledged.

Table 40: Negative acknowledgment of disconnect messages

Attribute	Attribute ID	Presence	Type/Description
Message Code		M	41

Attribute	Attribute ID	Presence	Type/Description
Error-Cause	101	C	Included only if the *Service-Type* attribute is present in CoA request is set to *authorize only*. It is included only if the *Error-Cause* attribute is set to *request initiated*.

Disconnect Messages - Dynamic Authorization Client (AAA server)

A disconnect request packet is sent by the Dynamic Authorization Client for terminating user session(s) on a NAS and to discard all associated session context. The disconnect request packet is sent to UDP port 3799 where it identifies the NAS as well as the user session(s) to be terminated by including the identification attributes.

Disconnected messages can have any of the following attributes as a session identifier.

- User name
- CUI with MSISDN
- Acct-Sess-Id

The table lists the attribute details of the disconnect messages, which are initiated by the dynamic authorization client of the AAA server.

Table 41: Disconnected messages initiated by dynamic authorization client (DAC)

Attribute	Attribute ID	Presence	Type/Description
Message Code		M	40
User-Name	1	C	Identifies the username of the UE/subscriber to be disconnect. User name received from NAS during authentication or accounting session.
NAS-IP-Address	4	C	This attribute is the IP address of the AP which is serving the station or controller's control IP address, controller's management IP address and user defined value.
Calling Station ID	31	O String	This attribute will contain the Calling Station ID as received from NAS during authentication or the accounting procedure.

Attribute	Attribute ID	Presence	Type/Description
NAS-Identifier	32	C	If present, it should match with the value in the controller session table.
Proxy-State	33	O	This attribute is available to be sent by a proxy server to another server.
Acct-Session-ID	44	C	This attribute should have the same value as sent by NAS during accounting procedure.
Chargeable User ID	89	C String	This attribute is MSISDN or any chargeable user identity returned by the AAA server.

List of Vendor Specific Attributes

This section lists the vendor specific attributes.

This section includes:

WISPr Vendor Specific Attributes

The table lists the WISPr vendor specific attributes. The VSA ID for the following VSAs is 14122 and the type is 26.

Table 42: WISPr vendor specific attributes - 14122

Attribute Name	Vendor Type	RADIUS Message Type	Purpose
WISPr-Location-ID	1	Access-Accept Accounting Start - Stop	This attribute indicates the WISPr location id for the specified WISPr service.
WISPr-Location-Name	2	Access-Accept Accounting Start - Stop and Interim	This attribute indicates the WISPr location name for the specified WISPr service.
WISPr-Bandwidth-Max-UP	7	Access-Accept	This attribute specifies the maximum rate at which the corresponding user is allowed to transmit for upstream data.
WISPr-Bandwidth-Max-DOWN	8	Access-Accept	This attribute specifies the maximum rate at which the corresponding user is allowed to transmit for downstream data

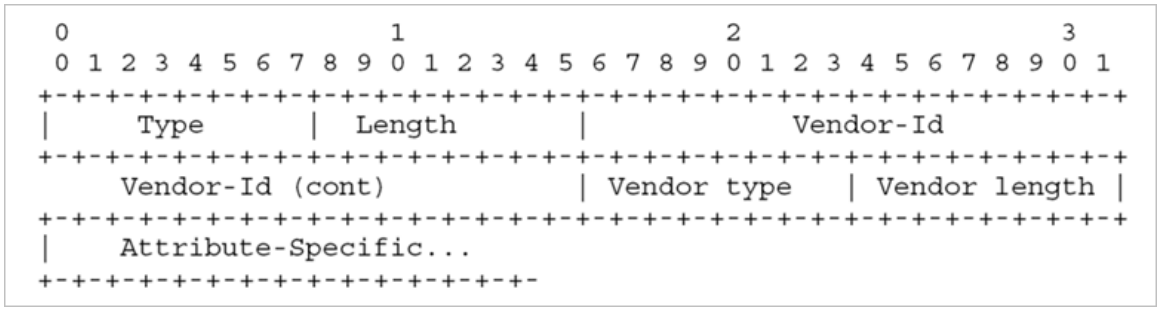
Ruckus Wireless Vendor Specific Attributes

All Ruckus Wireless vendor specific attributes are encoded as sequence of:

- Vendor type
- Vendor length
- Value fields

The figure shows the VSA fields.

Figure 8: VSA fields



The table lists the Ruckus Wireless vendor specific attributes. The VSA ID for all the following VSAs is 25053 and type is 26.

Table 43: Ruckus Wireless vendor specific attributes - 25053

Attribute Name	Vendor Type	RADIUS Message Type	Purpose
Ruckus-User-Groups	1	Access-Accept	RADIUS server uses this attribute to indicate the access point group, specifying the UE group.
Ruckus-STA-RSSI	2	Accounting - Interim - Stop	This attribute reports the UEs current RSSI value in the accounting packet.

Attribute Name	Vendor Type	RADIUS Message Type	Purpose
Ruckus-SSID	3	Access- Request Accounting - Start -Interim- Stop	This attribute reports the associated WLANs SSID in the access request and accounting packet.
Ruckus-WLan-ID	4	Access- Request Accounting - Start -Interim- Stop	This attribute reports the associated WLANs ID. Ruckus VSA is received only from Ruckus AP. Note: It is optional for 3rd party APs.
Ruckus-Location	5	Access- Request Accounting - Start -Interim- Stop	This attribute reports the device location for the current/specified access point. This is a configurable value in the device location setting. Ruckus VSA is received only from Ruckus AP. It is optional for 3rd party APs.
Ruckus-Grace-Period	6	Access- Request Accounting - Start -Interim- Stop	This attribute is the grace period in Hotspot WLANs.

Attribute Name	Vendor Type	RADIUS Message Type	Purpose
Ruckus-SCG-CBLADE-IP	7	Access- Request Accounting - Start -Interim- Stop	This attribute reports the control plane IP address.
Ruckus-SCG-DBLADE-IP	8	Access- Request Accounting - Start -Interim- Stop	This attribute reports the data plane IP address.
Ruckus-VLAN-ID	9	Access-Accept	This attribute value is as per the configuration specified on the WLAN configuration page of the controller web interface and indicates the VLAN ID when it is not zero. Refer to the figure showing the VSA fields.
Ruckus-Sta-Expiration	10		This attribute indicates the expiration value from the RADIUS server.
Ruckus-Sta-UUID	11		This attribute indicates the UUID value from the RADIUS server, when the UUID exists.

Attribute Name	Vendor Type	RADIUS Message Type	Purpose
Ruckus-Accept-Enhancement-Reason	12		This attribute indicates the reason from the RADIUS server, when the reason exists.
Ruckus-VLAN-ID	13		This attribute indicates the user name from the RADIUS server, when the user exists.
Ruckus-IMSI	102	Accounting - Start-Stop	This is sent by AAA to the controller as an authorization accept RADIUS message. M-controller utilizes this information to create the PDP context toward GGSN. Refer to the figure showing the VSA fields.
Ruckus-MSISDN	103		The CUI is generally used, but MSISDN can also be used.

Attribute Name	Vendor Type	RADIUS Message Type	Purpose
Ruckus-APN	104	Access- Request Accounting - Start - Stop	This attribute carries the APN subscribed by the user. It contains only the network identifier (NI), which is part of the APN. The operator identifier part is stored separately in Ruckus-APN-OI. Note: This attribute is always sent and received as a string format, as explained in the figure showing the VSA fields.
Ruckus-QoS	105		3GPP-QoS is now used instead of this VSA. However, this VSA is supported in 2.1.x releases.
Ruckus-NAS-Type	109	Accounting - Start	The value for this parameter is always 1.

Attribute Name	Vendor Type	RADIUS Message Type	Purpose
Ruckus-Status	110		The Accounting Response does not have a status type. This attribute was added to inform AUT that the Accounting has failed due to the setting of this VSA.
Ruckus-APN-OI	111	Access-Accept Accounting - Start	It contains the Operator ID, which is part of the APN name. APN NI part is sent in the Ruckus-APN attribute. Refer to the encoding as explained in Figure 8 .
Ruckus-Session-Type	125	Access- Accept	The controller server uses this attribute on the access-accept to indicate forward policy of the specific UE.

Attribute Name	Vendor Type	RADIUS Message Type	Purpose
Ruckus-Acct-Status	126	Access- Accept	The controller server uses this attribute on the access accept to indicate if the authenticator needs to send the accounting start for the current/specified client.
Ruckus-Zone-ID	127	Access- Request	The controller server uses this attribute to report the zone ID to which the 3rd party AP is associated. This VSA is received only for 3rd party APs.
Ruckus-Auth-Server-Id	128		RAS(IDM) and SCG-RACC use this attribute to obtain the AAA UUID from RAS(IDM) and SCG-RAC.
Ruckus-Utp-Id	129		SCG-RAC and Ruckus-AP use this attribute to provide the UTP ID value to the AP.
Ruckus-Area-Code	130		This attribute carries the area code of the NAS location.

Attribute Name	Vendor Type	RADIUS Message Type	Purpose
Ruckus-Cell-Identifier	131		This attribute carries the cell ID of the NAS location.
Ruckus-Wispr-Redirect-Policy	132		External AAA and SCG-RAC use this attribute to get the vanilla values for the WISPr-TTG feature.
Ruckus-Eth-Profile-Id	133		Ruckus-AP and SCG-RAC use this attribute to find the Ethernet-Profile-Id for a particular session.
Ruckus-Zone-Name	134		SCG-RAC and the external AAA use this attribute to notify the Zone that the AP belongs to.
Ruckus-Wlan-Name	135		SCG-RAC and the external AAA use this attribute to notify the name of the WLAN that the AP belongs to.
Ruckus-Read-Preference	137		The NBI/RAC and external AAA use this attribute to notify the primary/secondary database from where the data is to be read.

Attribute Name	Vendor Type	RADIUS Message Type	Purpose
Ruckus-Client-Host-Name	138	String	Host name of the client device accessing the network
Ruckus-Client-Os-Type	139	String	Operating System on the client device.
Ruckus-Client-Os-Class	140	String	Operating System groups classes category that represent the OS related objects on the client device.
Ruckus-Vlan-Pool	141	String	List of VLAN identifiers supported for the WLAN. This attribute can be found only in RADIUS Access-Accept. APs use the MAC hashing to find the proper VLAN ID from the VLAN pool dynamically and tag all the user equipment data traffic.

AP Roaming Scenarios

A

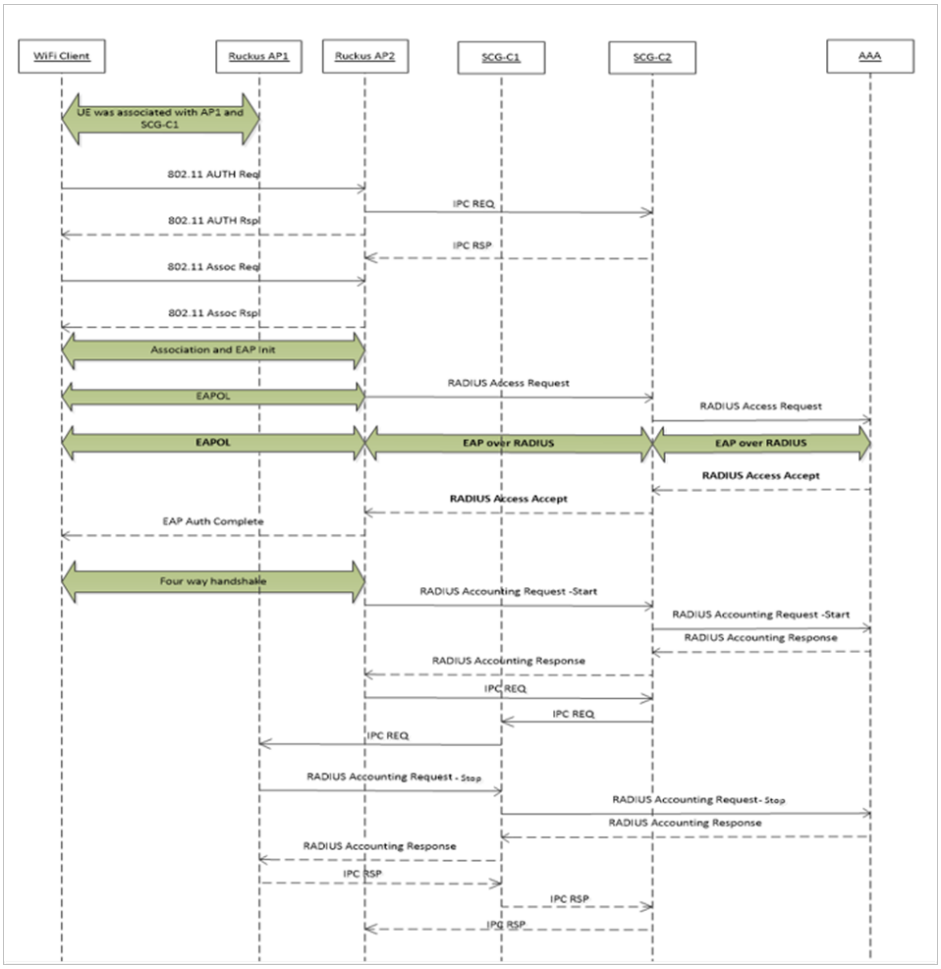
The AP roaming scenarios are as follows.

NOTE The session timeout values received from the AAA server are used for maintaining the PMK/OKC cache timer values at the controller and AP. If the timer value received is less than the default value of 12 hours, it will be used. Otherwise the default value will be used as the maximum value.

AP1 to AP2 Connected to Different Controller Node - PMK / OKC Disabled

In this scenario as seen in the figure, the UE (subscriber) roams from AP1 to AP2 with both the APs connected to the different controller nodes in a cluster environment. This scenario is specific to TTG sessions, where the controller has a GTP tunnel from the controller to the GGSN/PGW. The AP initiates authentication of messages whereas accounting messages are initiated by the controller. PMK / OKC cache is disabled.

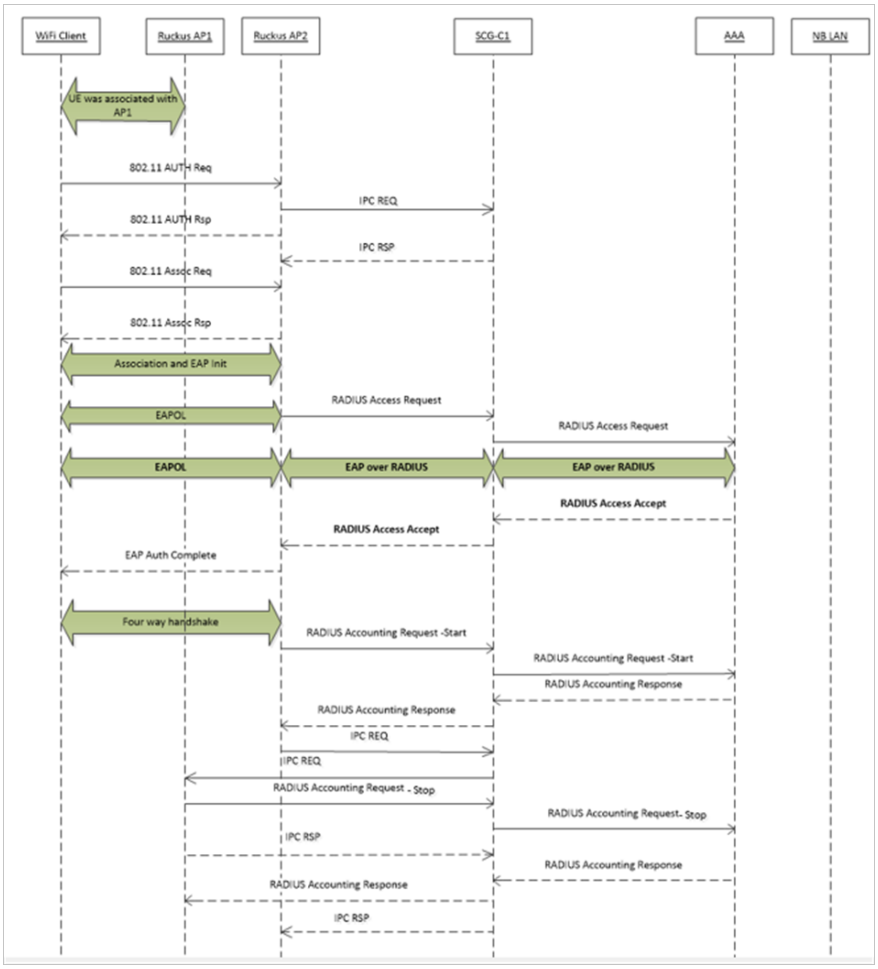
Figure 9: UE roams from AP1 to AP2 connected to different controller node



Roaming from AP1 to AP2 - PMK / OKC Disabled

In this scenario as seen in the figure, the UE (subscriber) roams from AP1 to AP2. Authentication and accounting messages are initiated from the AP and the PMK (Pairwise Master Key) / OKC (Opportunistic Key Caching) cache is disabled.

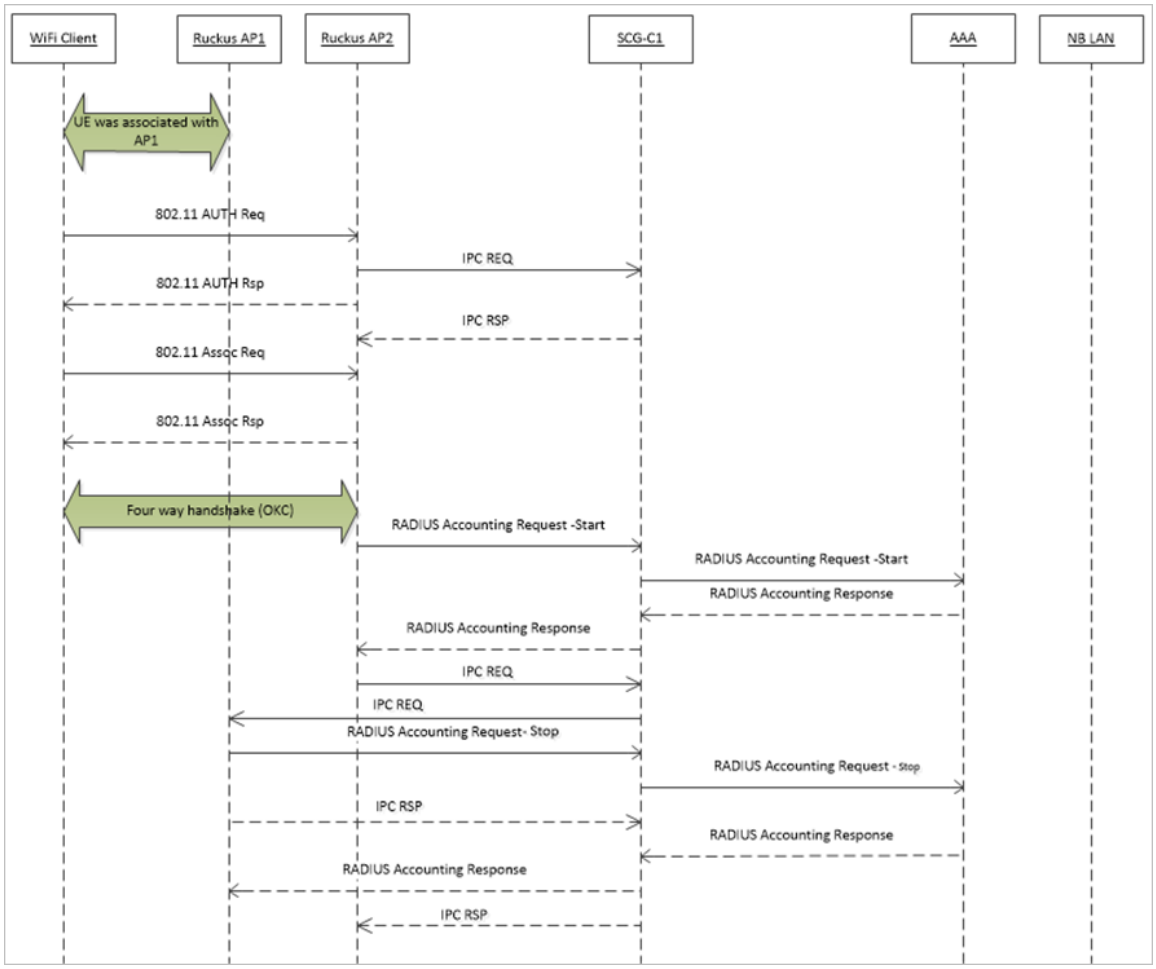
Figure 10: UE roaming from AP1 to AP2 - PMK / OKC disabled



Roaming from AP1 to AP2 - PMK / OKC Enabled

In this scenario as seen in the figure, the UE (subscriber) roams from AP1 to AP2. Authentication and accounting messages are initiated from the AP and the PMK/OKC cache is enabled.

Figure 11: UE roaming from AP1 to AP2 - PMK/OKC enabled

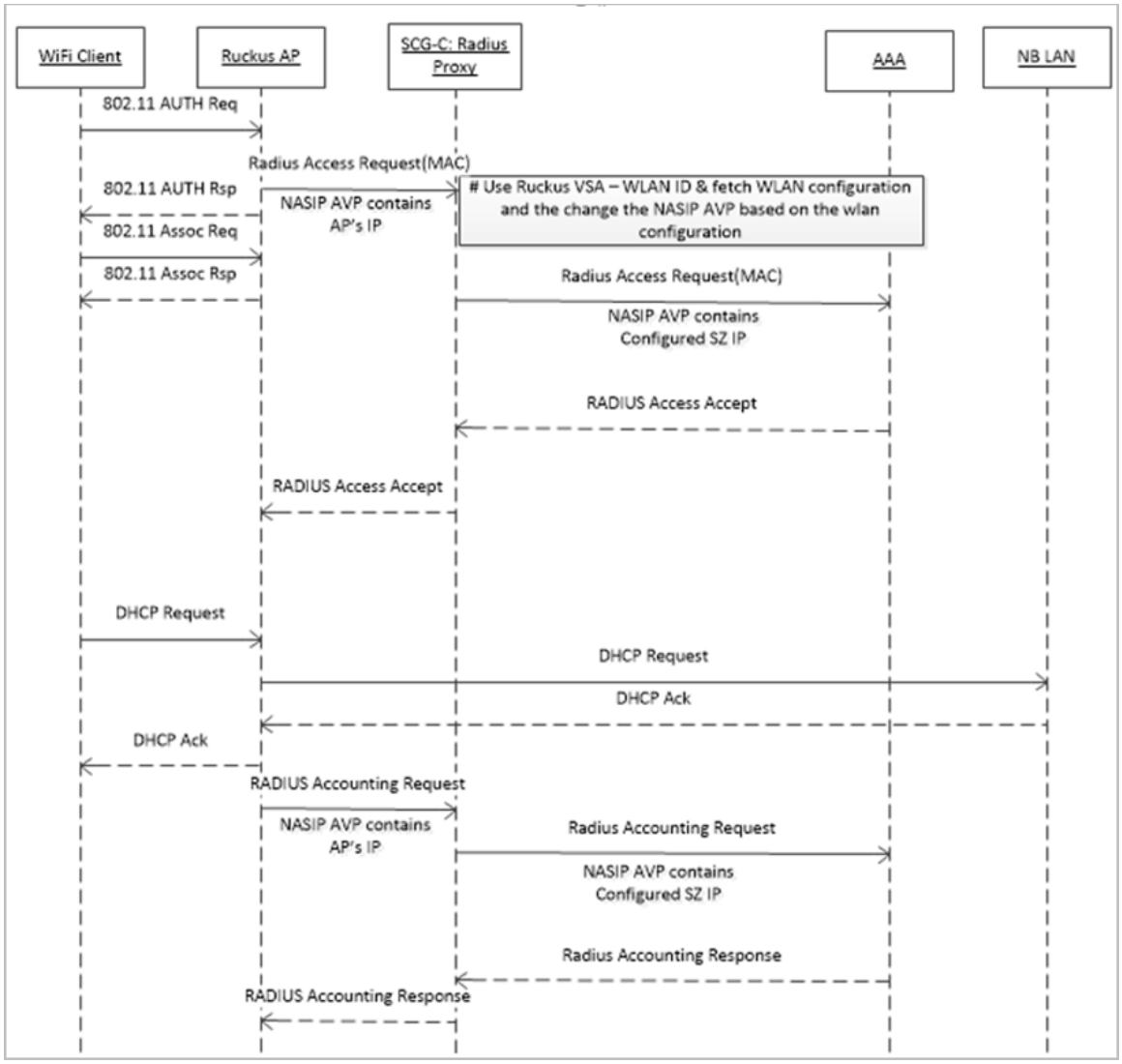

WiFi Client
Ruckus AP1
Ruckus AP2
SCG-C1
AAA
NB LAN
UE was associated with AP1
802.11 AUTH Req
IPC REQ
802.11 AUTH Rsp
IPC RSP
802.11 Assoc Req
802.11 Assoc Rsp
Four way handshake (OKC)
RADIUS Accounting Request -Start
RADIUS Accounting Request -Start
RADIUS Accounting Response
RADIUS Accounting Response
IPC REQ
IPC REQ
RADIUS Accounting Request- Stop
RADIUS Accounting Request - Stop
IPC RSP
RADIUS Accounting Response
RADIUS Accounting Response
IPC RSP

Use Cases

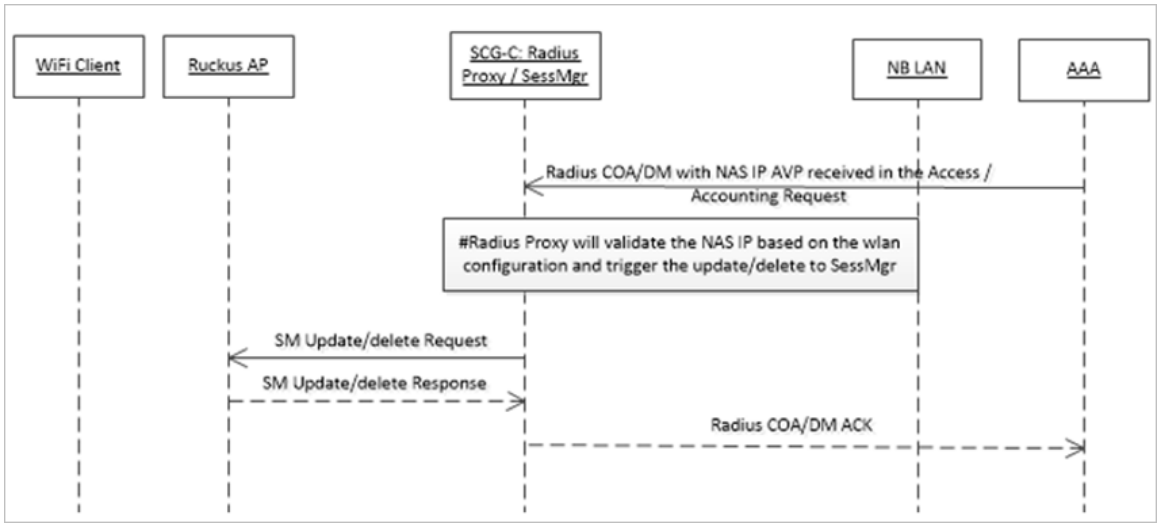
B

The following are the use cases pertaining to NAS IP, Accounting session identififer and filter identifier.

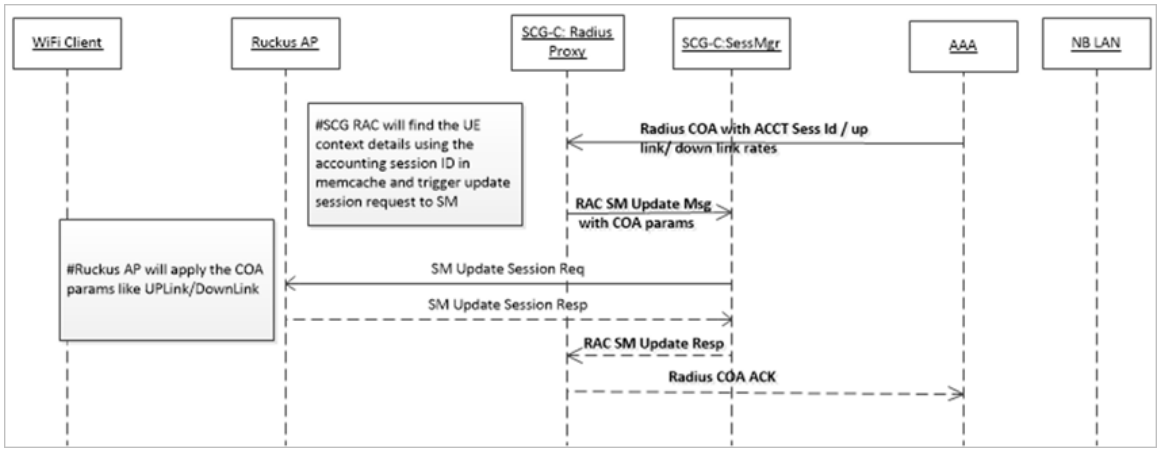
Authentication and Accounting of NAS IP AVP



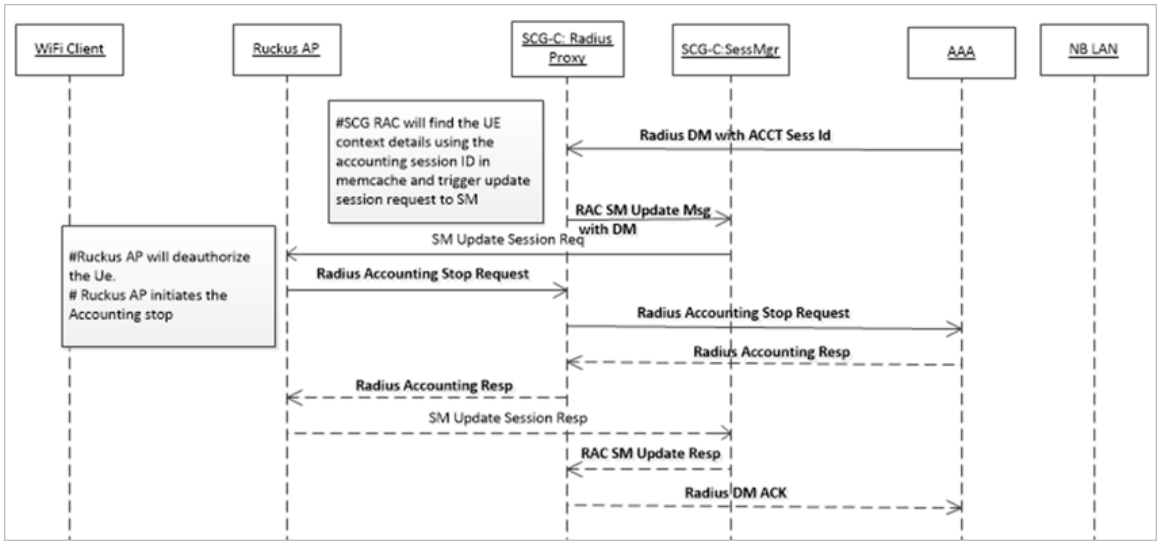
CoA / DM Handling with NAS IP AVP



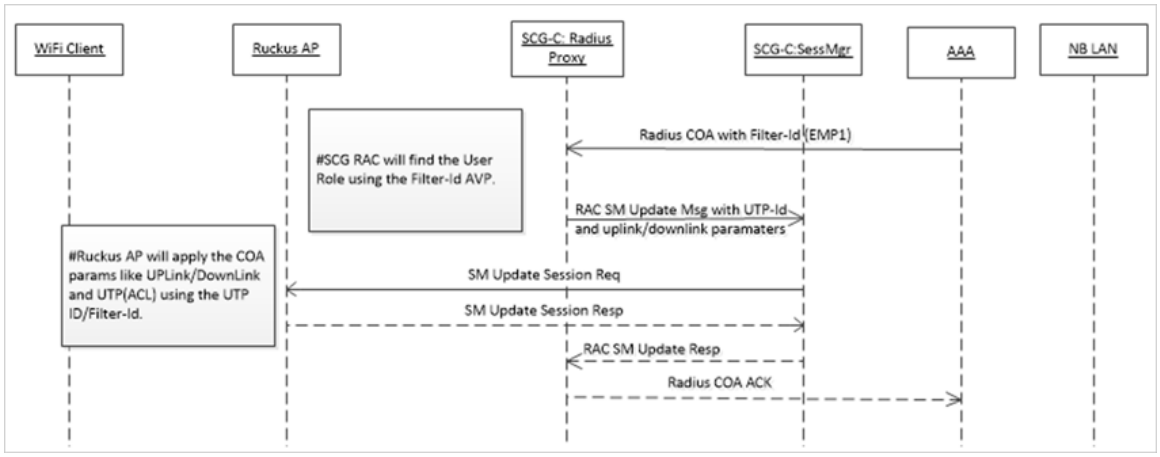
CoA Handling with Accounting Session Identifier



DM Handling with Accounting Session Identifier



User Role change using Radius CoA - Filter Identifier



External DPSK Over Radius

C

In the Wi-Fi world, there is always a need for securing access tunnel between the UE and the AP since the UE data traffic can be easily captured and the contents be seen by any networking monitoring devices.

There are two existing wireless encryption methods, Pre Shared Key(PSK) and 802.1X, for a secure channel over the air. Most common deployments are PSKs rather than 802.1X because of two main reasons:

1. Configuration for 802.1X on the UE is complex
2. Some devices do not support 802.1X

In PSK WLAN, each UE uses the same shared key (passphrase) to encrypt the data traffic. The main disadvantage of having PSK is that if one of the WLAN user is compromised to share the PSK then the entire user traffic can easily be cracked using the PSK.

This brought the need for having a secure tunnel for each user connected to the WLAN. Ruckus Wireless has come with the solution to provide a robust and secure wireless access for each individual user.

Ruckus supports Dynamic Pre Shared Key (DPSK) with the following modes.

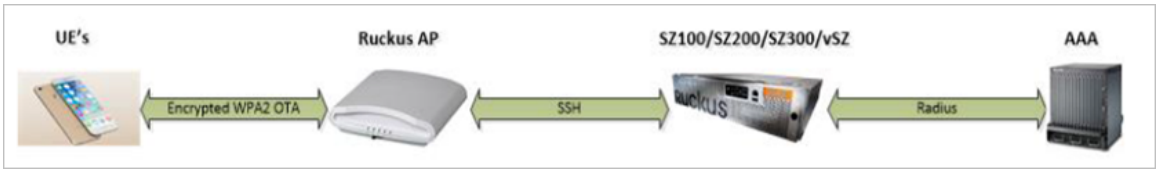
- **Internal:** Ruckus controller or AP manages and retains the DPSK for each individual user with a very optimistic way of handling the DPSK. The number of DPSK supported is limited.
- **External:** Ruckus controller or AP supports the external mode, which uses the RADIUS interface with the Radius Server (AAA) for the DPSK to be maintained at one place. There is no limitation to the number of DPSKs supported. It also simplifies the usecases for the operators and service providers.

DPSK - External

DSPK External is an open WLAN with external DPSK enabled. Ruckus controller or AP uses the existing Mac-Authentication (Over Radius) functionalities to obtain the user DPSK and other session authorization parameters from Radius server (AAA) as seen in the figure below.

How does the DSPK Work

Figure 12: DPSK - External



- AAA server generates and maintains the DPSK for each individual user through their UE MAC.
- During UE association, the controller or AP triggers the Radius Access Request to the Radius serverr (AAA)
- Radius server (AAA) sends back the Radius Access Accept with the new Ruckus VSA. If the user is found using the UE MAC, the Radius server can include other authorization parameter like session timeout/idle timeout/interim timeout/ user group(role) and more in the Radius Access Accept message.
- Radius server (AAA) sends back the Radius Access Reject if the UE MAC is not found in their data base. Ruckus AP or controller restricts the UE from being associated to the WLAN if it receives the access reject from the AAA server. Ruckus AP's are capable of barring the UE after couple of association attempts.

DPSK VSA

Table 44: DPSK VSA

VSA Attribute	Details
Attribute	Vendor-Specific
Attribute Type	26
Presence	Conditional
Vendor ID	Ruckus:25053
VSA	Ruckus-DPSK(142)
VSA Length	Variable

DPSK VSA Value Format'

DPSK VSA value contains the PSK and it is derived using the following procedure with the Pass Phrase and the WLAN SSID. The first byte of the VSA value, is reserved and the next 32 bytes generates the PSK value.

```
D-PSK = PBKDF2_SHA1(PassPhrase, Wlan-SSID, Wlan-SSID-Len,
4096*, 32**)
where:
* - Number of Iterations
** -Length of the generated PSK
```

NOTE WLAN SSID exists in the authentication request, which the AAA server uses to generate the PSK value. The AAA server can be pre-configured with WLAN SSID.

Example of VSA value

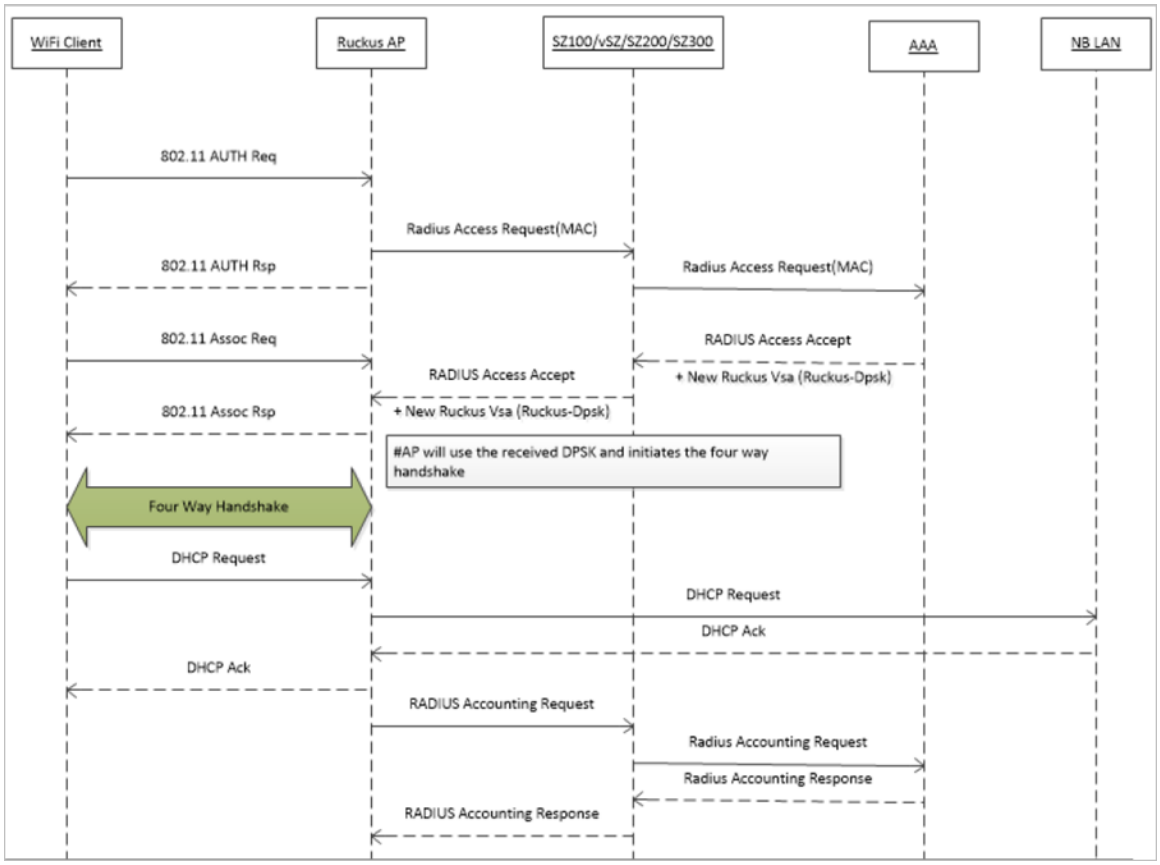
First byte is reserved and the rest gets filled with zero. The remaining 32 bytes holds the actual DPSK value.

```
00: 00xx xxxx xxxx xxxx xxxx xxxx xxxx xxxx
16: xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx
32: xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx
33: xx
```

UE Association Call Flow

Radius AAA server includes the new Ruckus DPSK VSA to retain the PSK value. It also includes the *Filter-Id AVP* for the controllerr or AP to map the user role and apply the uplink or downlink rates, D-Vlan or Vlan-pool and ACL. The Radius AAA server also has all the other standard sessions related attributes. It also uses the the session timeout to force the UE to re-associate (reauthenticate) with the AP and handles the expiry of the DPSK.

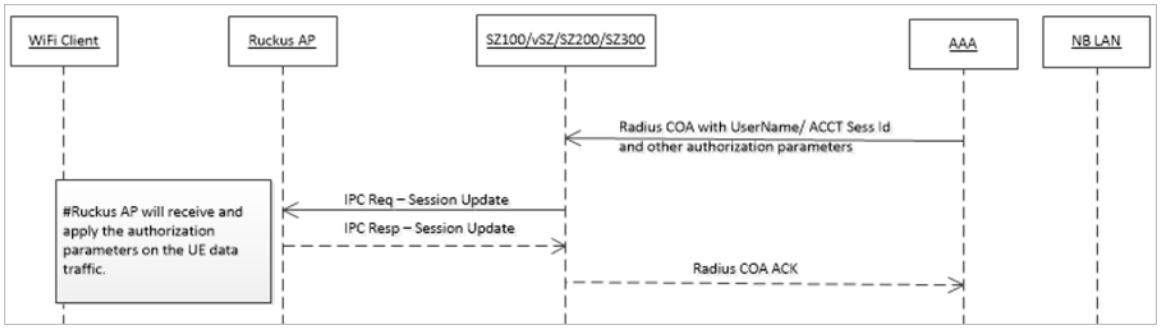
Figure 13: UE Association Call Flow



Radius Change of Authorization (CoA) Call Flow

Radius CoA is used for changing the authorization parameters like user role or all session related timeouts / uplink rate/downlink rate for the UE session. For example, if the user subscribes to a premium package when they are associated with the WLAN, then the Radius AAA server can trigger the CoA message to the controller and make the changes applied on the UE traffic.

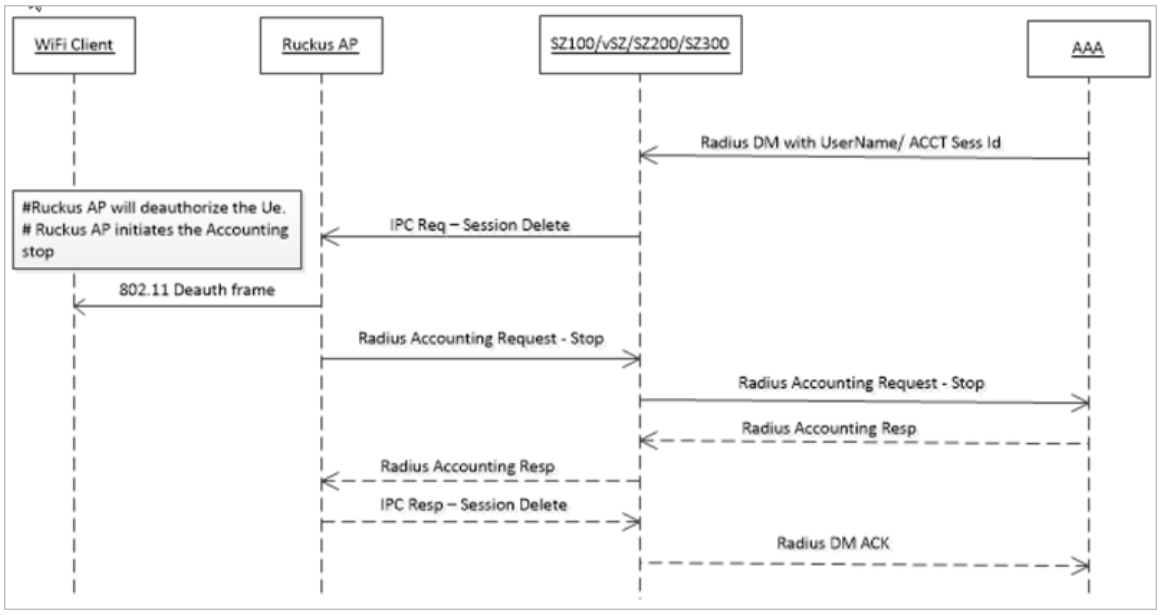
Figure 14: CoA Call Flow



Radius Disconnect Message (DM) Call Flow

Radius DM is used for the de-authenticating the authorized UE from the AP and forces the UE to re-associate with the WLAN. For example, if the operator deletes the DPSK for the user or expiry of the DPSK or for other reasons.

Figure 15: DM Call Flow


WiFi Client
Ruckus AP
SZ100/vSZ/SZ200/SZ300
AAA
Radius DM with UserName/ ACCT Sess Id
#Ruckus AP will deauthorize the Ue.
Ruckus AP initiates the Accounting stop
IPC Req – Session Delete
802.11 Deauth frame
Radius Accounting Request - Stop
Radius Accounting Request - Stop
Radius Accounting Resp
Radius Accounting Resp
IPC Resp – Session Delete
Radius DM ACK

Index

O

P

Q

R

S

T

U

V

W

350 West Java Drive, Sunnyvale, CA

www.ruckuswireless.com