API REFERENCE GUIDE

# Ruckus SmartZone 100 and Virtual SmartZone-Essentials AAA(RADIUS) Interface Reference Guide, 5.1.1

Supporting SmartZone 5.1.1

*Part Number: 800-72262-001 Rev A*
*Publication Date: April 2019*

# Copyright, Trademark and Proprietary Rights Information



## Export Restrictions

These products and associated technical data (in print or electronic form) may be subject to export control laws of the United States of America. It is your responsibility to determine the applicable regulations and to comply with them. The following notice is applicable for all products or technology subject to export control:

*These items are controlled by the U.S. Government and authorized for export only to the country of ultimate destination for use by the ultimate consignee or end-user(s) herein identified. They may not be resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorized ultimate consignee or end-user(s), either in their original form or after being incorporated into other items, without first obtaining approval from the U.S. government or as otherwise authorized by U.S. law and regulations.*

## Disclaimer

THIS CONTENT AND ASSOCIATED PRODUCTS OR SERVICES ("MATERIALS"), ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, ARRIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, FREEDOM FROM COMPUTER VIRUS, AND WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE. ARRIS does not represent or warrant that the functions described or contained in the Materials will be uninterrupted or error-free, that defects will be corrected, or are free of viruses or other harmful components. ARRIS does not make any warranties or representations regarding the use of the Materials in terms of their completeness, correctness, accuracy, adequacy, usefulness, timeliness, reliability or otherwise. As a condition of your use of the Materials, you warrant to ARRIS that you will not make use thereof for any purpose that is unlawful or prohibited by their associated terms of use.

## Limitation of Liability

IN NO EVENT SHALL ARRIS, ARRIS AFFILIATES, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS, LICENSORS AND THIRD PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF ARRIS HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS. Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

## Trademarks

ARRIS, the ARRIS logo, Ruckus, Ruckus Wireless, Ruckus Networks, Ruckus logo, the Big Dog design, BeamFlex, ChannelFly, EdgeIron, FastIron, HyperEdge, ICX, IronPoint, OPENG, SmartCell, Unleashed, Xclaim, ZoneFlex are trademarks of ARRIS International plc and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access (WPA), the Wi-Fi Protected Setup logo, and WMM are registered trademarks of Wi-Fi Alliance. Wi-Fi Protected Setup™, Wi-Fi Multimedia™, and WPA2™ are trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

# Contents

# Preface



# Document Conventions

The following table lists the text conventions that are used throughout this guide.

**TABLE 1 Text Conventions**

| Convention | Description | Example |
|---|---|---|
| `monospace` | Identifies command syntax examples | `device(config)# interface ethernet 1/1/6` |
| **bold** | User interface (UI) components such as screen or page names, keyboard keys, software buttons, and field names | On the **Start** menu, click **All Programs**. |
| *italics* | Publication titles | Refer to the *Ruckus Small Cell Release Notes* for more information. |

## Notes, Cautions, and Warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

**NOTE**
A NOTE provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

**ATTENTION**
An ATTENTION statement indicates some information that you must read before continuing with the current action or task.

**CAUTION**
**A CAUTION statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.**

**DANGER**
***A DANGER statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.***

# Command Syntax Conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

| Convention | Description |
|---|---|
| **bold** text | Identifies command names, keywords, and command options. |
| *italic* text | Identifies a variable. |
| [ ] | Syntax components displayed within square brackets are optional.<br>Default responses to system prompts are enclosed in square brackets. |
| { **x** \| **y** \| **z** } | A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options. |
| **x** \| **y** | A vertical bar separates mutually exclusive elements. |
| < > | Nonprinting characters, for example, passwords, are enclosed in angle brackets. |
| ... | Repeat the previous element, for example, *member*[*member*...]. |
| \ | Indicates a "soft" line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash. |

# Document Feedback

Ruckus is interested in improving its documentation and welcomes your comments and suggestions.

You can email your comments to Ruckus at ruckus-docs@arris.com.

When contacting us, include the following information:

- Document title and release number
- Document part number (on the cover page)
- Page number (if appropriate)

For example:

- Ruckus SmartZone Upgrade Guide, Release 5.0
- Part number: 800-71850-001 Rev A
- Page 7

# Ruckus Product Documentation Resources

Visit the Ruckus website to locate related documentation for your product and additional Ruckus resources.

Release Notes and other user documentation are available at https://support.ruckuswireless.com/documents. You can locate the documentation by product or perform a text search. Access to Release Notes requires an active support contract and a Ruckus Support Portal user account. Other technical documentation content is available without logging in to the Ruckus Support Portal.

White papers, data sheets, and other product documentation are available at https://www.ruckuswireless.com.

# Online Training Resources

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

# Contacting Ruckus Customer Services and Support

The Customer Services and Support (CSS) organization is available to provide assistance to customers with active warranties on their Ruckus products, and customers and partners with active support contracts.

For product support information and details on contacting the Support Team, go directly to the Ruckus Support Portal using https://support.ruckuswireless.com, or go to https://www.ruckuswireless.com and select **Support**.

## What Support Do I Need?

Technical issues are usually described in terms of priority (or severity). To determine if you need to call and open a case or access the self-service resources, use the following criteria:

- Priority 1 (P1)—Critical. Network or service is down and business is impacted. No known workaround. Go to the **Open a Case** section.
- Priority 2 (P2)—High. Network or service is impacted, but not down. Business impact may be high. Workaround may be available. Go to the **Open a Case** section.
- Priority 3 (P3)—Medium. Network or service is moderately impacted, but most business remains functional. Go to the **Self-Service Resources** section.
- Priority 4 (P4)—Low. Requests for information, product documentation, or product enhancements. Go to the **Self-Service Resources** section.

## Open a Case

When your entire network is down (P1), or severely impacted (P2), call the appropriate telephone number listed below to get help:

- Continental United States: 1-855-782-5871
- Canada: 1-855-782-5871
- Europe, Middle East, Africa, Central and South America, and Asia Pacific, toll-free numbers are available at https://support.ruckuswireless.com/contact-us and Live Chat is also available.
- Worldwide toll number for our support organization. Phone charges will apply: +1-650-265-0903

We suggest that you keep a physical note of the appropriate support number in case you have an entire network outage.

## Self-Service Resources

The Ruckus Support Portal at https://support.ruckuswireless.com offers a number of tools to help you to research and resolve problems with your Ruckus products, including:

- Technical Documentation—https://support.ruckuswireless.com/documents

- Community Forums—https://forums.ruckuswireless.com/ruckuswireless/categories
- Knowledge Base Articles—https://support.ruckuswireless.com/answers
- Software Downloads and Release Notes—https://support.ruckuswireless.com/#products_grid
- Security Bulletins—https://support.ruckuswireless.com/security

Using these resources will help you to resolve some issues, and will provide TAC with additional data from your troubleshooting analysis if you still require assistance through a support case or RMA. If you still require help, open and manage your case at https://support.ruckuswireless.com/case_management.

# About This Guide



# About this Guide

This SmartZone100 (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 devices. Consequently, it assumes a basic working knowledge of local area networks, wireless networking, and wireless devices.

**NOTE**
The latest RADIUS versions support the TLS interface and can be used in the SmartZone controller to support a TLS connection with the AAA server as RadSec proxy.

**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 Networks Support Web site at https://support.ruckuswireless.com/contact-us.

## Terminology

The table lists the terms used in this guide.

**TABLE 2 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 |

**TABLE 2 Terms used in this guide (continued)**

| Terminology | Description |
|---|---|
| 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 |
| 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 3 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 4 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. |
| 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. |

# RFCs and Standards

The table lists the references used in this guide

**TABLE 5 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 |
| 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



# EAP Full Authentication Overview

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 the AP Roaming Scenarios chapter for various scenario cases.

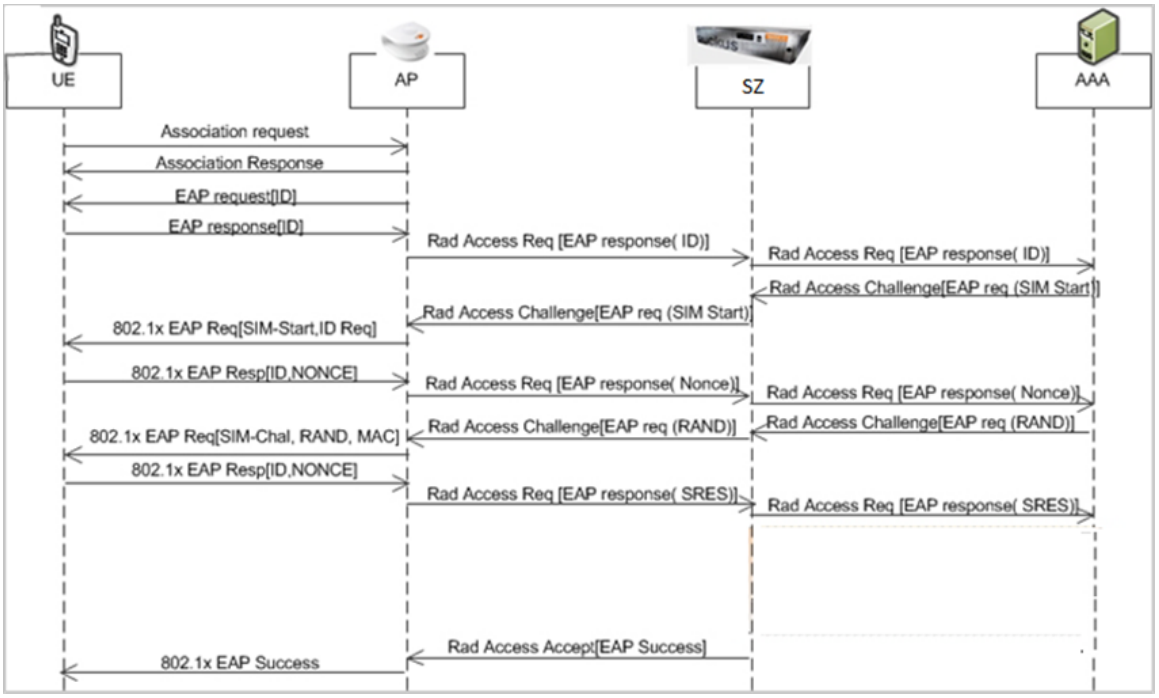
**NOTE**
Refer to the Use Cases chapter for flow details on NAS IP, accounting session identifier and filter identifier.

# 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] on page 14
- RADIUS Access Challenge [EAP Request (SIM Start)] on page 18
- RADIUS Access Request [EAP Response (NONCE_MT)] on page 19
- RADIUS Access Challenge [EAP Request (RAND, MAC)] on page 21
- RADIUS Access Request [EAP Response (SRES)] on page 22
- RADIUS Access Accept [EAP Success (MSK)] on page 23

# 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 6** 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. |

**TABLE 6** RADIUS access request attributes (continued)

| 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. |
| Vendor-Specific | 26 | C | Integer | Vendor ID: Ruckus:25053<br>VSA: Ruckus-WLan-ID (4)<br>VSA Length: 6<br>Reports the associated WLANs ID. Ruckus VSAs are received from Ruckus APs only. It is optional for 3rd party APs. |
| Vendor-Specific | 26 | C | Integer | Vendor ID: Ruckus:25053<br>VSA: Ruckus-SCG-CBLADE-IP (7)<br>VSA Length: 6<br>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<br>VSA: Ruckus-SCG-DBLADE-IP (8)<br>VSA Length: 6<br>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<br>VSA: Ruckus-SSID (3)<br>VSA Length: Variable<br>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<br>VSA: Ruckus-Location (5)<br>VSA Length: Variable<br>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 |

**TABLE 6 RADIUS access request attributes (continued)**

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| | | | | 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. |
| 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.<br>**NOTE**<br>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. |

**TABLE 6** RADIUS access request attributes (continued)

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| | | | | **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 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. |
| 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 7 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). |
| 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.<br>**NOTE**<br>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.<br>**NOTE**<br>This attribute is expected from the AAA server in the initial request location delivery method 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.<br>**NOTE**<br>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 8** 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. |
| 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<br>VSA: Ruckus-SCG-CBLADE-IP (7)<br>VSA Length: 6<br>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<br>VSA: Ruckus-SCG-DBLADE-IP (8)<br>VSA Length: 6<br>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<br>VSA: Ruckus-SSID (3)<br>VSA Length: Variable<br>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<br>VSA: Ruckus-Location (5)<br>VSA Length: Variable<br>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. |

**TABLE 8 RADIUS access request attributes (continued)**

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| | | | | 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. |
| 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.<br>**NOTE**<br>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.<br>**NOTE**<br>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.<br>**NOTE**<br>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. |

**TABLE 8** RADIUS access request attributes (continued)

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| | | | | **NOTE**<br>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.<br>**NOTE**<br>This attribute is included only if the location delivery method is the initial request as specified in RFC 5580. |
| 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.<br>**NOTE**<br>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 9** 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). |
| 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 10** 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. |
| 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<br>VSA: Ruckus-WLan-ID (4)<br>VSA Length: 6<br>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<br>VSA: Ruckus-SCG-CBLADE-IP (7)<br>VSA Length: 6<br>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<br>VSA: Ruckus-SCG-DBLADE-IP (8)<br>VSA Length: 6<br>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<br>VSA: Ruckus-SSID (3)<br>VSA Length: Variable<br>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<br>VSA: Ruckus-Location (5)<br>VSA Length: Variable |

**TABLE 10** RADIUS access request attributes (continued)

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| | | | | 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. |
| 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 11** RADIUS access accept attributes

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

**TABLE 11 RADIUS access accept attributes (continued)**

| 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<br>VSA: 3GPP-GPRS-Negotiated-QoS-Profile (5)<br>VSA Length: Variable<br>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<br>VSA: WISPr-Bandwidth-Max-UP (7) VSA Length: Variable<br>The attribute contains the maximum uplink value in bits per second. |
| Vendor-Specific | 26 | O | Integer | Vendor ID: WISPr: 14122<br>VSA: WISPr-Bandwidth-Max-DOWN (8)<br>VSA Length: Variable<br>The attribute contains the maximum downlink value in bits per second. |
| Vendor-Specific | 26 | C | Charging characteristics | Vendor ID:Ruckus:25053<br>VSA: Ruckus-Charging-Charac (118)<br>VSA Length: 4<br>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<br>VSA: Ruckus-IMSI (102)<br>VSA Length: Variable<br>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. |

**TABLE 11** RADIUS access accept attributes (continued)

| 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. |
| 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<br>VSA: Ruckus-Acct-Status (126)<br>VSA Length: 4<br>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<br>VSA: MS-MPPE-Send-Key (16)<br>VSA Length: Variable<br>This attribute contains a session key used by Microsoft Point-to-Point Encryption Protocol (MPPE). |
| Vendor-Specific | 26 | O | Integer | Vendor ID: Microsoft: 311<br>VSA: MS-MPPE-Recv-Key (17)<br>VSA Length: Variable<br>This attribute contains a session key used by the Microsoft Point-to-Point Encryption Protocol (MPPE). |
| Vendor-Specific | 26 | C | Octets | Vendor ID: Ruckus:25053<br>VSA: Ruckus-APN-NI (104)<br>VSA Length: Variable |

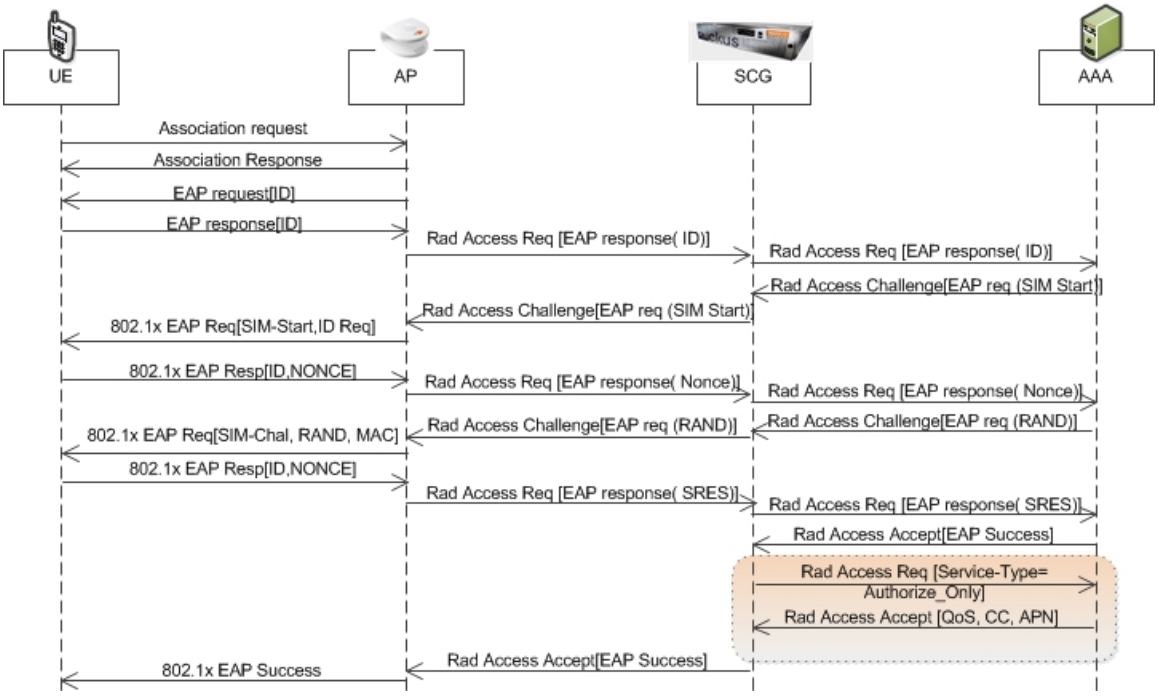
**TABLE 11 RADIUS access accept attributes (continued)**

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| | | | | 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<br>VSA: Ruckus-Session-Type(125)<br>VSA Length: 6<br>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.<br>**NOTE**<br>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.<br>**NOTE**<br>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.<br>**NOTE**<br>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] on page 27
- RADIUS Access Challenge [EAP Request (SIM Start)] on page 30
- RADIUS Access Request [EAP Response (NONCE_MT) on page 31
- RADIUS Access Challenge [EAP Request (RAND, MAC)] on page 33
- RADIUS Access Request [EAP Response (SRES)] on page 34
- RADIUS Access Accept [EAP Success (MSK)] on page 36
- Authorization Access Request on page 38
- Authorization Access Accept on page 39


## 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 12 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<br>VSA: Ruckus-WLan-ID (4)<br><br>VSA Length: 6<br>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<br>VSA: Ruckus-SCG-CBLADE-IP (7)<br><br>VSA Length: 6<br>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<br>VSA: Ruckus-SCG-DBLADE-IP (8)<br><br>VSA Length: 6<br>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<br>VSA: Ruckus-SSID (3)<br><br>VSA Length: Variable.<br>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<br>VSA: Ruckus-Location (5)<br><br>VSA Length: Variable.<br>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. |

**TABLE 12 RADIUS access request attributes (continued)**

| 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). |
| 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. |
| 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 |

**TABLE 12** RADIUS access request attributes (continued)

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| | | | | 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 13** 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). |
| 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 14** 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. |
| 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<br>VSA: Ruckus-WLan-ID (4)<br><br>VSA Length: 6<br>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<br>VSA: Ruckus-SCG-CBLADE-IP (7)<br><br>VSA Length: 6<br>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<br>VSA: Ruckus-SCG-DBLADE-IP (8)<br><br>VSA Length: 6<br>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<br>VSA: Ruckus-Location(5)<br><br>VSA Length: Variable<br>Reports the device location for this AP. This is a configurable value in the device location setting. |

**TABLE 14 RADIUS access request attributes (continued)**

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| | | | | Ruckus VSA is received only from Ruckus AP. It is optional for 3rd party APs. |
| Vendor-Specific | 26 | C | String | Vendor ID: Ruckus:25053<br>VSA: Ruckus-SSID (3)<br><br>VSA Length: Variable<br>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. |
| 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). |
| 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. |

**TABLE 14** RADIUS access request attributes (continued)

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| | | | | **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. |

# 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 15** 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. |
| 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.<br>VSA: Ruckus-WLan-ID (4)<br><br>VSA Length: 6<br>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.<br>VSA: Ruckus-SCG-CBLADE-IP (7)<br><br>VSA Length: 6<br>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.<br>VSA: Ruckus-SCG-DBLADE-IP (8)<br><br>VSA Length: 6 |

**TABLE 15** RADIUS access accept messages (continued)

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| | | | | 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.<br>VSA: Ruckus-Location (5)<br><br>VSA Length: Variable.<br>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.<br>VSA: Ruckus-SSID (3)<br><br>VSA Length: Variable.<br>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). |
| 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 16** 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.<br>VSA: WISPr-Bandwidth-Max-UP (7)<br>VSA Length: Variable.<br>The attribute contains the maximum uplink value in bits per second. |
| Vendor-Specific | 26 | O | Integer | Vendor ID: WISPr: 14122.<br>VSA: WISPr-Bandwidth-Max-DOWN (8).<br>VSA Length: Variable.<br>The attribute contains the maximum downlink value in bits per second. |
| Vendor-Specific | 26 | M | Integer | Vendor ID: Microsoft 311.<br>VSA: MS-MPPE-Send-Key (16).<br>VSA Length: Variable.<br>This attribute contains a session key used by Microsoft Point-to-Point Encryption Protocol (MPPE). |
| Vendor-Specific | 26 | M | Integer | Vendor ID: Microsoft 311.<br>VSA: MS-MPPE-Recv-Key (17).<br>VSA Length: Variable.<br>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.<br>VSA: Ruckus-IMSI (102).<br>VSA Length: Variable.<br>BCD encoded IMSI of the subscriber. |
| Vendor-Specific | 26 | C | Integer | Vendor ID: Ruckus:25053.<br>VSA: Ruckus-Session-Type (125).<br>VSA Length: 6.<br>Session Type - TTG (2), Local-Breakout(3), Local-Breakout-AP(4), L3oGRE (5), L2oGRE (6), QinQL3 (7), PMIP (8).<br>The controller server uses this attribute on the access - accept to indicate the forward policy of the specific UE. |
| Vendor-Specific | 26 | C | Integer | Vendor ID: Ruckus:25053.<br>VSA: Ruckus-Acct-Status (126).<br>VSA Length: 6. |

**TABLE 16** RADIUS access request messages (continued)

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| | | | | 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. |
| 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.<br>**NOTE**<br>This attribute is expected from the AAA server 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.<br>**NOTE**<br>This attribute is expected from the AAA server if the location delivery method is accounting request as specified in RFC 5580. |

**TABLE 16** RADIUS access request messages (continued)

| 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.<br>**NOTE**<br>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 17** Authorisation Access request attributes

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| User-Name | 1 | M | String | Indicates the name of the user to be authenticated. |
| Vendor-Specific | 26 | C | Integer | Vendor ID: Ruckus VSA: 25053<br>VSA: Ruckus-SGSN-Number(124)<br>VSA Length: Variable.<br>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<br>VSA: Ruckus-SSID (3)<br>VSA Length: Variable.<br>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<br>VSA: Ruckus-Location (5)<br>VSA Length: Variable.<br>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 18** 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<br>VSA: WISPr-Bandwidth-Max-UP (7)<br><br>VSA Length: Variable.<br>The attribute contains the maximum uplink value in bits per second. |
| Vendor-Specific | 26 | O | Integer | Vendor ID: WISPr: 14122<br>VSA: WISPr-Bandwidth-Max-DOWN (8)<br><br>VSA Length: Variable.<br>The attribute contains the maximum downlink value in bits per second. |
| Vendor-Specific | 26 | O | Octets | Vendor ID: Ruckus: 25053<br>VSA: Ruckus-APN-NI(104)<br><br>VSA Length: Variable.<br>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 | O | String | Vendor ID: 3GPP: 10415<br>VSA:3GPP-GPRS-Negotiated-QoS-Profile (5)<br><br>VSA Length: Variable.<br>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<br>VSA: Ruckus-Charging-Charac (118)<br><br>VSA Length: 4<br>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. |
| 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. |

# 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 19** 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

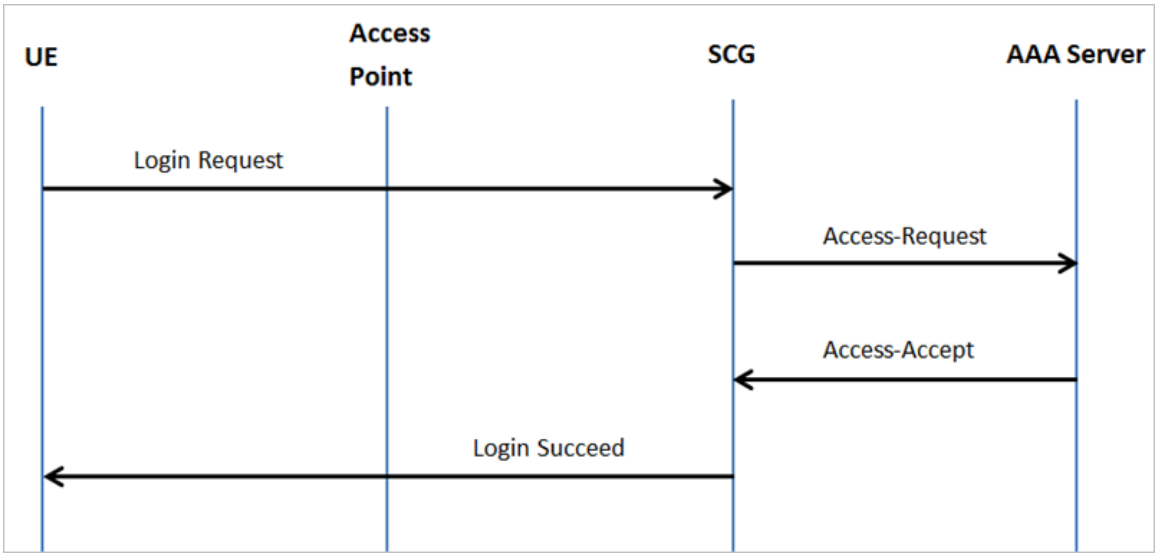


# Hotspot (WISPr) Authentication and Accounting Overview

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 on page 42
- Hotspot (WISPr) Authentication Response on page 45
- Hotspot (WISPr) Accounting Request [Start] on page 46

# 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

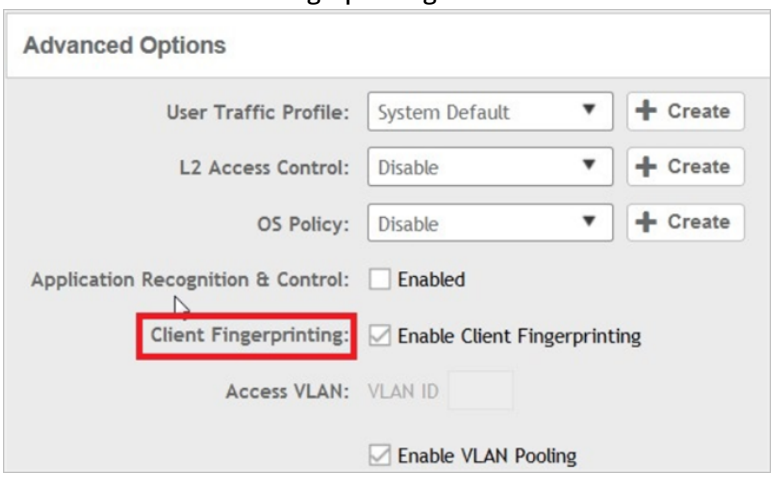



**TABLE 20** Hotspot (WISPr) authentication request attributes

| 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. |
| 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.<br>**NOTE**<br>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<br>Vendor Type: 1<br>VSA: WISPr-Location-ID<br>VSA Length: Variable<br>This attribute is a configurable value in the hotspot (WISPr) user interface. |
| Vendor-Specific | 26 | O | Integer | Vendor ID: WISPr: 14122<br>Vendor Type: 2 |

**TABLE 20 Hotspot (WISPr) authentication request attributes (continued)**

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| | | | | VSA: WISPr-Location-Name<br>VSA Length: Variable<br>This attribute is a configurable value in the hotspot (WISPr) user interface. |
| Vendor-Specific | 26 | O | Integer | Vendor ID: WISPr: 14122<br>Vendor Type: 3<br>VSA: WISPr-Logoff-URL<br>VSA Length: Variable<br>This attribute indicates the hotspot (WISPr) service logout URL. |
| Vendor-Specific | 26 | O | String | Vendor ID: Ruckus<br>Vendor Type: 3<br>VSA: Ruckus-Client-Host-name<br>VSA Length: 138<br>This attribute reports the configured client host name |
| Vendor-Specific | 26 | O | String | Vendor ID: Ruckus<br>Vendor Type: 3<br>VSA: Ruckus-Client-Os-Type<br>VSA Length: 139<br>This attribute reports the Client OS Type. |
| Vendor-Specific | 26 | O | String | Vendor ID: Ruckus<br>Vendor Type: 3<br>VSA:Ruckus-Client-Os-Class<br>VSA Length: Variable<br>This attribute reports the client OS class |
| Vendor-Specific | 26 | O | String | Vendor ID: WISPr: 25053<br>Vendor Type: 3<br>VSA: Ruckus-SSID (3)<br>VSA Length: Variable<br>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<br>VSA: Ruckus-Zone-ID (127)<br>VSA Length: 6<br>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. |
| 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 |

**TABLE 20 Hotspot (WISPr) authentication request attributes (continued)**

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| | | | | 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<br>Vendor Type: 9<br>VSA: VLAN-ID<br>VSA Length: Variable<br>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.<br>**NOTE**<br>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-Information | 127 | C | Octets | This is a composite attribute, which provides meta data about the location information. It is encoded as per RFC 5580.<br>**NOTE**<br>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.<br>**NOTE**<br>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.<br>**NOTE**<br>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. |

**TABLE 20 Hotspot (WISPr) authentication request attributes (continued)**

| 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.<br><br>**NOTE**<br>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-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.<br><br>**NOTE**<br>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 21 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<br>VSA: WISPr-Bandwidth-Max-UP (7)<br><br>VSA Length: Variable<br><br>The attribute contains the maximum uplink value in bits per second. |
| Vendor-Specific | 26 | O | Integer | Vendor ID: WISPr: 14122<br>VSA: WISPr-Bandwidth-Max-DOWN (8)<br><br>VSA Length: Variable<br><br>The attribute contains the maximum downlink value in bits per second. |
| Vendor-Specific | 26 | O | Integer | Vendor ID: Ruckus: 25053<br>Vendor Type: 7<br><br>VSA: Ruckus-Grace-Period<br><br>VSA Length: Variable<br><br>This attribute is the grace period in hotspot (WISPr) WLANs. |

**TABLE 21 Hotspot (WISPr) authentication request attributes (continued)**

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| 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.<br>**NOTE**<br>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.<br>**NOTE**<br>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.<br>**NOTE**<br>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 22 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. |
| 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<br>Vendor Type: 1<br>VSA: WISPr-Location-ID<br>VSA Length: Variable<br>This attribute is a configurable value in the hotspot (WISPr) user interface. |
| Vendor-Specific | 26 | O | Integer | Vendor ID: WISPr: 14122 |

**TABLE 22 Hotspot (WISPr) accounting request (start) attributes (continued)**

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| | | | | Vendor Type: 2<br>VSA: WISPr-Location-Name<br>VSA Length: Variable<br>This attribute is a configurable value in the hotspot (WISPr) user interface. |
| Vendor-Specific | 26 | O | Integer | Vendor ID: Ruckus: 25053<br>Vendor Type: 2<br>VSA: Ruckus-STA-RSSI (2)<br>VSA Length: Variable<br>This attribute can only be present with Acct-Status-Type = Interim or Stop. |
| Vendor-Specific | 26 | O | String | Vendor ID: Ruckus: 25053<br>Vendor Type: 3<br>VSA: Ruckus-SSID (3)<br>VSA Length: Variable<br>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<br>Vendor Type: 5<br>VSA: Ruckus-Location<br>VSA Length: Variable<br>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<br>Vendor Type: 7<br>VSA: Ruckus-SCG-CBLADE-IP VSA VSA Length: 6<br>This attribute indicate the control plane IP address that is being used. |
| Vendor-Specific | 26 | O | Integer | Vendor ID: Ruckus: 25053<br>Vendor Type: 8<br>VSA: Ruckus-SCG-DBLADE-IP VSA VSA Length: 6<br>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. |
| 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 |

**TABLE 22 Hotspot (WISPr) accounting request (start) attributes (continued)**

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| | | | | (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-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.<br>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. |
| 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.<br>**NOTE**<br>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.<br>**NOTE**<br>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.<br>**NOTE**<br>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 23 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. |
| 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<br>Vendor Type: 1<br>VSA: WISPr-Location-ID<br>VSA Length: Variable<br>This attribute is a configurable value in the hotspot (WISPr) user interface. |
| Vendor-Specific | 26 | O | Integer | Vendor ID: WISPr: 14122<br>Vendor Type: 2<br>VSA: WISPr-Location-Name<br>VSA Length: Variable<br>This attribute is a configurable value in the hotspot (WISPr) user interface. |
| Vendor-Specific | 26 | O | Integer | Vendor ID: Ruckus: 25053<br>Vendor Type: 2<br>VSA: Ruckus-STA-RSSI (2)<br>VSA Length: Variable<br>This attribute can only be present with Acct-Status-Type = Interim or Stop. |
| Vendor-Specific | 26 | O | String | Vendor ID: Ruckus: 25053<br>Vendor Type: 3<br>VSA: Ruckus-SSID (3)<br>VSA Length: Variable<br>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<br>Vendor Type: 5<br>VSA: Ruckus-Location<br>VSA Length: Variable |

**TABLE 23 Hotspot (WISPr) accounting request (stop/interim) attributes (continued)**

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| | | | | 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<br>Vendor Type: 7<br>VSA: Ruckus-SCG-CBLADE-IP VSA VSA Length: Variable<br>This attribute indicate the control plane IP address that is being used. |
| Vendor-Specific | 26 | O | Integer | Vendor ID: Ruckus: 25053<br>Vendor Type: 8<br>VSA: Ruckus-SCG-DBLADE-IP VSA VSA Length: Variable<br>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. |
| 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. |
| 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-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-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. |

**TABLE 23 Hotspot (WISPr) accounting request (stop/interim) attributes (continued)**

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| | | | | 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. |
| 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.<br>**NOTE**<br>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.<br>**NOTE**<br>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.<br>**NOTE**<br>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.<br>**NOTE**<br>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 24 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



## Hotspot 2.0 Authentication Overview

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] on page 27
- RADIUS Access Request [EAP Response (NONCE_MT)] on page 19
- RADIUS Access Request [EAP Response (SRES)] on page 22

**TABLE 25 Hotspot 2.0 RADIUS access request attributes**

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| Vendor-Specific | 26 | C | String | Vendor ID: 40808<br>Vendor Type: 2<br>VSA: AP Version<br>VSA Length: Variable<br>This attribute indicates version 0 as R1 compliant AP and version 1as R2 compliant AP. |
| Vendor-Specific | 26 | C | String | Vendor ID: 40808<br>Vendor Type: 3 |

**TABLE 25 Hotspot 2.0 RADIUS access request attributes (continued)**

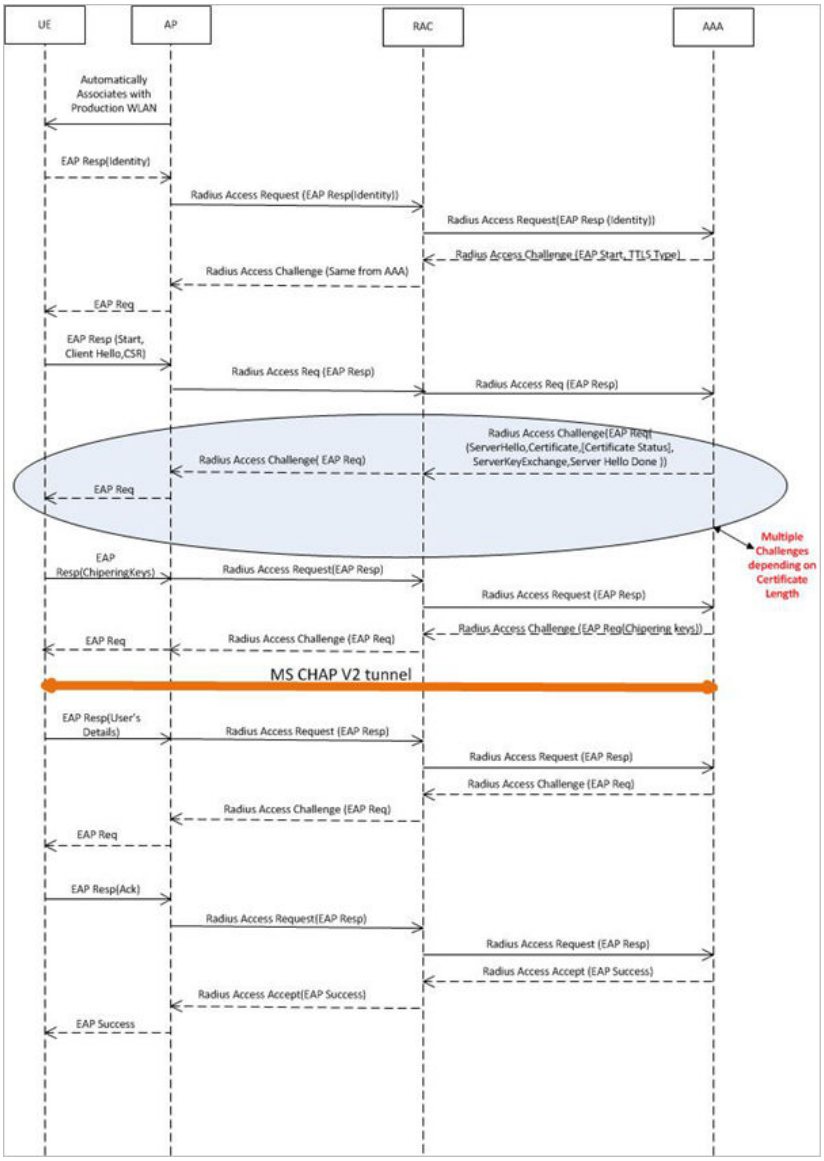
| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| | | | | VSA: Mobile Device Version<br>VSA Length: Variable<br>This attribute indicates version 0 as R1 compliant AP and version 1 as R2 compliant AP. Version 1 also includes the update identifier details. |

# 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




# Access Request

The table lists the attributes specific to Hotspot 2.0.

**TABLE 26** Hotspot 2.0 RADIUS access request attributes

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| Vendor-Specific | 26 | C | String | Vendor ID: 40808<br>Vendor Type: 2<br>VSA: AP Version<br>VSA Length: Variable<br>This attribute indicates version 0 as R1 compliant AP and version 1as R2 compliant AP. |

**TABLE 26 Hotspot 2.0 RADIUS access request attributes (continued)**

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| Vendor-Specific | 26 | C | String | Vendor ID: 40808<br>Vendor Type: 3<br>VSA: Mobile Device Version<br>VSA Length: Variable<br>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 27 Hotspot 2.0 RADIUS access response attributes**

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| Vendor-Specific | 26 | C | String | Vendor ID: 40808<br>Vendor Type: 1<br>VSA: Subscription Remediation Needed<br>VSA Length: Variable<br>This attribute provides the remediation URL. |
| Vendor-Specific | 26 | C | String | Vendor ID: 40808<br>Vendor Type: 4<br>VSA: De-authentication Request<br>VSA Length: Variable<br>This attribute is applicable only for R2 devices. It gives the de-authenticated URL and the re-authentication delay. |
| Vendor-Specific | 26 | C | String | Vendor ID: 40808<br>Vendor Type: 5<br>VSA: Session Information URL<br>VSA Length: Variable |

**TABLE 27 Hotspot 2.0 RADIUS access response attributes (continued)**

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| | | | | 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 28 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. |
| 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 29 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. |

**TABLE 29 Onboarding Access Response (continued)**

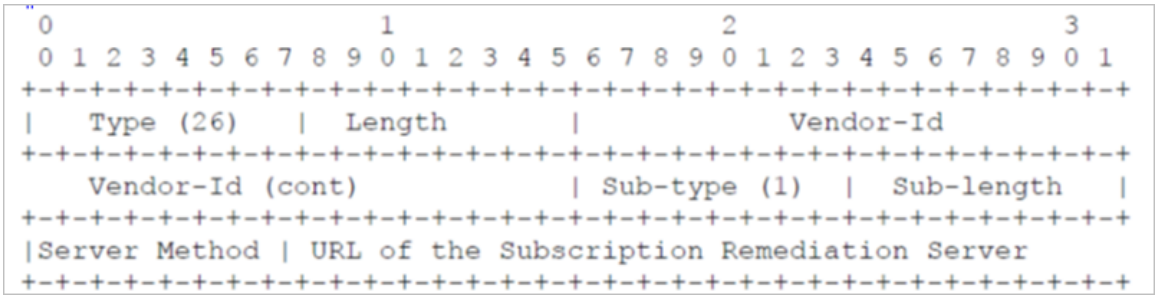
| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| Filter-Id | 11 | O | String | Represents the User Role name sent by AAA. This is used by SCG to map the received Group Role Name to the UTP profile and forward the corresponding ACL/rate limiting parameters to NAS. NAS 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. |
| WISPr uplink | 26 | O | Integer | Vendor ID: WISPr: 14122<br>VSA: WISPr-Bandwidth-Max-UP (7)<br>VSA Length: Variable<br>The attribute contains the maximum uplink value in bits per second. |
| WISPr downlink | 26 | O | Integer | Vendor ID: WISPr: 14122<br>VSA: WISPr-Bandwidth-Max-DOWN (8)<br>VSA Length: Variable<br>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

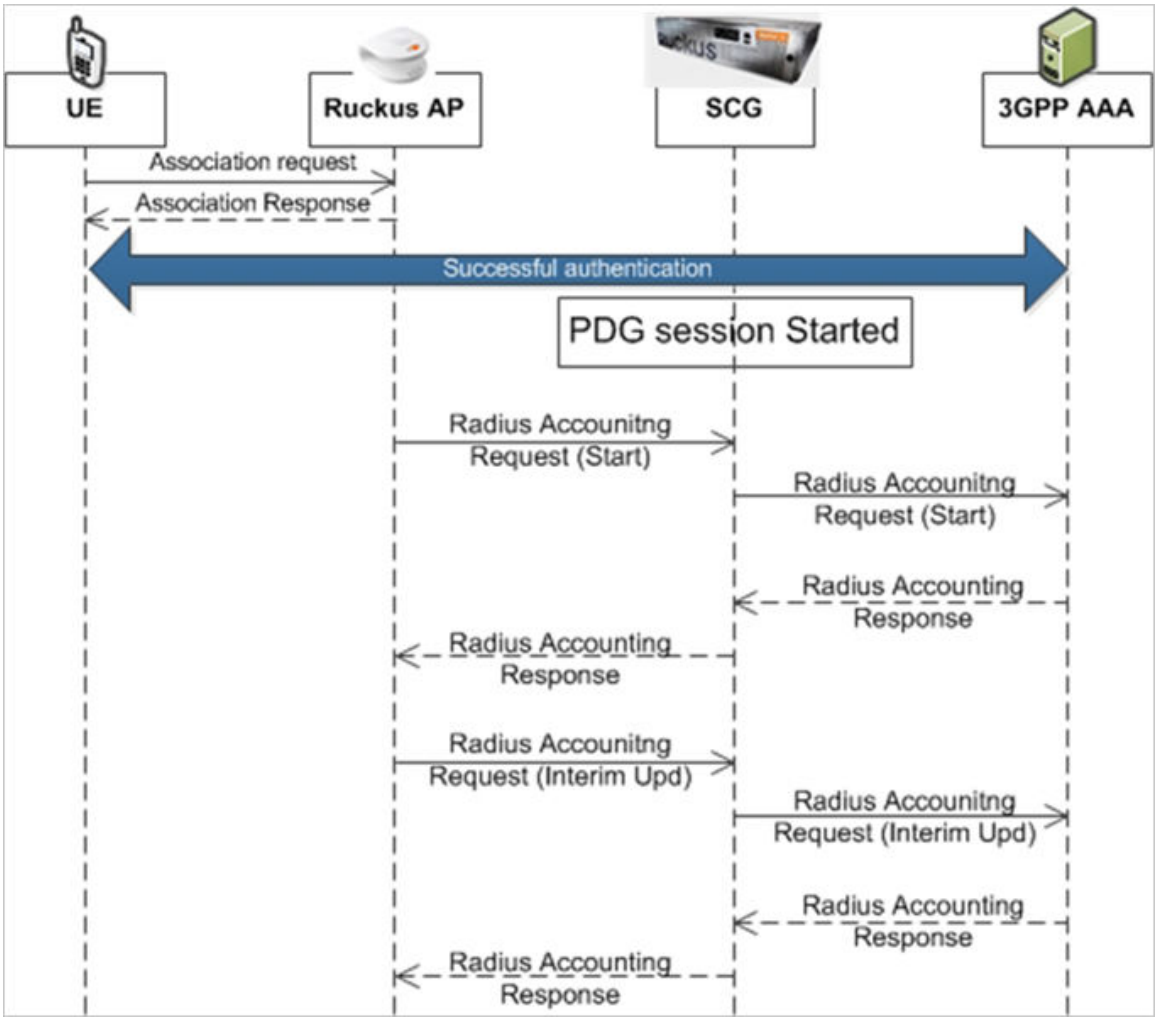


## AP Initiated Accounting Messages (PDG/LBO Sessions)

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 30** Accounting start message attributes

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

**TABLE 30 Accounting start message attributes (continued)**

| 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 user equipment, 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. |
| Vendor-Specific | 26 | C | String | Vendor ID: Ruckus:25053<br>VSA: Ruckus-SSID (3)<br>VSA Length: Variable<br>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<br>VSA: Ruckus-Location (5)<br>VSA Length: Variable<br>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<br>VSA: Ruckus-SCG-CBLADE-IP (7)<br>VSA Length: 6<br>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<br>VSA: Ruckus-SCG-DBLADE-IP (8)<br>VSA Length: 6<br>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: 11-22-33-AA-BB-CC:SSID. |
| 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). |
| 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. |
| 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. |

**TABLE 30 Accounting start message attributes (continued)**

| 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-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. |
| 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.<br>**NOTE**<br>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.<br>**NOTE**<br>This attribute is included only when the expected location delivery method is accounting 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.<br>**NOTE**<br>This attribute is included only when the expected 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.<br>**NOTE**<br>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 31 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. |
| 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. |
| Vendor-Specific | 26 | C | Integer | Vendor ID: Ruckus:25053<br>VSA: Ruckus-STA-RSSI (2)<br>VSA Length: 6<br>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<br>VSA: Ruckus-SSID (3)<br>VSA Length: Variable<br>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. |
| Vendor-Specific | 26 | C | String | Vendor ID: Ruckus:25053<br>VSA: Ruckus-Location (5)<br>VSA Length: Variable<br>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<br>VSA: Ruckus-SCG-CBLADE-IP (7)<br>VSA Length: 6<br>Reports the control plane IP address. Ruckus VSA is received only from Ruckus AP. It is optional for 3rd party APs. |
| Vendor-Specific | 26 | C | Integer | Vendor ID: Ruckus:25053<br>VSA: Ruckus-SCG-DBLADE-IP (8)<br>VSA Length: 6<br>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 |
| Calling Station ID | 31 | O | String | Allows NAS to send the ID (UE MAC), which indicates as to who is calling this server. |

**TABLE 31 Accounting interim update and stop message attributes (continued)**

| 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. |
| 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. |
| 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. |
| 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. |
| 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. |

**TABLE 31** Accounting interim update and stop message attributes (continued)

| 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. |
| Chargeable User ID | 89 | C | String | AP includes Chargeable User ID attribute along with the values received from the AAA server. |
| 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.<br>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.<br>**NOTE**<br>This attribute is included only when the expected location delivery method is accounting 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.<br>**NOTE**<br>This attribute is included only when the expected 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.<br>**NOTE**<br>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 32** Accounting on 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 controller's control IP address, controller's management IP address and user defined value. |
| Vendor-Specific | 26 | C | String | Vendor ID: Ruckus:25053<br>VSA: Ruckus-SSID (3)<br>VSA Length: - Variable<br>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. |
| Vendor-Specific | 26 | C | String | Vendor ID: Ruckus:25053<br>VSA: Ruckus-Location(5) |

**TABLE 32** Accounting on message attributes (continued)

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| | | | | VSA Length: Variable<br>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<br>VSA: Ruckus-SCG-CBLADE-IP (7)<br>VSA Length: 6<br>Reports the control plane IP address. Ruckus VSA is received only from Ruckus AP. It is optional for 3rd party APs. |
| Vendor-Specific | 26 | C | Integer | Vendor ID: Ruckus:25053<br>VSA: Ruckus-SCG-DBLADE-IP (8)<br>VSA Length: 6<br>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 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 |
| 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. |
| 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 33** Accounting off 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 controller's control IP address, controller's management IP address and user defined value. |
| Vendor-Specific | 26 | C | String | Vendor ID: Ruckus:25053<br>VSA: Ruckus-SSID (3) |

**TABLE 33 Accounting off message attributes (continued)**

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| | | | | VSA Length: Variable<br>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<br>VSA: Ruckus-Location (5)<br>VSA Length: Variable<br>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<br>VSA: Ruckus-SCG-CBLADE-IP (7)<br>VSA Length: 6<br>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<br>VSA: Ruckus-SCG-DBLADE-IP (8)<br>VSA Length: 6<br>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 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. |
| 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. |
| 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. |

# AAA Server Dynamic Authorization and List of Vendor Specific Attributes



## Dynamic Authorization and List of Vendor Specific Attributes - AAA Server

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. We have key attributes to uniquely identify the session context tables and session identifier attributes, which if present in the CoA/DM message should match with the session context table attributes.

The following section lists the key attributes which are supported for COA/DM.

- User-Name
- Acct-Session-Id
- CUI/MSISDN

The following table lists the key attributes with different combinations of Auth type and Auth method.

| AuthType | AuthMethod | Key Attribute |
|---|---|---|
| Standard | Open/802.1x/MAC/802.1x & MAC | Username or<br>AcctSessId or<br>Username + AcctSessId |
| Wispr & Web-Auth | Open/MAC/8021.x | AcctSessId or<br>Username + AcctSessId |
| TTG (vSZ-H + vDP) | 802.1x | Username or<br>AcctSessId or<br>CUI/MSISDN or<br>Username + AcctSessId or<br>Username + CUI/MSISDN or<br>AcctSessId + CUI/MSISDN or<br>AcctSessId + Username +<br>CUI/MSISDN |

The following section lists the Identification attributes including NAS and session identification attributes, which supports both CoA/DM.

NAS identification attributes:

- NAS-IP-Address
- NAS-Identifier
- NAS-IPv6-Address

Session identification attributes:

- User-Name
- NAS-Port
- Framed-IP-Address
- Called-Station-Id
- Calling-Station-Id
- Acct-Session-Id
- Acct-Multi-Session-Id
- NAS-Port-Id
- Chargeable-User-Identity
- Framed-Interface-Id
- Framed-IPv6-Prefix

# Service Authorization

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 Networks or from 3rd Party APs.

**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.

**TABLE 34 Change of Authorization (CoA) messages - Authorize-Only is not set**

| Attribute | Attribute ID | Presence | Type/Description |
|---|---|---|---|
| Message Code | | M | 43 |

**TABLE 34 Change of Authorization (CoA) messages - Authorize-Only is not set (continued)**

| Attribute | Attribute ID | Presence | Type/Description |
|---|---|---|---|
| User-Name | 1 | C | Identifies the username of the UE/subscriber to be disconnected. Username is 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 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.<br>**NOTE**<br>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. |
| 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<br>VSA: WISPr-Bandwidth-Max-UP (7)<br>VSA Length: Variable<br>The attribute contains the maximum uplink value in bits per second. |
| Vendor-Specific | 26 | O | Vendor ID: WISPr: 14122<br>VSA: WISPr-Bandwidth-Max-DOWN (8)<br>VSA Length: Variable<br>The attribute contains the maximum downlink value in bits per second. |
| 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 |

**TABLE 34 Change of Authorization (CoA) messages - Authorize-Only is not set (continued)**

| Attribute | Attribute ID | Presence | Type/Description |
|---|---|---|---|
| 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. |
| 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. |
| 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. |
| 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 35 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 36 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. |
| 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*.<br>**NOTE**<br>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 37 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. |
| 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. |

**TABLE 37 Disconnected messages (continued)**

| Attribute | Attribute ID | Presence | Type/Description |
|---|---|---|---|
| Calling Station ID | 31 | C | This attribute will contain the Calling Station ID as received from NAS during authentication or the accounting procedure. |
| 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-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. |
| 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. |
| 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 38** 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 39** Negative acknowledgment of disconnect messages

| Attribute | Attribute ID | Presence | Type/Description |
|---|---|---|---|
| Message Code | | M | 41 |
| 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.

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

**TABLE 40** 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. |

**TABLE 40 Disconnected messages initiated by dynamic authorization client (DAC) (continued)**

| 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 on page 76
- Ruckus Vendor Specific Attributes on page 76

## 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 41 WISPr vendor specific attributes - 14122**

| Attribute Name | Vendor Type | RADIUS Message Type | Purpose |
|---|---|---|---|
| WISPr-Location-ID | 1 | Access-Accept<br>Accounting Start - Stop | This attribute indicates the WISPr location id for the specified WISPr service. |
| WISPr-Location-Name | 2 | Access-Accept<br>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 Vendor Specific Attributes

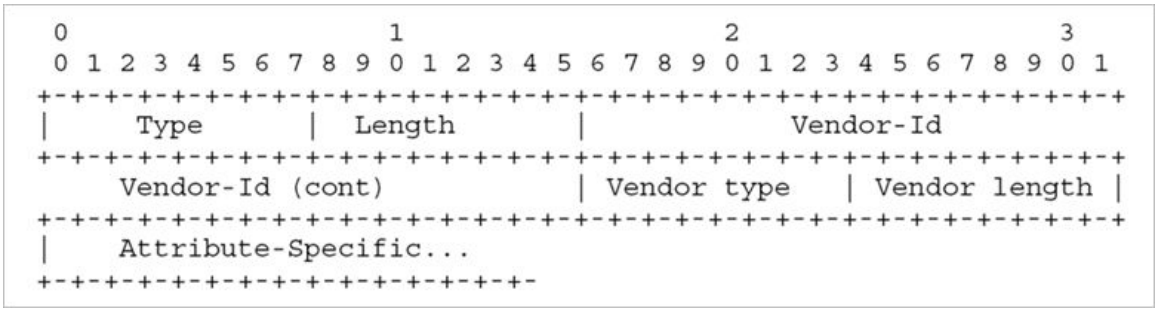
All Ruckus Networks vendor specific attributes are encoded as sequence of:

- Vendor type
- Vendor length

- Value fields

The figure shows the VSA fields.

**FIGURE 8** VSA fields




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

**TABLE 42** Ruckus Networks vendor specific attributes - 25053

| Attribute Name | Vendor Type | RADIUS Message Type | Purpose |
|---|---|---|---|
| Ruckus-TC-Acct-Ids-With-Quota | 146 | Access-Accept<br>CoA-Request | This attribute reports the messages from AAA to AP via SCG. |
| Ruckus-TC-Acct-Ctrs | 149 | Accounting-Interim-Stop | This attribute reports the messages from AP to SCG. |
| 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. |
| Ruckus-SSID | 3 | Access- Request<br>Accounting - Start -Interim- Stop | This attribute reports the associated WLANs SSID in the access request and accounting packet. |
| Ruckus-WLan-ID | 4 | Access- Request<br>Accounting - Start -Interim- Stop | This attribute reports the associated WLANs ID. Ruckus VSA is received only from AP.<br>Note: It is optional for 3rd party APs. |
| Ruckus-Location | 5 | Access- Request<br>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 AP. It is optional for 3rd party APs. |
| Ruckus-Grace-Period | 6 | Access- Request<br>Accounting - Start -Interim- Stop | This attribute is the grace period in Hotspot WLANs. |
| Ruckus-SCG-CBLADE-IP | 7 | Access- Request<br>Accounting - Start -Interim- Stop | This attribute reports the control plane IP address. |

**TABLE 42 Ruckus Networks vendor specific attributes - 25053 (continued)**

| Attribute Name | Vendor Type | RADIUS Message Type | Purpose |
|---|---|---|---|
| Ruckus-SCG-DBLADE-IP | 8 | Access- Request<br>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. |
| 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.<br>Refer to the figure showing the VSA fields. |
| Ruckus-MSISDN | 103 | | The CUI is generally used, but MSISDN can also be used. |
| Ruckus-APN | 104 | Access- Request<br>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.<br>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. |

**TABLE 42 Ruckus Networks vendor specific attributes - 25053 (continued)**

| Attribute Name | Vendor Type | RADIUS Message Type | Purpose |
|---|---|---|---|
| Ruckus-NAS-Type | 109 | Accounting - Start | The value for this parameter is always 1. |
| 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<br>Accounting - Start | It contains the Operator ID, which is part of the APN name. APN NI part is sent in the Ruckus-APN attribute.<br>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. |
| 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. |
| 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. |

**TABLE 42 Ruckus Networks vendor specific attributes - 25053 (continued)**

| Attribute Name | Vendor Type | RADIUS Message Type | Purpose |
|---|---|---|---|
| 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. |
| 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



## AP Roaming Scenarios

The AP roaming scenarios are as follows.

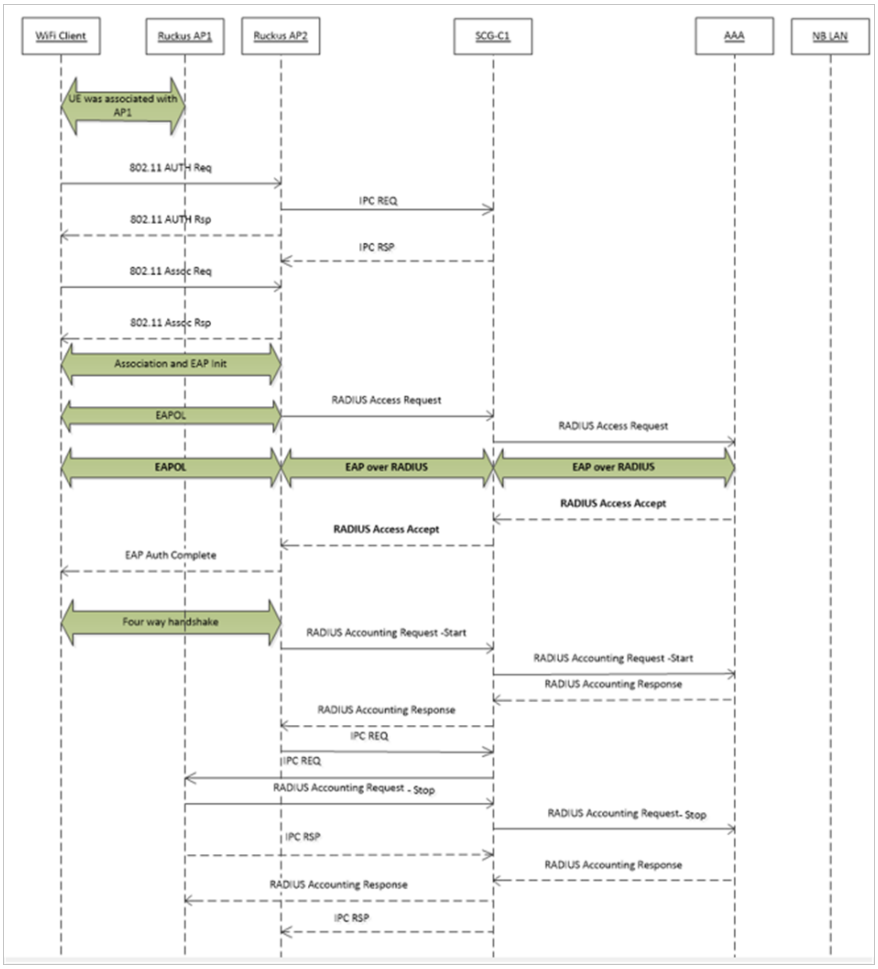
**NOTE**
The session timeout values received from the AAA server are used for maintaining the PMK/OKC cache timer values at the controller and AP. If the timer value received is less than the default value of 12 hours, it will be used. Otherwise the default value will be used as the maximum value.


- Roaming from AP1 to AP2 - PMK / OKC Disabled on page 82
- Roaming from AP1 to AP2 - PMK / OKC Enabled on page 82
- AP1 to AP2 Connected to Different Controller Node - PMK / OKC Disabled on page 83

# 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.

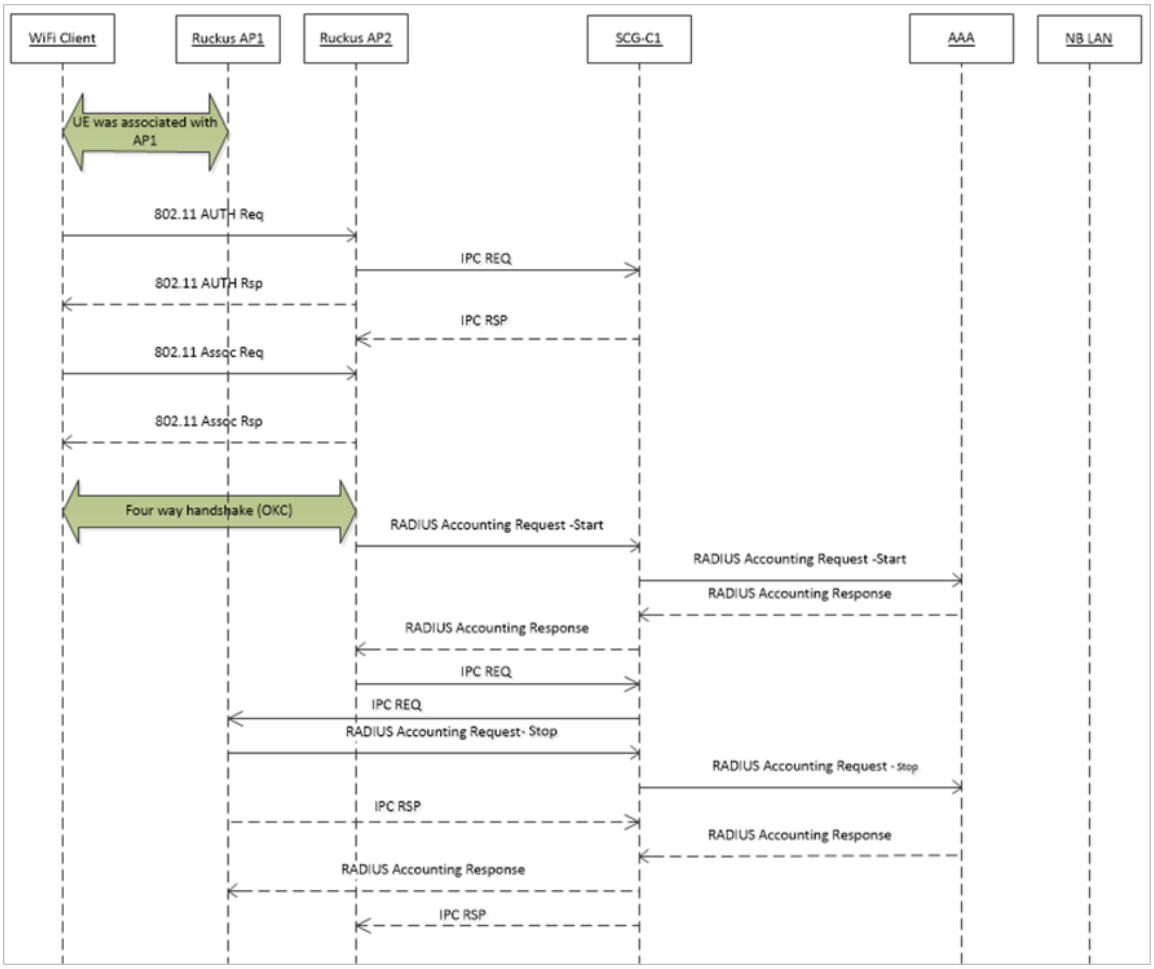
**FIGURE 9** UE roaming from AP1 to AP2 - PMK / OKC disabled




# 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.

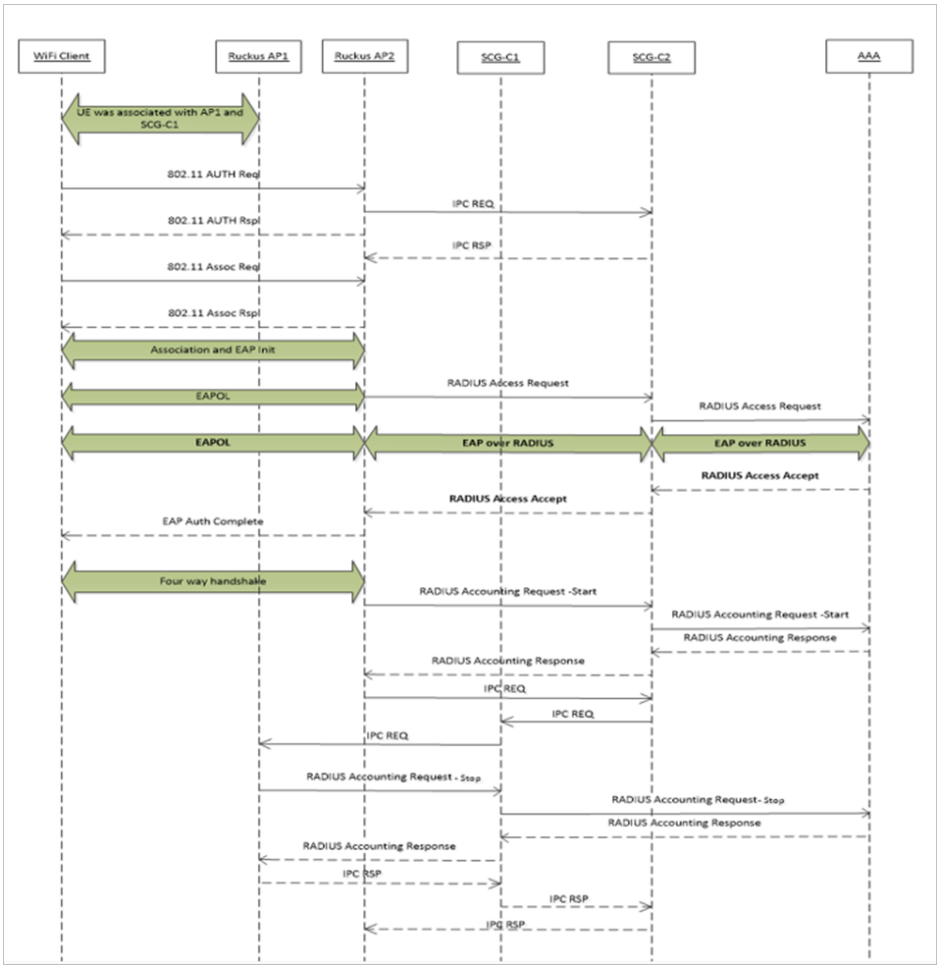
**FIGURE 10** UE roaming from AP1 to AP2 - PMK/OKC enabled




# 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 11** UE roams from AP1 to AP2 connected to different controller node



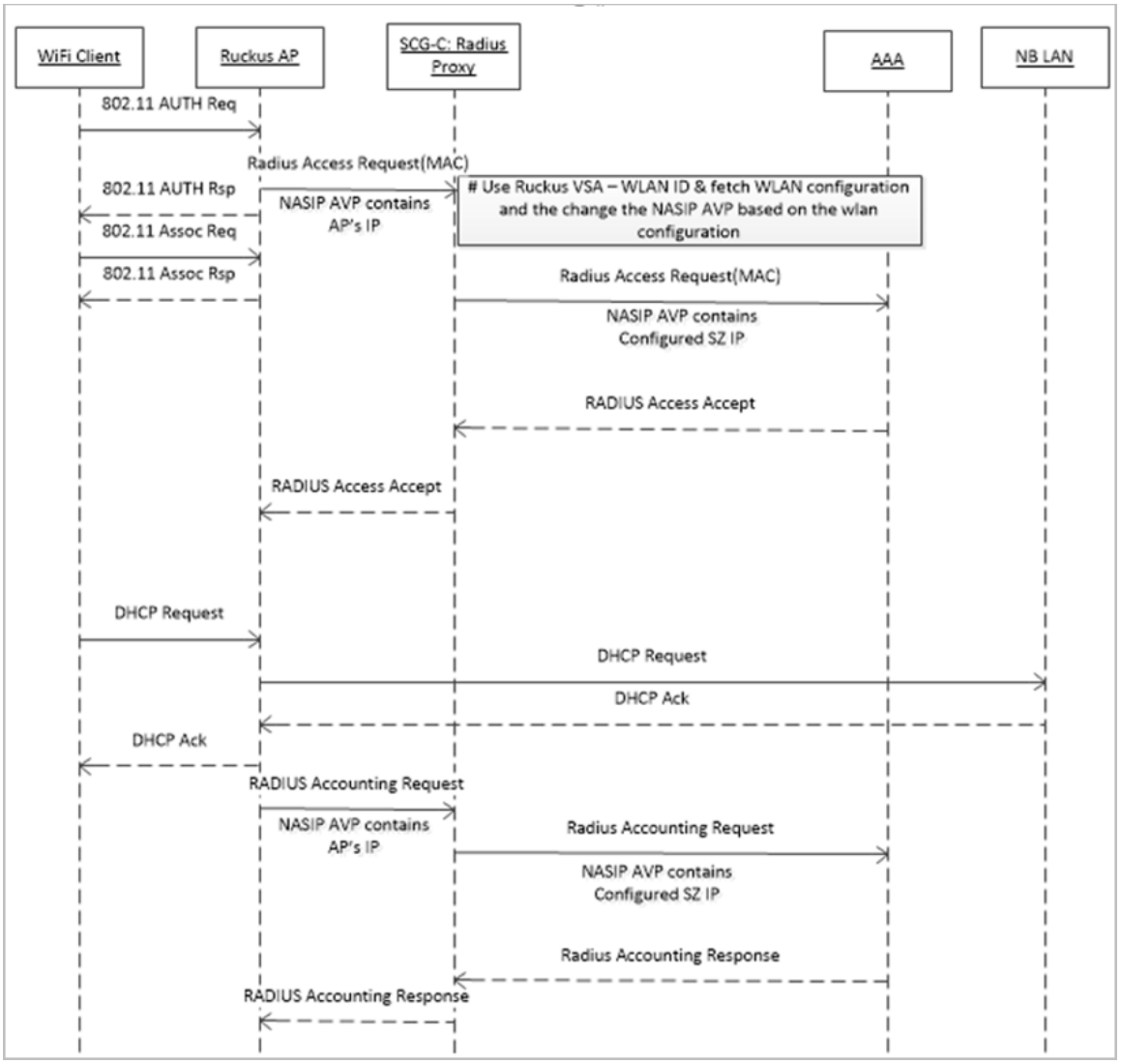
# Use Cases



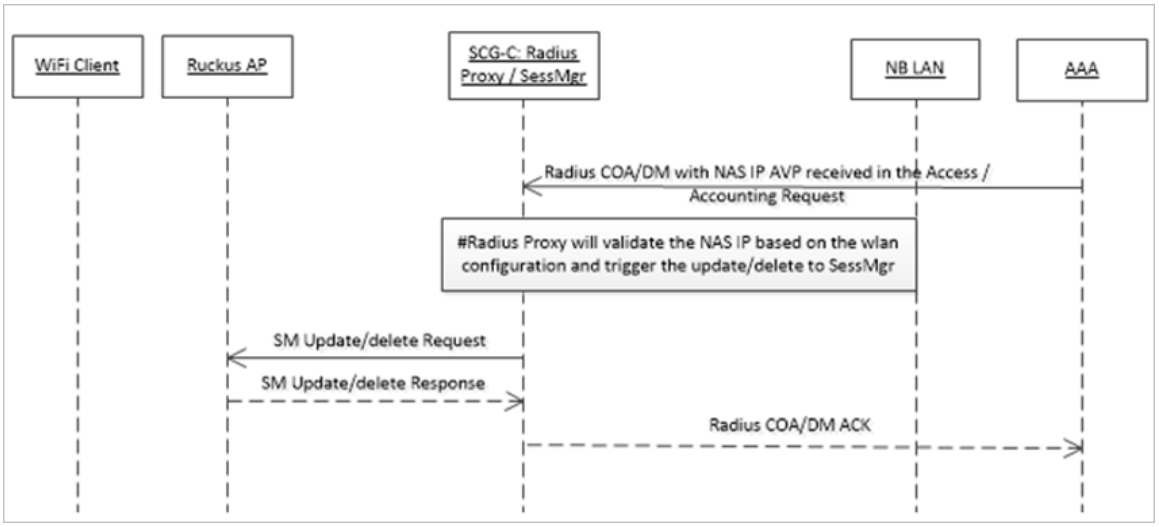
# Use Case Scenarios

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

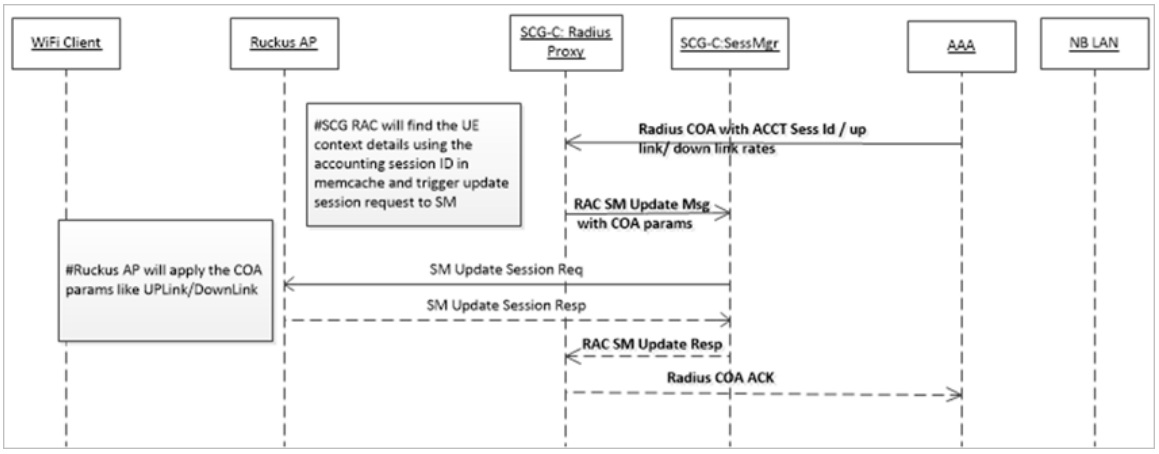
**Authentication and Accounting of NAS IP AVP**



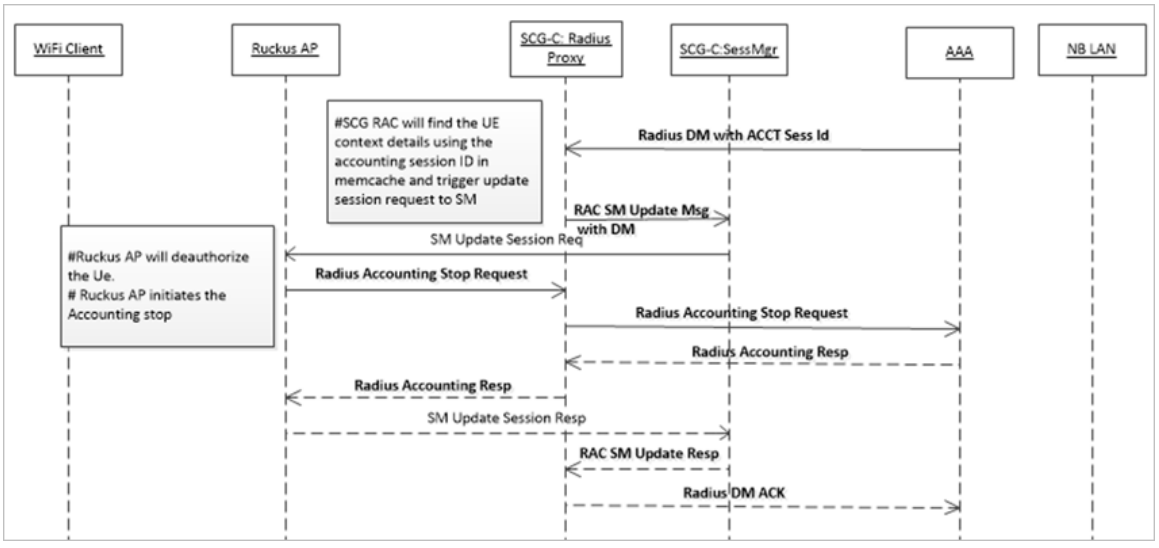

**CoA / DM Handling with NAS IP AVP**



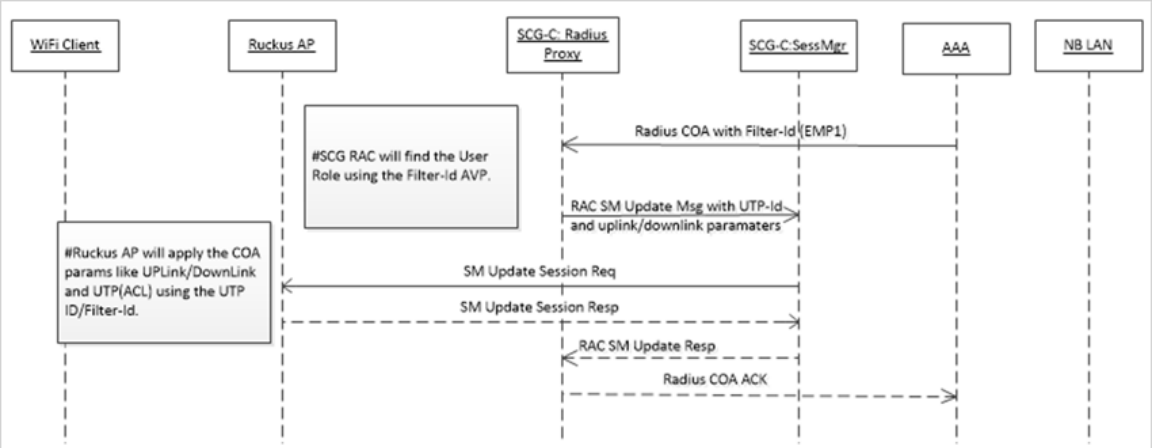

**CoA Handling with Accounting Session Identifier**




**DM Handling with Accounting Session Identifier**



### User Role change using Radius CoA - Filter Identifier





Ruckus Wireless, Inc., a wholly owned subsidiary of ARRIS International plc.
350 West Java Dr., Sunnyvale, CA 94089 USA
www.ruckuswireless.com