# Ruckus Wireless™ SmartCell Gateway™ 200 and Virtual SmartZone High-Scale

## AAA (RADIUS) Interface Reference Guide for SmartZone 3.4

Part Number 800-71098-001 Rev A
Published July 2016

www.ruckuswireless.com

# Copyright Notice and Proprietary Information



## Destination Control Statement

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

## Disclaimer

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

## Limitation of Liability

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

## Trademarks

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

# Contents

# About This Guide

This *SmartCell Gateway™ (SCG) 200 and Virtual SmartZone (vSZ-H) High-Scale AAA (RADIUS) Interface Reference Guide* describes the interface between the SCG/vSZ-H (collectively referred to as "the controller" throughout this guide) and the Authentication, Authorization and Accounting (AAA) server. It describes the message flow between the controller and AAA for EAP-based full authentication, authorization, and accounting.

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

---

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

---

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

# Document Conventions

Table 1 and Table 2 list the text and notice conventions that are used throughout this guide.

Table 1. Text conventions

| Convention | Description | Example |
|---|---|---|
| `monospace` | Represents information as it appears on screen | `[Device name]>` |
| **`monospace bold`** | Represents information that you enter | `[Device name]>` **`set ipaddr 10.0.0.12`** |
| **default font bold** | Keyboard keys, software buttons, and field names | On the **Start** menu, click **All Programs**. |
| *italics* | Screen or page names | Click **Advanced Settings**. The *Advanced Settings* page appears. |

Table 2. Notice conventions

| Notice Type | Description |
|---|---|
| NOTE | Information that describes important features or instructions |
| CAUTION! | Information that alerts you to potential loss of data or potential damage to an application, system, or device |
| WARNING! | Information that alerts you to potential personal injury |

# Terminology

Table 3 lists the terms used in this guide.

Table 3. Terms used

| Term | Description |
|---|---|
| AAA | Authentication, Authorization, and Accounting |
| CHAP | Challenge Handshake Authentication Protocol |
| EAP | Extensible Authentication Protocol |
| EPS | Evolved Packet System |
| GGSN | Gateway GPRS Support Node |

Table 3. Terms used

| Term | Description |
|---|---|
| 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 Signup |
| Passpoint | Hotspot 2.0 certification |
| PDP | Packet Data Protocol |
| PKI | Public Key Infrastructure |
| PMK | Pairwise Master Key |
| PPS-MO | Per Provider Subscription Management Object |
| R-WSG/WSG | Ruckus Wireless Security Gateway |
| R1 Device | Hotspot 2.0 R1 specification compliant device |
| R2 Device | Hotspot 2.0 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 |

# References

Table 4 lists the specifications and standards that are referred to in this guide.

Table 4. References used in this guide

| No. | Title | 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 | RFC5580 | Carrying Location Objects in RADIUS and Diameter (August 2009) |

# Legend

Table 5 lists the legends/presence used in this guide.

Table 5. 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

Table 6 lists the data types used in this guide.

Table 6. 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 |

| Data Type | Description |
|---|---|
| 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<br>where 'h' is hex digits, upper or lowercase. |
| short | 16-bit unsigned integer. |
| octets | Raw octets, printed and input as hex strings. For example, 0x123456789abcdef. |

# Related Documentation

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

# Online Training Resources

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

# Documentation Feedback

Ruckus Wireless is interested in improving its documentation and welcomes your comments and suggestions. You can email your comments to Ruckus Wireless at:

docs@ruckuswireless.com

When contacting us, please include the following information:

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

For example:

- Ruckus Wireless SmartCell Gateway 200 Administrator Guide (Release 3.4)
- Part number: 800-70917-001
- Page 88

# EAP Full Authentication

1

In this chapter:

# 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 About This Guide for the conventions used in this guide.

---

---

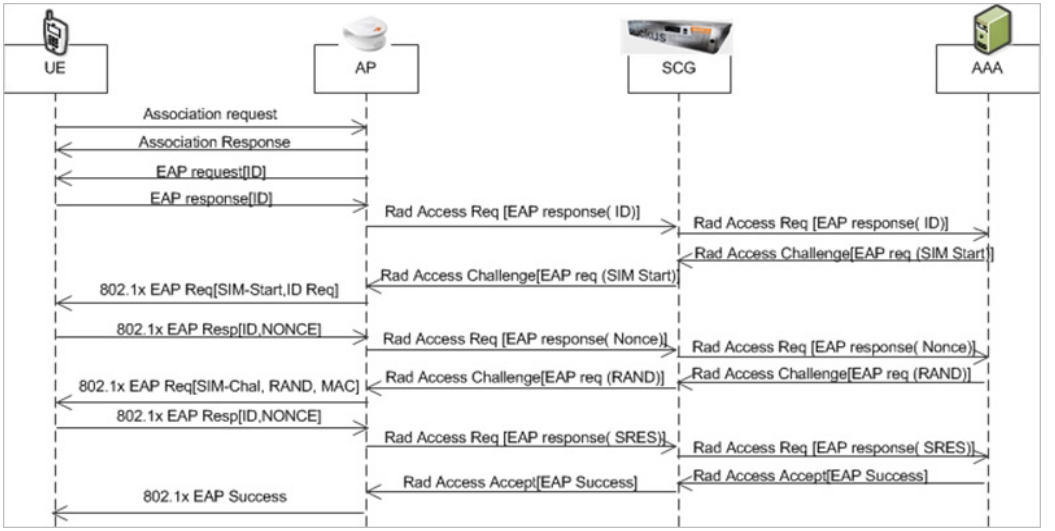
**NOTE:** Refer to AP Roaming Scenarios appendix for various scenario cases.

---

# 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. Figure 1 shows the detailed call flow.

Figure 1. Combined authentication sequence diagram




This section covers:

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

## RADIUS Access Request [ID]

Table 7 lists the attribute details for the first message sent by the controller to the AAA server.

**NOTE:** The attributes listed in this section are also described in Figure 1, Step 1.

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

Table 7. RADIUS access request attributes

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

Table 7. RADIUS access request attributes (Continued)

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

Table 7. RADIUS access request attributes (Continued)

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

Table 7. RADIUS access request attributes (Continued)

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| 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: 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: This attribute is included only if the location delivery method is Out of Band as specified in RFC 5580. |

Table 7. RADIUS access request attributes (Continued)

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| Location-Data | 128 | C | Octets | This attribute contains the actual location information. It is encoded as per RFC 5580.<br>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.<br>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.<br>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.<br>Note: This attribute is included only if location delivery method is not Out of Band. |

## RADIUS Access Challenge [EAP Request (SIM Start)]

Table 8 lists the attribute details of the first message sent by the AAA to the controller, which is forwarded to the RADIUS client (access point).

**NOTE:** The attributes listed in this section are also described in Figure 1, Step 2.

Table 8. RADIUS access challenge attributes

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

Table 8. RADIUS access challenge attributes (Continued)

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| Basic-Location-Policy-Rules | 129 | C | Octets | This attribute provides the basic privacy policy associated to the location information. It is encoded as per RFC 5580.<br>Note: This attribute is expected from the AAA server in the initial request location delivery method mentioned in RFC 5580. |
| Extended-Location-Policy-Rules | 130 | C | Octets | This attribute provides the extended privacy policy for the target whose location is specified. This attribute is sent with the above attribute (*basic location policy*). It is encoded as per RFC 5580.<br>Note: 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: 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)]

Table 9 lists the attribute details of messages sent by the controller to the AAA server and responses received from the UEs.

**NOTE:** The attributes listed in this section are also described in Figure 1, Step 3.

Table 9. RADIUS access request attributes

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| User-Name | 1 | M | String | Indicates the name of the user to be authenticated. |
| NAS-IP-Address | 4 | C | Integer | This attribute is the IP address of the AP which is serving the station/UE. |
| 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 | Integer | 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. |

Table 9. RADIUS access request attributes (Continued)

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

Table 9. RADIUS access request 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), 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 | 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). |

Table 9. RADIUS access request attributes (Continued)

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

Table 9. RADIUS access 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>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.<br>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 (RAN, MAC)]

Table 10 lists the attribute details of messages sent by the AAA to the controller, which are forwarded to the RADIUS client (access point).

**NOTE:** The attributes listed in this section are also described in Figure 1, Step 4.

Table 10. RADIUS access challenge attributes

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| State | 24 | O | Integer | 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. |

Table 10. RADIUS access challenge attributes (Continued)

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

## RADIUS Access Request [EAP Response (SRES)]

Table 11 lists the attribute details of messages sent by the controller to the AAA server.

**NOTE:** The attributes listed in this section are also described in Figure 1, Step 5.

Table 11. RADIUS access request attributes

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

Table 11. RADIUS access request attributes

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

Table 11. RADIUS access request attributes

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| 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 | 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), APMAC (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. |

Table 11. RADIUS access request attributes

| 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. |
| 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)]

Table 12 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).

**NOTE:** The attributes listed in this section are also described in Figure 1, Step 6.

Table 12. RADIUS access accept attributes

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| User-Name | 1 | O | String | Indicates the name of the user to be authenticated |
| 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. |
| Chargeable User ID | 89 | C | String | 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)<br>VSA Length: Variable<br>The attribute contains the maximum uplink value in bits per second. |

Table 12. RADIUS access accept attributes (Continued)

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| 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 12. 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. |

Table 12. RADIUS access accept attributes (Continued)

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| Accounting-Interim-Interval | 85 | O | Integer | Indicates the number of seconds between each interim update for this specific session. If the value is blank, the configured default value is used as the accounting interim interval. |
| 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 server 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). |

Table 12. RADIUS access accept attributes (Continued)

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| Vendor-Specific | 26 | C | APN-NI | Vendor ID: Ruckus:25053<br>VSA: Ruckus-APN-NI (104)<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 | 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: 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: This attribute is expected from the AAA server in the initial request location delivery method as mentioned in RFC 5580. |

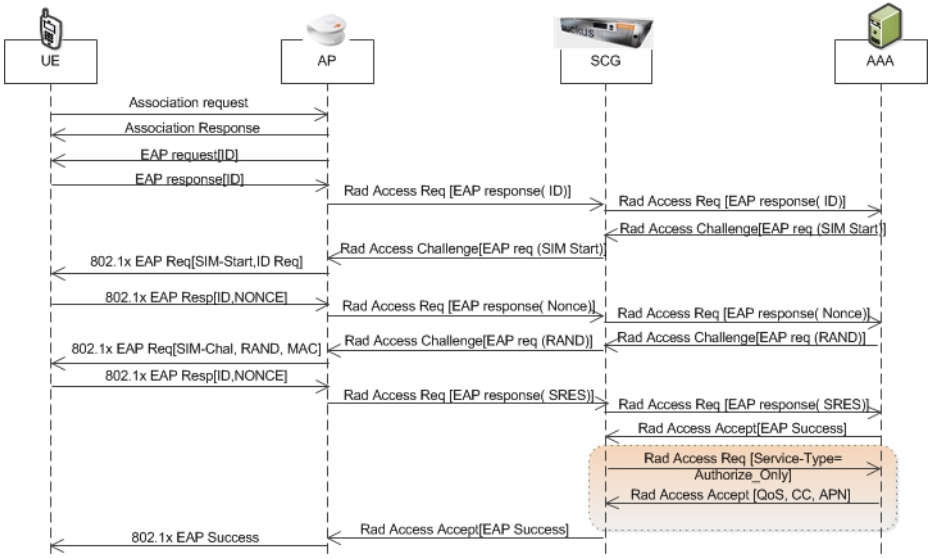
Table 12. RADIUS access accept attributes (Continued)

| 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: 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, an additional access request is sent to the AAA server to process a service authorization. Figure 2 shows the detailed call flow.

Figure 2. 3GPP based solution sequence diagram




This section covers:

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

## RADIUS Access Request [ID]

Table 13 lists the attribute details of the first message sent by the controller to AAA.

**NOTE:** The attributes listed in this section are also described in Figure 2, Step 1.

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

Table 13. RADIUS access request attributes

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| User-Name | 1 | M | String | Indicates the name of the user for authentication. |
| NAS-IP-Address | 4 | C | Integer | This attribute is the IP address of the AP which is serving the station/UE. |
| 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, which is 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-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. |

Table 13. RADIUS access request attributes (Continued)

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

Table 13. RADIUS access request attributes (Continued)

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

Table 13. RADIUS access request attributes (Continued)

| 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. |
| 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: 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: This attribute is included only if the location delivery method is Out of Band as specified in RFC 5580. |
| Location-Data | 128 | C | Octets | This attribute contains the actual location information. It is encoded as per RFC 5580.<br>Note: This attribute is included only if the location delivery method is Out of Band as specified in RFC 5580. |

Table 13. RADIUS access request attributes (Continued)

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| Basic-Location-Policy-Rules | 129 | C | Octets | This attribute provides the basic privacy policy associated to the location information. It is encoded as per RFC 5580.<br>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.<br>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.<br>Note: This attribute is included only if the location delivery method is not Out of Band as specified in RFC 5580. |

## RADIUS Access Challenge [EAP Request (SIM Start)]

Table 14 lists the attribute details of the messages sent by the AAA server to the controller and forwarded to the RADIUS client (NAS).

**NOTE:** The attributes listed in this section are also described in Figure 2, Step 2.

Table 14. RADIUS access challenge attributes

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| State | 24 | O | String | 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). |

Table 14. RADIUS access challenge attributes (Continued)

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| Message Authenticator | 80 | M | Octets | This attribute is used for signing access request for preventing spoofing of access request using CHAP, ARAP or EAP authentication methods. It authenticates this whole RADIUS packet - HMAC-MD5 (Type\| Identifier \| Length \| Request Authenticator \| Attributes). |
| 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: 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: This attribute is expected from the AAA server in the initial request location delivery method as mentioned in RFC 5580. |

Table 14. RADIUS access challenge attributes (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: 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)]

Table 15 lists the attribute details for messages sent by the controller to the AAA server (response received from UE).

**NOTE:** The attributes listed in this section are also described in Figure 2, Step 3.

Table 15. RADIUS access request attributes

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

Table 15. 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. |
| State | 24 | O | String | 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. |

Table 15. RADIUS access request attributes (Continued)

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

Table 15. 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), 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). |

Table 15. RADIUS access request attributes (Continued)

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

Table 15. RADIUS access request attributes (Continued)

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| Basic-Location-Policy-Rules | 129 | C | Octets | This attribute provides the basic privacy policy associated to the location information. It is encoded as per RFC 5580.<br>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.<br>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)]

Table 16 lists the attribute details for messages sent by the AAA server to the controller and forwarded to the RADIUS client NAS.

**NOTE:** The attributes listed in this section are also described in Figure 2, Step 4.

Table 16. RADIUS access challenge attributes

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| State | 24 | O | String | 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 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). |

## RADIUS Access Request [EAP Response (SRES)]

Table 17 lists the attribute details for messages sent by controller to AAA.

**NOTE:** The attributes listed in this section are also described in Figure 2, Step 5.

Table 17. RADIUS access request messages

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| User-Name | 1 | M | String | Indicates the name of the user for authentication. |
| 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/UE. |
| 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 | String | 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. |

Table 17. RADIUS access request messages (Continued)

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| 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.<br>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>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>VSA Length: Variable<br>Reports the associated WLANs SSID in access request and accounting packet.<br>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 | String | Allows NAS to send the ID (UE MAC), which indicates as to who is calling this server. |

Table 17. RADIUS access request messages (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), 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). |

Table 17. RADIUS access request messages (Continued)

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

## RADIUS Access Accept [EAP Success (MSK)]

Table 18 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).

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

**NOTE:** The attributes listed in this section are also described in Figure 2, Step 6.

Table 18. RADIUS access accept messages

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| User-Name | 1 | M | String | Indicates the name of the user for authentication. |
| 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). |

Table 18. RADIUS access accept messages (Continued)

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| 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). 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<br>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. |

Table 18. RADIUS access accept messages (Continued)

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

Table 18. RADIUS access accept messages (Continued)

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| 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 | C | String | This attribute is MSISDN or any chargeable user identity returned by the AAA server. This attribute is mandatory for TTG sessions only. |
| 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: 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: This attribute is expected from the AAA server if the location delivery method is accounting request as specified in RFC 5580. |

Table 18. RADIUS access accept 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: 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. Table 19 lists the attribute details for messages sent by the controller to the AAA server.

**NOTE:** The attributes listed in this section are also described in Figure 2, Step 7.

Table 19. Authorization 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. |

Table 19. Authorization access request attributes (Continued)

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| 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), 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. |
| 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).

Table 20 lists the attribute details for messages sent by the AAA server to the controller.

**NOTE:** The attributes listed in this section are also described in Figure 2, Step 8.

Table 20. Authorization access accept attributes

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| User-Name | 1 | O | String | Indicates the name of the user for authentication. |
| 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 | O | APN-NI | Vendor ID: Ruckus: 25053<br>VSA: Ruckus-APN-NI(104)<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. |

Table 20. Authorization access accept attributes

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

Table 20. Authorization access accept attributes

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| Chargeable User ID | 89 | C | String | This attribute is MSISDN or any chargeable user identity returned by the AAA server. This attribute is mandatory for TTG sessions only. |

# RADIUS Access Reject

Table 21 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 21. 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

# 2

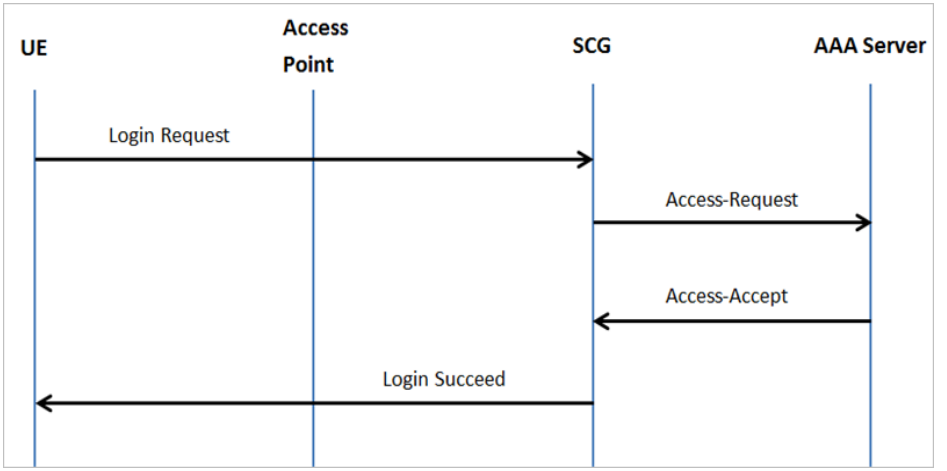
In this chapter:

# 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. Figure 3 shows the detailed call flow.

Figure 3. Hotspot (WISPr) call flow




This section covers:

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

# Hotspot (WISPr) Authentication Request

Table 22 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 Finger' is enabled in **Configuration>> AP Zones>> WLAN>> Advanced Options**.

Table 22. 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 | C | 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*: The attribute will not be available if the MTU size is set to auto in the WLAN configuration page of the controller Web interface. |

Table 22. Hotspot (WISPr) authentication request attributes

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

Table 22. Hotspot (WISPr) authentication request attributes

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| 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 | 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 | STA's MAC address where the letters in the MAC address are in uppercase. For example, 11-22-33-AA-BB-CC. |

Table 22. Hotspot (WISPr) authentication request attributes

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| 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). APMAC (MAC address of AP) is a user defined attribute where the maximum length is 62. This attribute can also be configured as per the configuration specified on the WLAN configuration page of the controller web interface. This attribute can also be configured as per the configuration specified on the WLAN configuration page of the controller web interface. |
| Chap-Challenge | 60 | M | String | This attribute contains the chap challenge sent by NAS to a PPP CHAP user. |
| NAS-Port-Type | 61 | O | Integer | This attribute indicates the physical port type of the NAS, which authenticates the user. |
| Vendor-Specific | 26 | C | Integer | Vendor ID: Ruckus: 2503<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. |

Table 22. Hotspot (WISPr) authentication request attributes

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| 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: 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: 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 | C | Octets | This attribute contains the actual location information. It is encoded as per RFC 5580.<br>Note: This attribute is included in the first access request when the location delivery method is Out of Band. If the location delivery method is the initial request then the subsequent access request is included in this parameter - as specified in RFC 5580. |

Table 22. Hotspot (WISPr) authentication request attributes

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| 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: This attribute is included in the first access request when the location delivery method is Out of Band. If the location delivery method is the initial request then the subsequent access request is included in this parameter - as specified in RFC 5580. |
| Extended-Location-Policy-Rules | 130 | C | Octets | This attribute provides the extended privacy policy for the target whose location is specified. This attribute is sent with the above attribute (*basic location policy*). It is encoded as per RFC 5580.<br>Note: This attribute is included in the first access request when the location delivery method is Out of Band. If the location delivery method is the initial request then the subsequent access request is included in this parameter - as specified in RFC 5580. |
| Location-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: This attribute is included only if the location delivery method is the initial request or accounting request as specified in RFC 5580. |

# Hotspot (WISPr) Authentication Response

Table 23 lists the attribute details of messages sent by the Hotspot (WISPr) module to the controller.

Table 23. Hotspot (WISPr) authentication request attributes

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| 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>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 | O | Integer | Vendor ID: Ruckus: 25053<br>Vendor Type: 7<br>VSA: Ruckus-Grace-Period<br>VSA Length: Variable<br>This attribute is the grace period in hotspot (WISPr) WLANs. |
| Session-Timeout | 27 | O | Integer | This attribute de-authenticates the UE when the session time expires. |
| Idle-Timeout | 28 | O | Integer | This attribute sets the maximum number of consecutive seconds of idle connection allowed to the user before termination of the session. |

Table 23. Hotspot (WISPr) authentication request attributes

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| Accounting-Interim-Interval | 85 | O | Integer | Indicates the number of seconds between each interim update for this specific session. If the value is blank, the configured default value is used as the accounting interim interval. |
| 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: 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: 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: 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]

Table 24 lists the attribute details of messages sent by the controller to the hotspot (WISPr) module.

Table 24. 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/UE. |
| 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. |

Table 24. Hotspot (WISPr) accounting request (start) attributes (Continued)

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| 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<br>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<br>VSA Length: 6<br>This attribute value is observed by NBI, when the GRE tunnel is set up. |

Table 24. Hotspot (WISPr) accounting request (start) attributes (Continued)

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| Called Station ID | 30 | M | 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 | 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). APMAC (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. |

Table 24. Hotspot (WISPr) accounting request (start) attributes (Continued)

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| Acct-Delay-Time | 41 | C | Integer | This attribute can only be seen in accounting retry packets. This is a configurable option and by default this attribute is disabled. |
| Acct-Session-ID | 44 | M | Integer | This attribute is a unique accounting identity to facilitate easy matching of start, interim and stop records in a log file. The start, interim and stop records for a given session must have the same *Acct-Session-ID.* |
| Acct-Authentic | 45 | M | Integer | This attribute value in EAP 802.1X-Auth and hotspot (WISPr) is: 1 for RADIUS-Auth and 2 for MAC-Auth local. |
| Acct-Session-Time | 46 | M | Integer | This attribute can only be present with *Acct-Status-Type = Interim, Stop.* |
| Acct-Terminate-Cause | 49 | M | Integer | This attribute can only be present with *Acct-Status-Type = Stop.* |
| Acct-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. |

Table 24. Hotspot (WISPr) accounting request (start) attributes (Continued)

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| 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 | C | Octets | This attribute contains the actual location information. It is encoded as per RFC 5580.<br>Note: This attribute is included only if the location delivery method is the accounting request as specified in RFC 5580. |
| Basic-Location-Policy-Rules | 129 | M | String | This attribute provides the basic privacy policy associated to the location information. It is encoded as per RFC 5580.<br>Note: This attribute is included only if the location delivery method is the accounting request as specified in RFC 5580. |
| Extended-Location-Policy-Rules | 130 | C | Octets | This attribute provides the extended privacy policy for the target whose location is specified.This attribute is sent with the above attribute (*basic location policy*). It is encoded as per RFC 5580.<br>Note: This attribute is included only if the location delivery method is the accounting request as specified in RFC 5580. |

# Hotspot (WISPr) Accounting Request [Stop/Interim]

Table 25 lists the attribute details of messages sent by the controller to the Hotspot (WISPr) module.

Table 25. 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 | IP Address | This attribute is the IP address of the AP which is serving the station/UE. |
| 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. |

Table 25. Hotspot (WISPr) accounting request (stop/interim) attributes

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| 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<br>VSA Length: 6<br>This attribute indicate the control plane IP address that is being used. |

Table 25. Hotspot (WISPr) accounting request (stop/interim) attributes

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| Vendor-Specific | 26 | O | Integer | Vendor ID: Ruckus: 25053<br>Vendor Type: 8<br>VSA: Ruckus-SCG-DBLADE-IP VSA<br>VSA Length: 6<br>This attribute value is observed by NBI, when the GRE tunnel is set up. |
| Called Station ID | 30 | M | 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 | 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). APMAC (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. |

Table 25. Hotspot (WISPr) accounting request (stop/interim) attributes

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| Proxy-State | 33 | O | Octets | This attribute is available to be sent by a proxy server (controller) to another server (AAA server) when forwarding an access request, accounting request (start, stop or interim) and must be returned unmodified in the access accept, access reject, access challenge and accounting response. |
| Acct-Status-Type | 40 | M | Integer | This attribute has the following values where 1 is Start, 2 is Stop, 3 is Interim, 7 are On and 8 are Off. |
| Acct-Delay-Time | 41 | C | Integer | This attribute can only be seen in accounting retry packets. This is a configurable option and by default this attribute is disabled. |
| Acct-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.* |

Table 25. Hotspot (WISPr) accounting request (stop/interim) attributes

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| 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. |
| 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: This attribute is included only if the location delivery method is accounting request as specified in RFC 5580. |

Table 25. Hotspot (WISPr) accounting request (stop/interim) attributes

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

# Hotspot (WISPr) Accounting Response

Table 26 lists the attribute details of messages received by the controller to the hotspot (WISPr) module.

Table 26. Hotspot (WISPr) accounting response attributes

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

# Hotspot 2.0 Authentication

# 3

In this chapter:

# 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 either / LOCAL DB / RADIUS / AD / LDAP / Facebook or LinkedIn or Google 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. Table 27 lists the attributes specific to Hotspot 2.0.

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

Table 27. Hotspot 2.0 RADIUS access request attributes

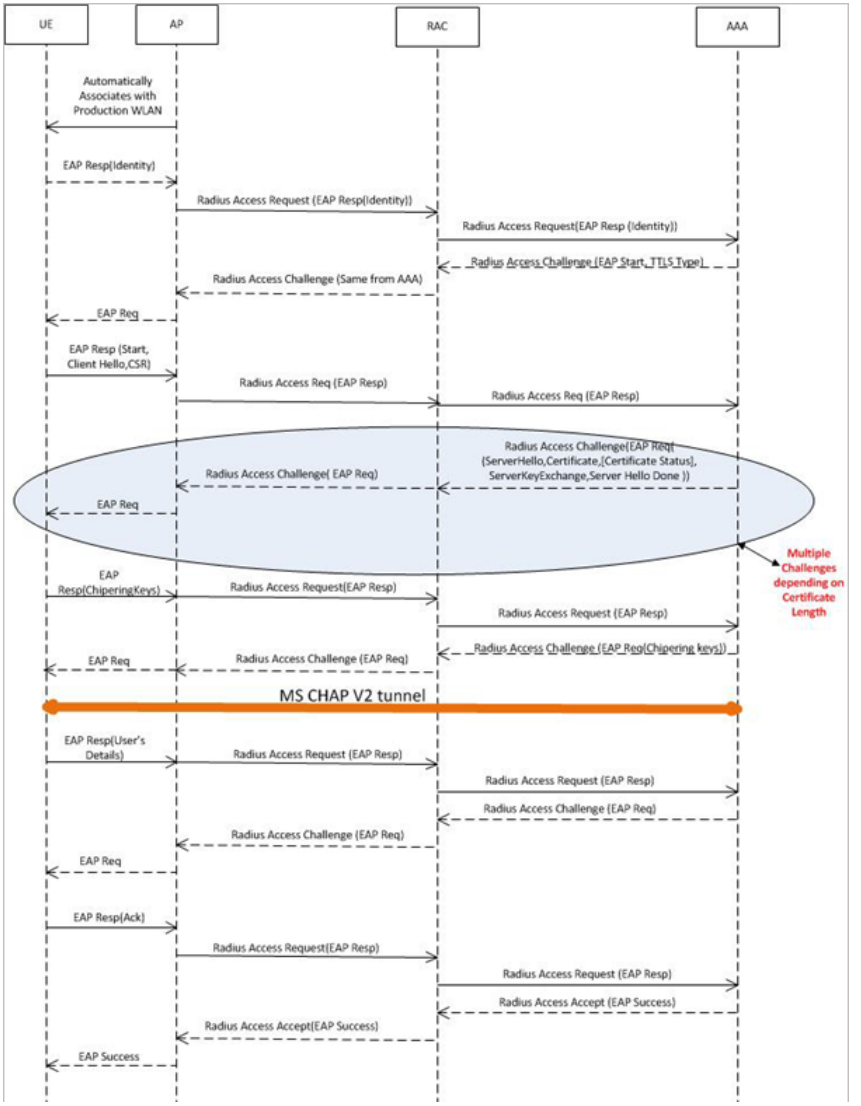
| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| Vendor-Specific | 26 | C | String | Vendor ID: 40808<br>Vendor Type: 2<br>VSA: AP Version<br>VSA Length: Variable<br>This attribute indicates version 0 as R1 compliant AP and version 1as R2 compliant AP. |
| Vendor-Specific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

# R2 Device 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 **Configuration** > **Services&Profiles > Hotspot 2.0 Identity** of the controller web interface. Internal OSU is also supported.

Figure 4 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 username attribute used in the request.

Figure 4. R2 device authentication



## Access Request

Table 28 lists the attributes specific to Hotspot 2.0.

Table 28. 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<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. |

## Access Response

Table 29 lists the attributes specific to Hotspot 2.0.

Table 29. Hotspot 2.0 RADIUS access response attributes

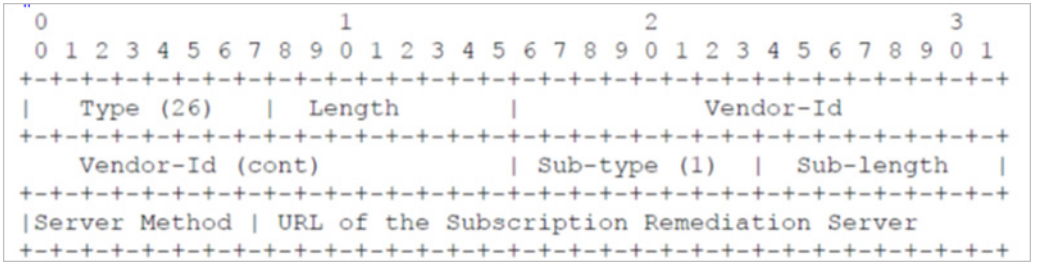
| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| Vendor-Specific | 26 | C | String | Vendor ID: 40808<br>Vendor Type: 1<br>VSA: Subscription Remediation Needed<br>VSA Length: Variable<br>This attribute provides the remediation URL. |
| Vendor-Specific | 26 | C | String | 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 reauthentication delay. |
| Vendor-Specific | 26 | C | String | Vendor ID: 40808<br>Vendor Type: 5<br>VSA: Session Information URL<br>VSA Length: Variable<br>This attribute provides the URL details seen before session termination. |

**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.

# 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). Figure 5 indicates the VSA fields in a hotspot 2.0 subscription remediation flow.

Figure 5. Hotspot 2.0 VSA fields



# Accounting

# 4

In this chapter:



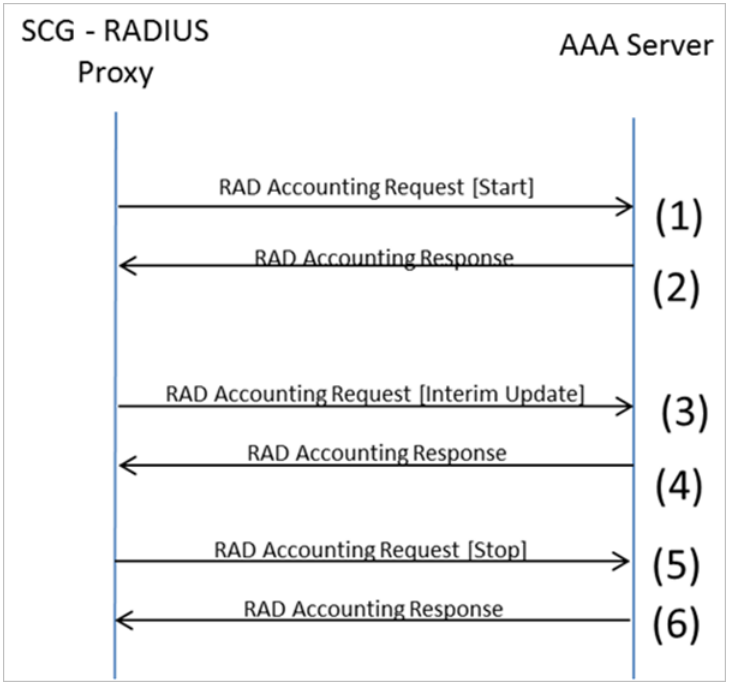
---

**NOTE:** The Accounting Interface between SZ or vSZ and the AAA server is IPv4 as well as IPv6. If SCG is configured with an IPv6 address and AAA is also configured with an IPv6 address and reachable from SZ/vSZ, then Accounting messages with IPv6 can be exchanged. This includes Account-Start/Interim/Stop/On/Off. For details on how to configure IPv6 Accounting AAA, refer the SCG vSZ-H Administrator guide.

# Controller Initiated Accounting Messages (TTG Sessions)

In this call flow, the controller initiates RADIUS accounting messages towards accounting AAA server after EAP-SIM authentication and when the data session is established. Figure 6 shows the detailed call flow.

Figure 6. RADIUS Accounting call flow




This section covers:

- RADIUS Accounting Request [Start]
- RADIUS Accounting Request [Stop/Interim Update]
- RADIUS Accounting Response

## RADIUS Accounting Request [Start]

Table 30 lists the attribute details of messages sent by the controller to the AAA server.

**NOTE:** The attributes listed in this section are also described in Figure 6, Step 1.

Table 30. RADIUS accounting attributes

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| User-Name | 1 | M | String | The username of the given accounting session. |
| NAS-IP-Address | 4 | C | Integer | This attribute is the IP address of the AP which is serving the station/UE. |
| Service-Type | 6 | O | Integer | Indicates the type of service based on the user request or the type of service to be provided. |
| Framed-IP-Address | 8 | O | IP Address | This attribute indicates the address to be configured for the user. |
| Login-IP-Host | 14 | M | Integer | Variable IP address. |
| Class | 25 | O | Integer | This attribute is sent by the server in access accept. The client should include this attribute in the accounting request without modifying it. |
| Vendor-Specific | 26 | C | Integer | Vendor ID:Ruckus:25053<br>VSA: Ruckus-APN-NI (104)<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. |

Table 30. RADIUS accounting attributes (Continued)

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| Vendor-Specific | 26 | C | Octets | Vendor ID:Ruckus:25053<br>VSA: Ruckus-APN-OI (111)<br>VSA Length: Variable<br>It contains the *Operator ID*, which is part of the APN name. |
| Vendor-Specific | 26 | C | String | Vendor ID: Ruckus:25053<br>VSA: Ruckus-IMSI (102)<br>VSA Length: Variable<br>This Ruckus VSA contains values to be used by the controller's CDR generating module. |
| Vendor-Specific | 26 | C | Integer | Vendor ID: Ruckus:25053<br>VSA: Ruckus-NAS-Type (109)<br>VSA Length: 6<br>This Ruckus VSA contains the value to be used by the controller's CDR generating module. |
| Vendor-Specific | 26 | M | Integer | Vendor ID: 3GPP: 10415<br>VSA: 3GPP-RAT-Type (21)<br>VSA Length: 3<br>This Ruckus VSA contains the value to be used by controller's CDR generating module. |

Table 30. RADIUS accounting attributes (Continued)

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| Vendor-Specific | 26 | O | String | Vendor ID: 3GPP: 10415<br>VSA:3GPP-GPRS-Negotiated-QoS-Profile (5)<br>VSA Length: Variable<br>QoS bytes (octets). This attribute contains QoS received from AAA or negotiated by GGSN, if it is not received from the core network, The controller will use the default QoS. GPP-GPRS-Negotiated-QoS-Profile will be present in this message. |
| Vendor-Specific | 26 | C | Integer | Vendor ID: Ruckus:25053<br>VSA: Ruckus-Charging-Charac (118)<br>VSA Length: Variable<br>This attribute carries the charging characteristics value, which is received from the AAA server. This attribute carries the charging characteristics value, which is received from the AAA server. |
| Vendor-Specific | 26 | C | Integer | Vendor ID: Ruckus:25053<br>VSA: Ruckus-PDP-Type (119)<br>VSA Length: 4<br>This Ruckus VSA contains the value to be used by the controller's CDR generating module. |
| Vendor-Specific | 26 | C | Integer | Vendor ID: Ruckus:25053<br>VSA: Ruckus-ChCh-Selection-Mode (121)<br>VSA Length: 3<br>This Ruckus VSA contains the value to be used by the controller's CDR generating module. |

Table 30. RADIUS accounting attributes (Continued)

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| Vendor-Specific | 26 | C | Integer | Vendor ID: 25053<br>VSA: Ruckus-AAA-IP (122)<br>VSA Length: 6<br>This Ruckus VSA contains the value to be used by the controller's CDR generating module. |
| 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 | Integer | Vendor ID: Ruckus:25053<br>VSA: Ruckus-Dynamic-Address-Flag (120)<br>VSA Length: 3<br>The flag value of this Ruckus VSA is either 0 or 1. This attribute contains the value to be used by the controller's CDR generating module. |
| Vendor-Specific | 26 | M | Integer | Vendor ID: 25053<br>VSA: Ruckus-SGSN-IP (117)<br>VSA Length: 6<br>This Ruckus VSA contains the value to be used by the controller's CDR generating module. |

Table 30. RADIUS accounting attributes (Continued)

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| Called Station ID | 30 | O | String | Integer |
| 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), APMAC (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) with the value of 1 as (Start). |
| Acct-Delay-Time | 41 | C | Integer | In case the accounting message gets retransmitted this attribute will contain the time stamp of the consecutive retransmitted message. |
| Acct-Session-ID | 44 | M | Integer | This attribute is a unique accounting identity to facilitate easy matching of start, interim and stop records in a log file. The start, interim and stop records for a given session must have the same *Acct-Session-ID.* |

Table 30. RADIUS accounting attributes (Continued)

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| 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 | Indicates the physical port type of NAS, which authenticates the user. |
| Chargeable User ID | 89 | C | String | This attribute is MSISDN or any chargeable user identity returned by the AAA server. This attribute is unchanged when it is received in the RADIUS Access Accept message. |
| Location-Information | 127 | M | Octets | Note: This attribute is included only when the expected location delivery method is accounting request as specified in RFC 5580. |
| Location-Data | 128 | C | Octets | This attribute contains the actual 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. |
| 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: This attribute is included only when the expected location delivery method is accounting request as specified in RFC 5580. |

Table 30. RADIUS accounting 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>Note: This attribute is included only when the expected location delivery method is accounting request as specified in RFC 5580. |

## RADIUS Accounting Request [Stop/Interim Update]

Table 31 lists the attribute details of messages sent by the controller to the AAA server.

**NOTE:** The attributes listed in this section are also described in Figure 6, Step 5.

Table 31. RADIUS accounting request (stop/interim update) attributes

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| User-Name | 1 | M | String | The username of the given accounting session. |
| NAS-IP-Address | 4 | C | Integer | This attribute is the IP address of the AP which is serving the station/UE. |
| Service-Type | 6 | O | Integer | Indicates the type of service based on the user request or the type of service to be provided. |
| Framed-IP-Address | 8 | O | IP Address | This attribute indicates the address to be configured for the user. |
| Login-IP-Host | 14 | O | Integer | Variable IP address. |

Table 31. RADIUS accounting request (stop/interim update) attributes (Continued)

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| Vendor-Specific | 26 | C | Integer | Vendor ID: Ruckus:25053<br>VSA: Ruckus-APN-NI(104)<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 | C | Integer | Vendor ID: Ruckus:25053<br>VSA: Ruckus-Selection-Mode (106)<br>VSA Length: 6<br>This Ruckus VSA contains the value to be used by the controller's CDR generating module. |
| Vendor-Specific | 26 | C | Octets | Vendor ID: Ruckus:25053<br>VSA: Ruckus-APN-OI (111)<br>VSA Length: Variable<br>This Ruckus VSA contains the value to be used by the controller's CDR generating module. |
| Vendor-Specific | 26 | C | String | Vendor ID: Ruckus:25053<br>VSA: Ruckus-IMSI (102)<br>VSA Length: Variable<br>This Ruckus VSA contains the value to be used by the controller's CDR generating module. |
| Vendor-Specific | 26 | M | Integer | Vendor ID: 25053<br>VSA: Ruckus-SGSN-IP (117)<br>VSA Length: 4<br>This Ruckus VSA contains the value to be used by the controller's CDR generating module. |

Table 31. RADIUS accounting request (stop/interim update) attributes (Continued)

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| Vendor-Specific | 26 | C | Integer | Vendor ID: Ruckus:25053<br>VSA: Ruckus-NAS-Type (109)<br>VSA Length: 6<br>This Ruckus VSA contains the value to be used by the controller's CDR generating module. |
| Vendor-Specific | 26 | O | Integer | Vendor ID: 3GPP: 10415<br>VSA: 3GPP-RAT-Type (21)<br>VSA Length: 3<br>This Ruckus VSA contains the value to be used by the controller's CDR generating module. |
| Vendor-Specific | 26 | O | String | Vendor ID: 3GPP: 10415<br>VSA:3GPP-GPRS-Negotiated-QoS-Profile(5)<br>VSA Length: Variable<br>QoS bytes (octets). This attribute contains QoS received from AAA or negotiated by GGSN, if it is not received from the core network, The controller will use the default QoS. GPP-GPRS-Negotiated-QoS-Profile will be present in this message. |
| 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. |

Table 31. RADIUS accounting request (stop/interim update) attributes (Continued)

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| 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. |
| 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 | 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), APMAC (MAC address of AP) and user defined address (maximum length of 62). |
| Acct-Status-Type | 40 | M | Integer | This attribute indicates the *Accounting-Request* type. Possible values are Stop(2), interim update (3). |
| Acct-Delay-Time | 41 | C | Integer | In case the accounting message gets retransmitted, this attribute will contain the time stamp of the consecutive retransmitted message. |

Table 31. RADIUS accounting request (stop/interim update) attributes (Continued)

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| 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-Session-Time | 46 | M | Integer | This attribute indicates the number of seconds the user receives the service for. |
| Acct-Input-Packets | 47 | M | Integer | This attribute indicates the number of packets received from the port over the course of this service provided. |
| Acct-Output-Packets | 48 | M | Integer | This attribute indicates the number of packets sent to the port in the course of delivering this service. |
| 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-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-input-octets counter is wrapped around 2^32 in the course of delivering this service. |

Table 31. RADIUS accounting request (stop/interim update) attributes (Continued)

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| 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. |
| Chargeable User ID | 89 | C | String | This attribute is MSISDN or any chargeable user identity returned by the AAA server. This attribute is unchanged when it is received in the RADIUS Access Accept message. |
| Location-Information | 127 | M | 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 | C | Octets | This attribute contains the actual 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. |
| 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: This attribute is included only when the expected location delivery method is Accounting Request as specified in RFC 5580. |

Table 31. RADIUS accounting request (stop/interim update) 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>Note: This attribute is included only when the expected location delivery method is accounting request as specified in RFC 5580. |

## RADIUS Accounting Response

Table 32 lists the attribute details of messages sent by the AAA to the controller.

**NOTE:** The attributes listed in this section are also described in Figure 6, Steps 2, 4, and 6.

Table 32. RADIUS accounting response attributes

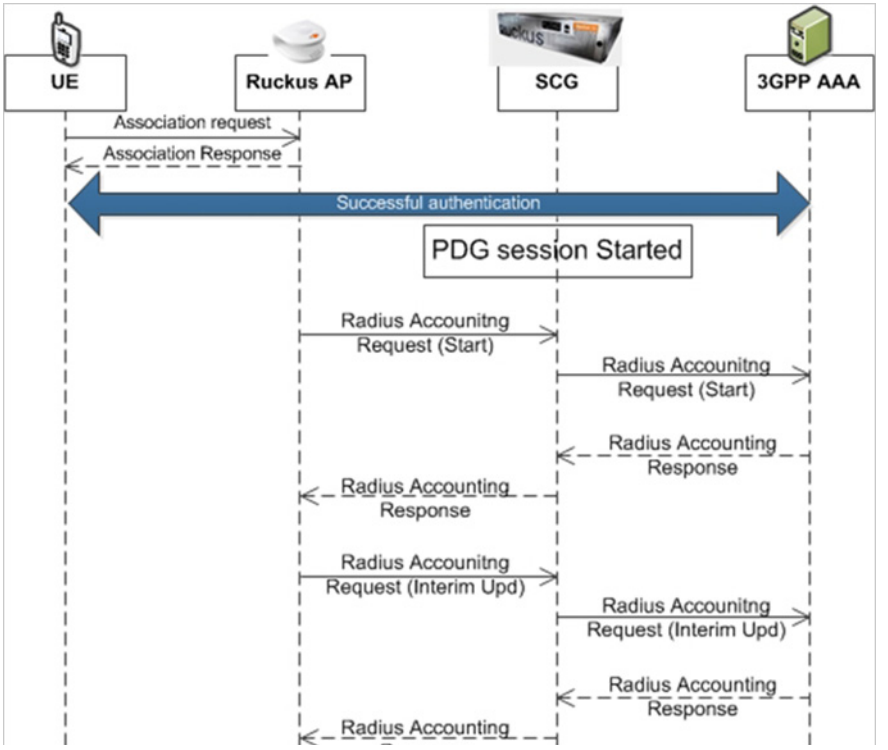
| Attribute | Presence | Type | Description |
|---|---|---|---|
| Response Authenticator | Integer | M | MD5(Code\|ID\|Length\|RequestAuth\|RequestAuth\|RequestAuth\|Attributes\|Secret) |

# 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).

Figure 7 shows the controller proxy accounting messages from NAS to external AAA server.

Figure 7. AP initiated accounting messages




This section covers:

- Accounting Start Messages
- Accounting Interim Update and Stop Messages

- Accounting On Messages
- Accounting Off Messages

## Accounting Start Messages

Table 33 lists the attribute details of messages sent by the controller to the AAA server.

Table 33. Accounting start message attributes

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| User-Name | 1 | M | String | The username of the given accounting session. |
| NAS-IP-Address | 4 | C | Integer | This attribute is the IP address of the AP which is serving the station/UE. |
| 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. |

Table 33. Accounting start message attributes (Continued)

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| 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 | String | This attribute supports two kinds of formats, namely, BSSID:SSID, which is the MAC address of the WLAN on AP and APMAC: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), APMAC (MAC address of AP) and user defined address (maximum length of 62). |

Table 33. Accounting start message attributes (Continued)

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| Proxy-State | 33 | C | Octets | This attribute is available to be sent by a proxy server (controller) to another server (AAA server) when forwarding an access request, accounting request (start, stop or interim) and must be returned unmodified in the access accept, access reject, access challenge and accounting response. |
| Acct-Status-Type | 40 | M | Integer | This attribute indicates whether the *Accounting-Request* attribute marks the beginning of the user service (Start). Start value is 1. |
| Acct-Delay-Time | 41 | C | Integer | This is a configurable option and by default this attribute is disabled. In case the accounting message gets retransmitted, this attribute contains the time stamp of the consecutive retransmitted message. |
| Acct-Session-ID | 44 | M | Integer | This attribute is a unique accounting identity to facilitate easy matching of start, interim and stop records in a log file. The start, interim and stop records for a given session must have the same *Acct-Session-ID.* |
| Acct-Authentic | 45 | M | Integer | This attribute indicates whether the user was authenticated through RADIUS server or NAS or remote authentication protocol. |
| 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. |

Table 33. Accounting start 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 | This attribute is MSISDN or any chargeable user identity returned by the AAA server. This attribute is unchanged when it is received in the RADIUS Access Accept message. |
| Location-Information | 127 | M | 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 | C | Octets | This attribute contains the actual 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. |
| 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: This attribute is included only when the expected location delivery method is accounting request as specified in RFC 5580. |

Table 33. Accounting start message 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>Note: This attribute is included only when the expected location delivery method is accounting request as specified in RFC 5580. |

## Accounting Interim Update and Stop Messages

Table 34 lists the attribute details of messages sent by the controller to AAA.

Table 34. Accounting interim update and stop message attributes

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| User-Name | 1 | M | String | The user name of the given accounting session. |
| NAS-IP-Address | 4 | C | Integer | This attribute is the IP address of the AP which is serving the station/UE. |
| 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. |

Table 34. Accounting interim update and stop message attributes (Continued)

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

Table 34. Accounting interim update and stop message attributes (Continued)

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| 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 | O | String | Allows NAS to send the ID (UE MAC), which indicates as to who is calling this server. |
| NAS-Identifier | 32 | C | Integer | NAS-IP-Address or NAS-Identifier attribute is mandatory in received messages. It supports 3 types of values, namely BSSID (MAC address of the WLAN on AP), 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-Status-Type | 40 | M | Integer | Value differs based on message type. Attribute *interim update* has the value 3 and *stop* has the value 2. |

Table 34. Accounting interim update and stop message attributes (Continued)

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| Acct-Delay-Time | 41 | C | Integer | This is a configurable option and by default this attribute is disabled. In case the accounting message gets retransmitted, this attribute contains the time stamp of the consecutive retransmitted message. |
| Acct-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. |

Table 34. Accounting interim update and stop message attributes (Continued)

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| 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. |
| 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. This attribute is unchanged when it is received in the RADIUS Access Accept message. |

Table 34. Accounting interim update and stop message attributes (Continued)

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| Location-Information | 127 | M | 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 | C | Octets | This attribute contains the actual 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. |
| 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: 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: This attribute is included only when the expected location delivery method is accounting request as specified in RFC 5580. |

## Accounting On Messages

Table 35 lists the attribute details of messages sent by the controller to the AAA server.

Table 35. 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 | Integer | This attribute is the IP address of the AP which is serving the station/UE. |
| 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 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. |

Table 35. Accounting on message attributes (Continued)

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| 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 | 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 |
| 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), 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-Status-Type | 40 | M | Integer | This attribute indicates whether the *Accounting-Request* attribute marks it as *Accounting-On (7)* and *Accounting-Off(8)*. |

Table 35. Accounting on message attributes (Continued)

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| 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

Table 36 lists the attribute details of messages sent by the controller to the AAA server.

Table 36. 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 | Integer | This attribute is the IP address of the AP which is serving the station/UE. |
| 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. |

Table 36. Accounting off message attributes (Continued)

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| 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 | 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. |
| 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), 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-Status-Type | 40 | M | Integer | This attribute indicates whether the *Accounting-Request* attribute marks it as *Accounting-On (7)* and *Accounting-Off(8)*. |

Table 36. Accounting off message attributes (Continued)

| Attribute | Attribute ID | Presence | Type | Description |
|---|---|---|---|---|
| Acct-Delay-Time | 41 | C | Integer | In case the accounting message gets retransmitted, this attribute contains the time stamp of the consecutive retransmitted message. |
| Acct-Authentic | 45 | M | Integer | This attribute indicates whether the user was authenticated through RADIUS server or NAS or Remote authentication protocol. |

# Dynamic Authorization and List of Vendor Specific Attributes

5

In this chapter:

# Dynamic Authorization from 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.

- Calling-Station-Id with MAC
- User name
- CUI with MSISDN

## 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 Wireless or from 3rd Party APs.

This section covers:

- Change of Authorization (CoA) Messages - Not Set to Authorize Only
- Change of Authorization (CoA) Messages - Set to Authorize Only
- Change of Authorization Acknowledge Message (CoA Ack)
- Change of Authorization Negative Acknowledge Messages (CoA NAK)

- Disconnected Messages
- Acknowledgment of Disconnected Messages (DM Ack)
- Negative Acknowledge of Disconnected Messages (DM NAK)
- Disconnected Messages - Dynamic Authorization Client (AAA server)

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

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

Table 37 lists the attribute details of CoA messages where the *Authorize-Only* is not set. CoA can have any of the following attributes as session identifier:

- User name
- CUI with MSISDN

Table 37. Change of Authorization (CoA) messages - Authorize-Only is not set

| Attribute | Attribute ID | Presence | Type/Description |
|---|---|---|---|
| Message Code | | M | 43 |
| User-Name | 1 | C | Identifies the username of the UE/subscriber to be disconnected. Username is received from NAS during authentication or accounting session. |
| NAS-IP-Address | 4 | C | This attribute is the IP address of the AP which is serving the station/UE. |
| VSA 3GPP-GPRS-Negotiated-QoS-Profile | 26 | O | This attribute carries the new QoS value and can be either be Ruckus defined VSA or 3GPP defined VSA.<br>Note: The controller uses 3GPP-GPRS-Negotiated-QoS-Profile for updating the QoS from the AAA server, whichever is present. If both are present priority is for 3GPP-QoS attribute. |
| Called Station ID | 30 | O String | This attribute will contain the Called Station ID as received from NAS during authentication or the accounting procedure. |

Table 37. Change of Authorization (CoA) messages - Authorize-Only is not set (Continued)

| Attribute | Attribute ID | Presence | Type/Description |
|---|---|---|---|
| Calling Station ID | 31 | O String | 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. |
| Chargeable User ID | 89 | C String | This attribute is MSISDN or any chargeable user identity returned by the AAA server. |
| 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 |
| Idle-Timeout | 28 | O | It sets the maximum number of consecutive seconds of idle connection allowed to the user before termination of the session. |
| 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. |

## Change of Authorization (CoA) Messages - Set to Authorize Only

The CoA from AAA Server sends the CoA message with Service-Type(6) set. The controller/Proxy initiates the access request to the AAA server for retrieving the new QoS value. The Service-Type(6) attribute value is set to *Authorize Only* and the state attribute is mandatory.

## Change of Authorization Acknowledge Message (CoA Ack)

Table 38 lists the attributes of CoA messages being acknowledged by controller to DAC.

Table 38. 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)

Table 39 lists the attributes of CoA messages that are not acknowledged by the controller to the DAC.

Table 39. 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. |

Table 39. Change of Authorization (CoA) messages - Negative Acknowledge (Continued)

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

## Disconnected Messages

Table 40 lists the attributes of disconnected messages, which are initiated by controller.

Table 40. Disconnected messages

| Attribute | Attribute ID | Presence | Type/Description |
|---|---|---|---|
| Message Code | | M | 40 |
| User-Name | 1 | M | Identifies the username of the UE/subscriber to be disconnected. Username 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. |
| Calling Station ID | 31 | C String | 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), APMAC (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. |
| Message Authenticator | 80 | O Octets | This attribute is used to sign a*ccess 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). |

Table 40. Disconnected messages (Continued)

| Attribute | Attribute ID | Presence | Type/Description |
|---|---|---|---|
| Chargeable User ID | 89 | C String | This attribute is MSISDN or any chargeable user identity returned by the AAA server. |

## Acknowledgment of Disconnected Messages (DM Ack)

Table 41 lists the attributes of disconnected messages, which are acknowledged.

Table 41. Acknowledgment of disconnected 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 Disconnected Messages (DM NAK)

Table 42 lists the attributes of disconnected messages, which are not acknowledged.

Table 42. Negative acknowledgment of disconnected messages

| Attribute | Attribute ID | Presence | Type/Description |
|---|---|---|---|
| Message Code | | M | 42 |
| 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*. |

## Disconnected 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

and the user session(s) to be terminated by including the identification attributes. Disconnected messages can have any of the following attributes as a session identifier.

- User name
- CUI with MSISDN.

Table 43 lists the attribute details of the disconnected messages, which are initiated by the dynamic authorization client of the AAA server.

Table 43. 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 disconnected. Username 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/UE. |
| Calling Station ID | 31 | O String | 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. |
| Proxy-State | 33 | O Octets | 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 includes:

- WISPr Vendor Specific Attributes
- Ruckus Wireless Vendor Specific Attributes

## WISPr Vendor Specific Attributes

Table 44 lists the WISPr vendor specific attributes. The VSA ID for the following VSAs is 14122 and the type is 26.

Table 44. 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-Logoff-URL | 3 | Access-Accept | This attribute indicates the WISPr service logout URL. |
| WISPr-Redirection-URL | 4 | Access-Accept | RADIUS server uses this attribute to indicate the location where the URL needs to be redirected. |
| WISPr-Bandwidth-Min-UP | 5 | Access-Accept | This attributes specifies the minimum guaranteed rate at which the bandwidth should be reserved for the user to upstream data. |
| WISPr-Bandwidth-Min-DOWN | 6 | Access-Accept | This attribute specifies the minimum guaranteed rate at which the bandwidth should be reserved for the user to downstream data. |
| WISPr-Bandwidth-Max-UP | 7 | Access-Accept | This attribute specifies the maximum rate at which the corresponding user is allowed to transmit for upstream data. |
| WISPr-Bandwidth-Max-DOWN | 8 | Access-Accept | This attribute specifies the maximum rate at which the corresponding user is allowed to transmit for downstream data. |

## Ruckus Wireless Vendor Specific Attributes

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

- Vendor type
- Vendor length
- Value fields

Figure 8 shows the VSA fields.

Figure 8. VSA fields

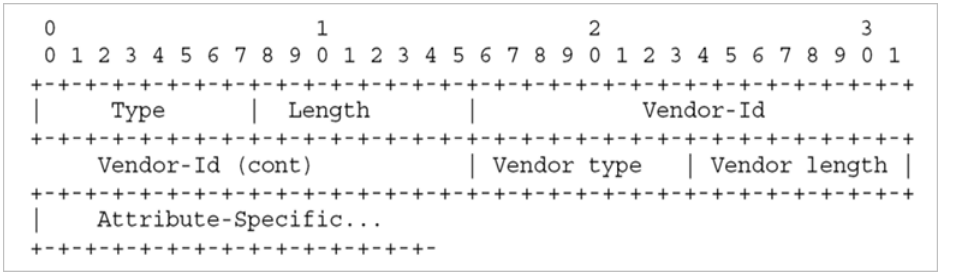



Table 45 lists the Ruckus Wireless vendor specific attributes. The VSA ID for all the following VSAs is 25053 and type is 26.

Table 45. Ruckus Wireless vendor specific attributes - 25053

| Attribute Name | Vendor Type | RADIUS Message Type | Purpose |
|---|---|---|---|
| Ruckus-User-Groups | 1 | Access-Accept | RADIUS server uses this attribute to indicate the access point group, specifying the UE group. |
| Ruckus-STA-RSSI | 2 | Accounting - Interim - Stop | This attribute reports the UEs current RSSI value in the accounting packet. |
| 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 Ruckus AP.<br>Note: It is optional for 3rd party APs. |

Table 45. Ruckus Wireless vendor specific attributes - 25053 (Continued)

| Attribute Name | Vendor Type | RADIUS Message Type | Purpose |
|---|---|---|---|
| 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 Ruckus 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. |
| 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. Refer to Figure 8. |
| 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-Sta-Inner-Id | 13 | | This attribute indicates the user name from the RADIUS server, when the user exists. |
| Ruckus-BSSID | 14 | | BSSID for each WLAN in each radio |

Table 45. Ruckus Wireless vendor specific attributes - 25053 (Continued)

| Attribute Name | Vendor Type | RADIUS Message Type | Purpose |
|---|---|---|---|
| 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 Figure 8. |
| 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 Figure 8. |
| Ruckus-QoS | 105 | | 3GPP-QoS is now used instead of this VSA. However, this VSA is supported in 2.1.x releases. |
| Ruckus-NAS-Type | 109 | Accounting - Start | The value for this parameter is always 1.<br>Refer to encoding as explained in Figure 8. |
| 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 encoding as explained in Figure 8. |

Table 45. Ruckus Wireless vendor specific attributes - 25053 (Continued)

| Attribute Name | Vendor Type | RADIUS Message Type | Purpose |
|---|---|---|---|
| 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 45. Ruckus Wireless 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. |

# AP Roaming Scenarios

# A

In this appendix:

The following are the AP roaming scenarios.

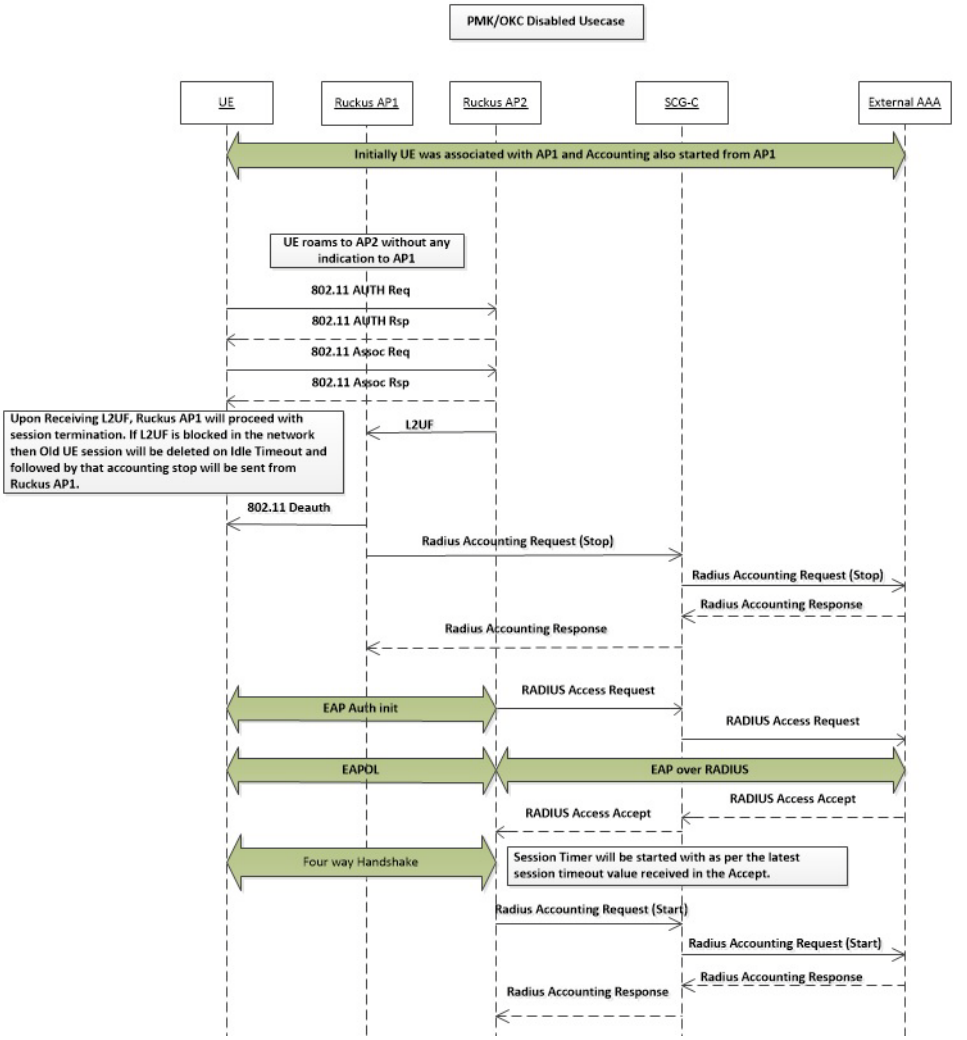
**NOTE:** The session timeout values received from the AAA server are used for maintaining the PMK/OKC cache timer values at the controller and AP. If the timer value received is less than the default value of 12 hours, it will be used. Otherwise the default value will be used as the maximum value.

# Roaming from AP1 to AP2 - PMK/OKC Disabled

In this scenario as seen in Figure 9, 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.

This call flow is applicable when L2UF is blocked in the customer network.

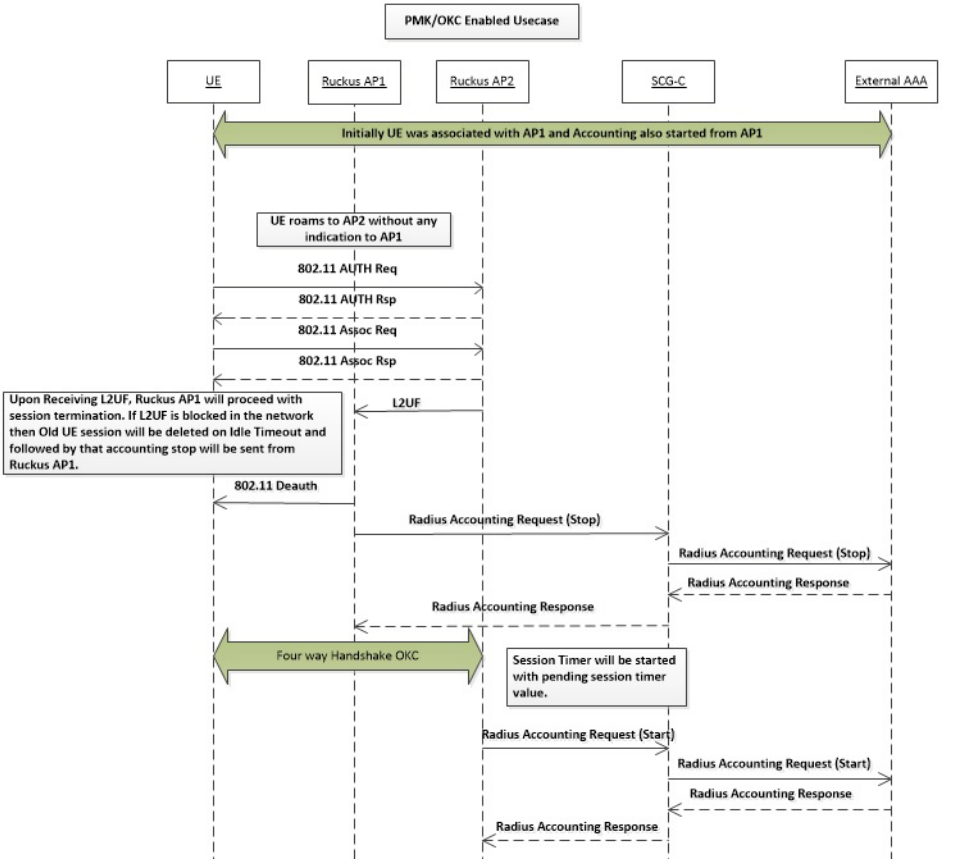
Figure 9. UE Roaming from AP1 to AP2 - PMK/OKC disabled



# Roaming from AP1 to AP2 - PMK/OKC Enabled

In this scenario as seen in Figure 10, 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

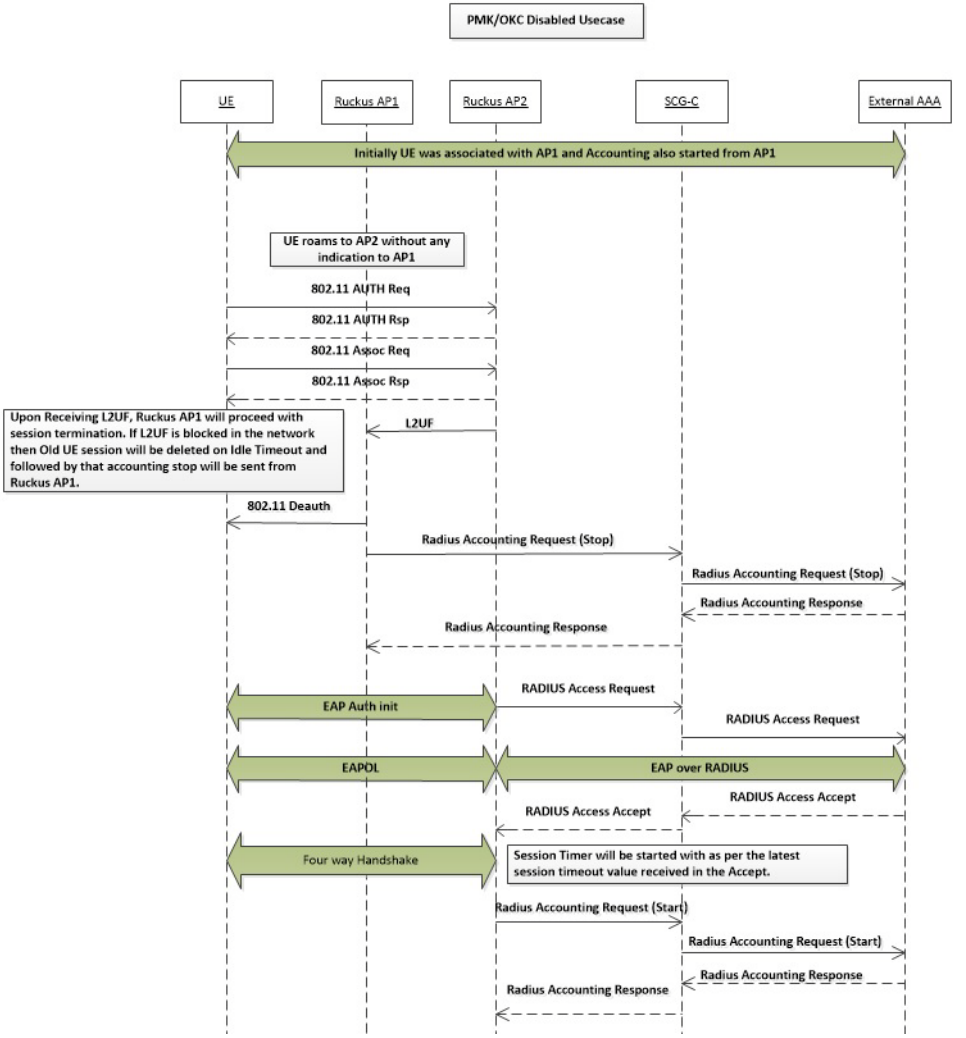



This call flow is applicable when L2UF is blocked in the customer network.

# Roams Back to the Same AP - PMK/OKC Disabled

In this scenario as seen in Figure 11, the UE (subscriber) moves out of range/ coverage of the first AP but joins back the same AP. Authentication and accounting messages are initiated from AP and the PMK/OKC cache is disabled.

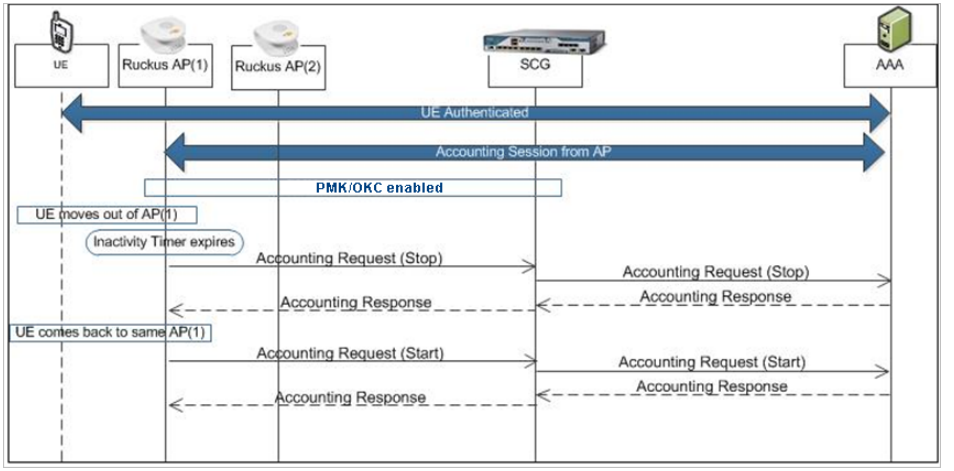
Figure 11. UE Roams Back to the Same AP- PMK/OKC disabled



# Roams Back to the Same AP - PMK/OKC Enabled

In this scenario as seen in Figure 12, the UE (subscriber) moves out of range/ coverage of the first AP but joins back the same AP. Authentication and accounting messages are initiated from AP and the PMK/OKC cache is enabled.

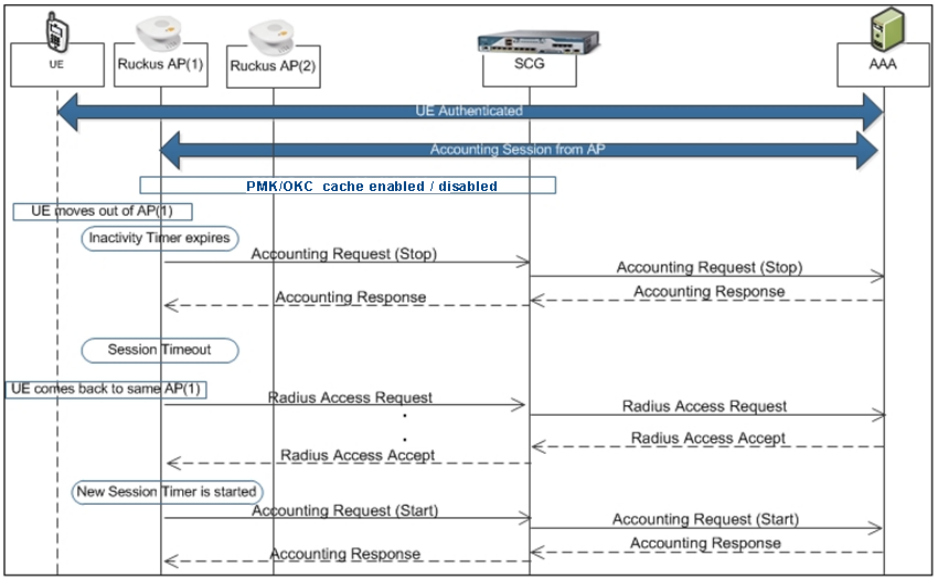
Figure 12. UE Roams Back to the Same AP- PMK/OKC enabled



# Same AP After Session Timeout

In this scenario as seen in Figure 13, the UE (subscriber) moves out of range/ coverage of the first AP but joins back the same AP, which is longer than the session timeout allocated. Authentication and accounting messages are initiated from the AP. This scenario is similar to the PMK/OKC cache enabled/disabled behavior.

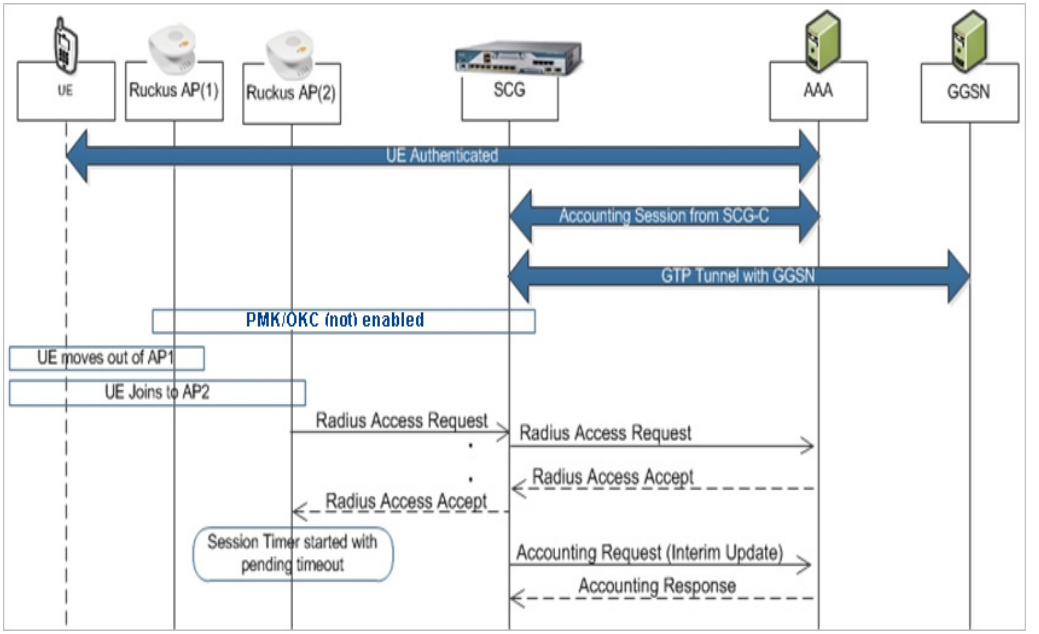
Figure 13. UE Roams Back to the Same AP After Session Timeout



# AP1 to AP2 Connected to the Same Controller Node

In this scenario as seen in Figure 14, the UE (subscriber) roams from AP1 to AP2 with both the APs connected to the same controller node. 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.

Figure 14. UE Roams from AP1 to AP2 Connected to the Same controller Node



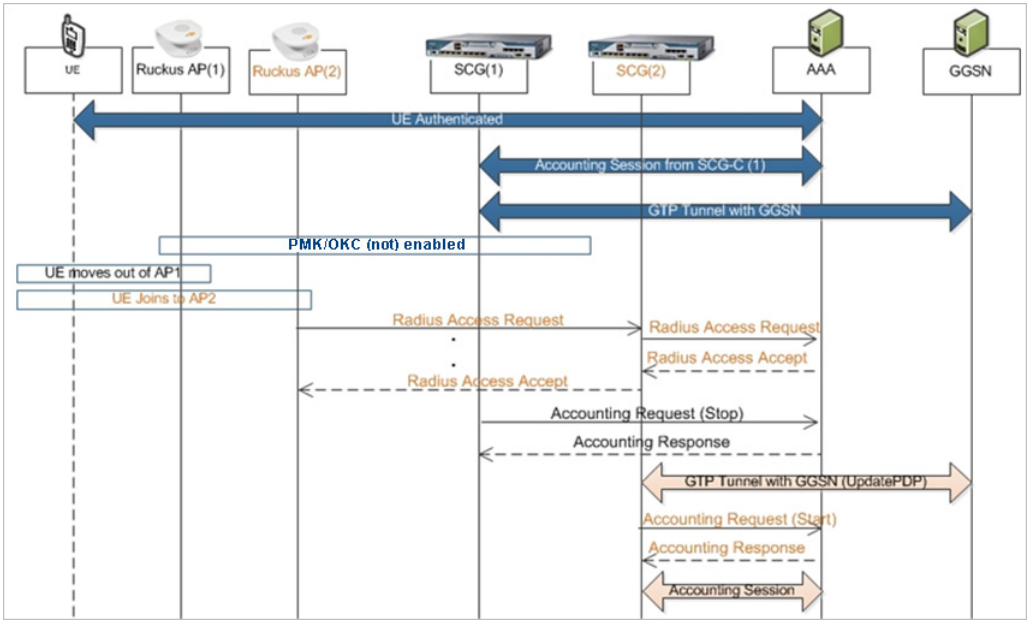

**NOTE:** Authentication procedures are not performed in scenarios where the UE moves from AP1 to AP2 and PMK/OKC is enabled.

**NOTE:** The update procedure towards GGSN/PGW is initiated in scenarios where the UE roams from AP1 to AP2 and the data plane changes.

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

In this scenario as seen in Figure 15, 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 15. UE Roams from AP1 to AP2 Connected to Different controller Node



# Index

## Numerics



## A



## B



## C



## D



## E

## S



## T



## U



## V



## W