Ruckus Tech Note

Working with

RADIUS Attributes & Accounting

ZONEDIRECTOR AND AP

Table of Contents

Copyright Notice and Proprietary Information

Intended Audience

This document addresses configuration and use of RADIUS accounting with Ruckus ZoneFlex products. The goal of this document is a successful implementation of this feature with Ruckus Wireless equipment.

This document provides step-by-step procedures for configuration and testing. Some knowledge of RADIUS, Wi-Fi design, 802.11 and 802.1X principles is recommended.

Overview

This document describes how to configure and test RADIUS accounting functionality with Ruckus Wireless products. The document is broken into the following main categories:

- Introduction and key concepts
- Accounting actions and behavior

What Is Covered Here

The usage cases in this document focus on configuring RADIUS attributes in a lab environment. This tech note describes the basic process as well as information that can be used to configure RADIUS in a lab environment.

Requirements for this Document

In order to successfully follow the steps in this document, the following equipment (at a minimum) is required and assumed:

- RADIUS server (installed)
- Ruckus ZoneDirector and AP
- Wireless client device

Introduction & Key Concepts

What is RADIUS?

The Remote Authentication Dial In User Service (RADIUS) is a networking protocol for authentication, authorization and accounting (AAA) services. A RADIUS server can provide a central database and/or proxy to other servers for client authentication. Many authentication methods use the RADIUS protocol for the underlying transactions, e.g. MAC authentication, 802.1X, web logins, etc.

Information such as the user name, password, etc. is included in the RADIUS messages as attribute value pairs (AVPs). An AVP consists of an attribute name (User-Password) and its value "Steve".

Packet Structure

A RADIUS packet (shown below) consists of a code that indicates the message type, packet identifier to match sessions, length, authenticator and AVPs.
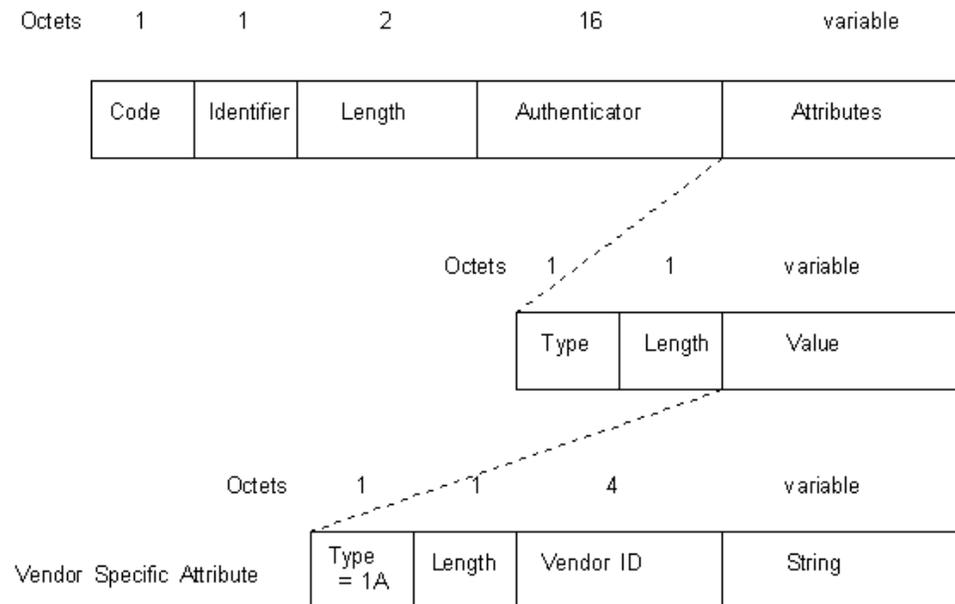
Figure 1 - RADIUS Packet Structure

- The Identifier field aids in matching requests and replies.
- The Length field indicates the length of the entire RADIUS packet including the Code, Identifier, Length, Authenticator and optional Attribute fields.

- The Authenticator is used to authenticate the reply from the RADIUS server, and is used in encrypting passwords; its length is 16 bytes.

Code	Assignment
1	Access-Request
2	Access-Accept
3	Access-Reject
4	Accounting-Request
5	Account-Response
11	Access-Challenge
12	Status-Server (experimental)
13	Status-Client (experimental)
255	Reserved

Authentication and Authorization

For these types of transactions, a device or user sends a network access request, which is sent to a Network Access Server (NAS). The NAS (e.g. a ZoneDirector) sends the client request to the RADIUS server as part of a special message called Access-Request. This request includes the user credentials as well as other information the NAS may know about the user such as 802.11 radio type, AP, etc.

The RADIUS server verifies the information and returns one of three responses: Access-Accept, Access-Reject or Access-Challenge.

RADIUS Client   **RADIUS Server**

Access-Request →

← *Access-Accept*

OR

← *Access-Challenge*

OR

← *Access-Reject*
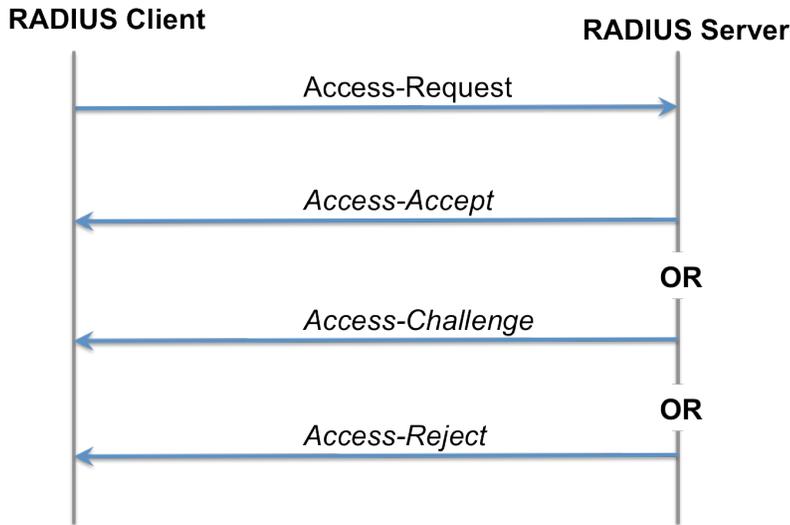
Figure 2 - RADIUS Authentication Flow

An Access-Accept response indicates the authentication was successful and the user is granted access. This response may be dependent on successful authorization steps taken by the RADIUS server as well. For example, a user might have permission to sign into the wired network but no the wireless network. Therefore, the same credentials will work from a wired machine and fail from a wireless device.

An Access-Challenge requests additional information such as a PIN, token or other secondary information and is an intermediate step.

If the server returns an Access-Reject the user has been denied access, this may be because the credentials were incorrect or the user did not have authorization for the requested resource.

Accounting

If configured, RADIUS servers can track information about users and devices. This is most often used for billing purposes in ISP hotspots or similar scenarios.

When network access is granted to a user, an Accounting-Request message is sent from the NAS to the RADIUS server. The Acct-Status-Type attribute in this message contains the value "start". An accounting start tells the server the user session has begun and can contain information such as network address, VLAN, SSID, etc. as well as a unique session identifier. In the case of multiple sessions for the same user, a unique multi-session ID is created to track two or more sessions.

Active user sessions will trigger periodic interim updates from the NAS to the RADIUS server. This takes the form of an Accounting-Request with Acct-Status-Type set to "interim-update". This is used to update the RADIUS server with information about a session such as data usage.

When the client leaves the network, the NAS sends a final Accounting-Request message with the status set to "stop" to the RADIUS server. This closes the session and updates the server on final session statistics such as total data transmitted, data received, reason for disconnect, etc.
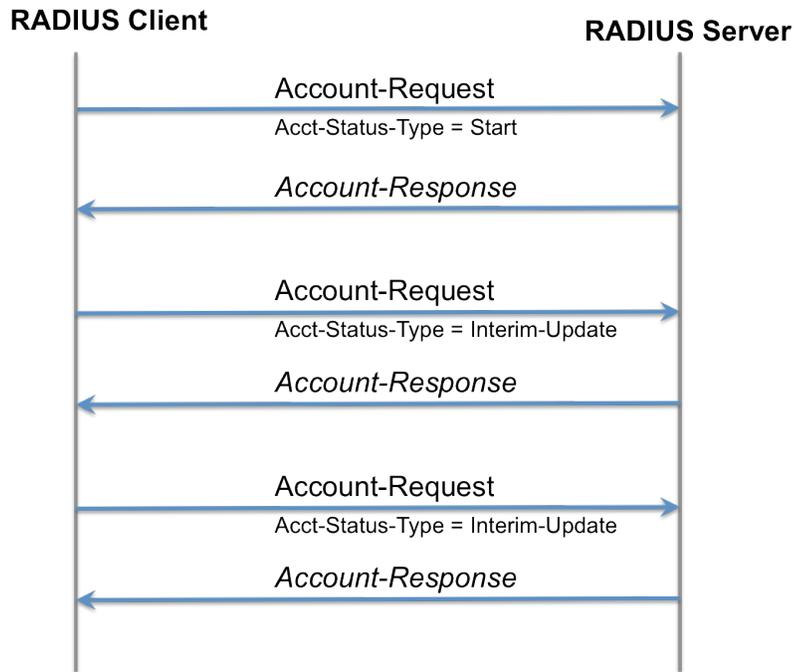
Figure 3 - RADIUS Accounting Flow

For more information on RADIUS, please see Appendix A: Further Reading.

RADIUS Attributes

RADIUS Attribute Value Pairs (AVPs) consist of a fixed attribute name and the value. AVPs are included in both authentication and accounting messages. Attributes are often used during authentication transactions for dynamic behavior such as dynamic VLAN assignment or group membership for role assignment.

The rest of this document will refer to AVPs by their attribute name and, optionally, a type number. For more information on specific AVPs, please refer to Appendix B: Attribute Value Pairs.

ZoneDirectors and APs as RADIUS Clients (NAS)

Ruckus products communicate with an external RADIUS server as a RADIUS client – also called a Network Access Server (NAS). Communications from Ruckus products are either Access-Request or Accounting-Requests. The RADIUS server can send Access-Challenge, Access-Accept, or Access-Reject in response to an Access-Request, and an accounting response to an Accounting-Request.

All RADIUS servers support both basic attributes and extended, vendor-specific attributes. Attributes are defined as part of a dictionary included on the server. Some of these are very generic and others are typically only used for specific usage scenarios.

Ruckus supports the following attribute sets and usage scenario:

- Basic RADIUS attributes (common dictionary)
- Dynamic VLAN assignment
- 802.1X authentication
- WISPr
- Ruckus-specific attributes

All attributes are supported equally on any ZoneDirector or AP unless otherwise noted.

RADIUS Dictionaries

A dictionary is a list of specific attributes available for use in RADIUS transactions and possible values. RADIUS servers include a basic RADIUS dictionary and, optionally, additional dictionaries that may be imported for extended functionality. A complete list of common RADIUS attributes is specified in RFC 2866.

Most vendors also publish their own RADIUS dictionaries. These dictionaries define attributes commonly known as Vendor Specific Attributes (VSAs). Ruckus has a dictionary available from the support site.

For information on Ruckus-supported attributes, please see Appendix B: Attribute Value Pairs.

Ruckus Dictionary

This dictionary is available for use with a RADIUS server. It is available from the Ruckus support site or from Appendix C: Ruckus RADIUS Dictionary.

Accounting Actions

Overview

RADIUS accounting interactions involve specific actions and responses between the Ruckus NAS and the RADIUS accounting server. This information can be used to track network and client behavior. This chapter discusses when accounting actions occur.

Accounting Requests

Accounting-Request packets are sent from a NAS client to a RADIUS accounting server. The message is used to convey information about the network or client. Any attribute valid in a RADIUS Access-Request or Access-Accept packet is valid in a RADIUS Accounting-Request packet with the exception of User-Password, CHAP-Password, Reply-Message and State.

The following events trigger an Accounting-Request by the ZoneDirector or the AP:

- Accounting-On when an AP joins
- Accounting-Off when an AP leaves or restarts
- Accounting-Start when a client associates
- Accounting-Stop when a client disassociates
- Associated clients will trigger an Interim-Update during the duration of their session

Accounting-On Example (AP join)

In this example, the AP with the MAC of 50-A7-33-5B-9F-28 has just powered up and joined. Note the WLAN name that it is broadcasting (8021X-Network) is included.

```
rad_recv: Accounting-Request packet from host 172.16.112.49 port
39569, id=0, length=98
      Acct-Status-Type = Accounting-On
      Acct-Authentic = RADIUS
      NAS-IP-Address = 172.16.112.49
      NAS-Identifier = "50-A7-33-5B-9F-28"
      Acct-Session-Id = "51ABB3A9-00000000"
      Ruckus-SSID = "802.1X-Network"
```

Accounting-Off Example (AP leaves)

In this example, the AP with the MAC of 50-A7-33-5B-9F-28 has restarted or powered down. The accounting message always includes the SSID of the WLAN.

```
rad_recv: Accounting-Request packet from host 172.16.112.49 port
39569, id=1, length=98
      Acct-Status-Type = Accounting-Off
      Acct-Authentic = RADIUS
```

```
        NAS-IP-Address = 172.16.112.49
        NAS-Identifier = "50-A7-33-5B-9F-28"
        Acct-Session-Id = "51ABB3A9-00000001"
        Ruckus-SSID = "802.1X-Network"
```

Accounting-Start Example (Client association)

In this example, the station with the MAC address 4C-B1-99-35-5F-D7 associates to the WLAN 8021X-Network from the AP (50-A7-33-5B-9F-2C). The user "steve" then authenticates. Note the connection information (802.11an band) is included.

```
rad_recv: Access-Request packet from host 172.16.112.49 port 49111,
id=25, length=214
        User-Name = "steve"
        Calling-Station-Id = "4C-B1-99-35-5F-D7"
        NAS-IP-Address = 172.16.112.49
        NAS-Port = 5
        Called-Station-Id = "C0-8A-DE-27-F9-DC:802.1X-Network"
        Service-Type = Framed-User
        Framed-MTU = 1400
        NAS-Port-Type = Wireless-802.11
        NAS-Identifier = "C0-8A-DE-27-F9-DC"
        Connect-Info = "CONNECT 802.11a/n"
        EAP-Message = 0x020500061500
        State = 0xbc22a2e3b827b73c018c7aa4dab5158c
        Ruckus-SSID = "802.1X-Network"
        Message-Authenticator = 0x1e66b5d0b1fbac85bcac86a262aa4028
```

Accounting Interim-Update Example (Status Update)

In this example, an interim-update is sent for an active session on the AP (50-A7-33-5B-9F-2C) of the station with the MAC address 4C-B1-99-35-5F-D7 and user "steve" and on the WLAN 8021X-Network. An interim-update provides information about ongoing sessions and is sent every X minutes where X is the interval defined in the WLAN configuration.

```
rad_recv: Accounting-Request packet from host 172.16.112.49 port
44274, id=7, length=281
        User-Name = "steve"
        Acct-Status-Type = Interim-Update
        Acct-Authentic = RADIUS
        Framed-IP-Address = 172.16.112.140
        Calling-Station-Id = "4C-B1-99-35-5F-D7"
        NAS-IP-Address = 172.16.112.49
        NAS-Port = 5
        Called-Station-Id = "50-A7-33-5B-9F-2C:802.1X-Network"
        NAS-Port-Type = Wireless-802.11
        NAS-Identifier = "50-A7-33-5B-9F-2C"
        Connect-Info = "CONNECT 802.11a/n"
        Acct-Session-Id = "51ABB3A9-00000005"
```

```
        Acct-Multi-Session-Id =
"50a7335b9f2c4cb199355fd7518d311f0006"
        Ruckus-SSID = "802.1X-Network"
        Acct-Session-Time = 60
        Acct-Input-Octets = 20716
        Acct-Output-Octets = 5921
        Acct-Input-Packets = 163
        Acct-Output-Packets = 46
        Ruckus-Sta-RSSI = 52
        Event-Timestamp = "May 10 2013 10:41:48 PDT"
```

Accounting-Stop Example (Client dissociates)

In this example, the station associated to the AP (50-A7-33-5B-9F-2C) with the station MAC address 4C-B1-99-35-5F-D7 and user "steve" disassociates from the "8021X-Network" WLAN. Note the total session information is recorded as well as the terminate cause. A session is stopped (terminated) based on any of the following actions:

1. User explicitly logs off via logout link
2. Client exceeds maximum session time
3. Client has been inactive longer than the maximum idle time
4. Client moves out of range of the WLAN

```
rad_recv: Accounting-Request packet from host 172.16.112.49 port
46298, id=15, length=287
        User-Name = "steve"
        Acct-Status-Type = Stop
        Acct-Authentic = RADIUS
        Framed-IP-Address = 172.16.112.140
        Calling-Station-Id = "4C-B1-99-35-5F-D7"
        NAS-IP-Address = 172.16.112.49
        NAS-Port = 2
        Called-Station-Id = "50-A7-33-5B-9F-2C:802.1X-Network"
        NAS-Port-Type = Wireless-802.11
        NAS-Identifier = "50-A7-33-5B-9F-2C"
        Connect-Info = "CONNECT 802.11a/n"
        Acct-Session-Id = "51ABB3A9-00000002"
        Acct-Multi-Session-Id =
"50a7335b9f2c4cb199355fd7518d30a00003"
        Ruckus-SSID = "802.1X-Network"
        Acct-Session-Time = 70
        Acct-Input-Octets = 70346
        Acct-Output-Octets = 7016
        Acct-Input-Packets = 572
        Acct-Output-Packets = 62
        Ruckus-Sta-RSSI = 44
        Event-Timestamp = "May 10 2013 10:39:51 PDT"
        Acct-Terminate-Cause = Lost-Carrier
```

802.1X Attributes & Accounting

Overview

802.1X is a common authentication method that involves a NAS client (ZoneDirector or AP) passing client communications to the RADIUS server.

ZoneDirector

Ruckus ZoneDirectors support the following attributes for 802.1X authentication and accounting:

Authentication Attributes

Attribute	Description
User-Name	The login name of the user to be authenticated.
Calling Station-Id	Allows the NAS to send client details in the Access-Request. A ZoneDirector will use the MAC address of the client. It is only used in Access-Request packets.
NAS-IP-Address	The IP Address of the ZoneDirector, which is requesting authentication of the user. NAS-IP-Address is only used in Access-Request packets.
NAS-Port	Indicates the physical port number of the NAS. It is only used in Access-Request packets.
Called-Station-Id	Allows the NAS to send information about the device the client is attempting to use. A ZoneDirector will use this to send the AP MAC and the SSID. It is only used in Access-Request packets.
Service-Type	Indicates the type of service the user has requested, or the type of service to be provided. It MAY be used in both Access-Request and Access-Accept packets. The ZoneDirector will typically use "Framed-User" as the value.
Framed-MTU	The Maximum Transmission Unit (MTU) to be configured for the user, when it is not negotiated by some other means. It may be used in Access-Accept and Access-Request packet as a hint by the NAS to the server that it would prefer that value, but the server is not required to honor the hint. The default value used by a ZoneDirector is 1400 bytes.
NAS-Port-Type	Indicates the type of physical port on the NAS. It can be used instead of or in addition to the NAS-Port (5) attribute. It is only used in Access-Request packets. The default value used by the ZoneDirector is "Wireless-802.11".
NAS-Identifier	A string identifying the NAS originating the Access-Request. It is only used in Access-Request packets. The default value sent by the ZoneDirector is the AP MAC or the BSSID of the WLAN a user is attempting to access.

Connect-Info	Indicates the type of user connection. The NAS may send this attribute in an Access-Request or Accounting-Request. The default value used by the ZoneDirector indicates the radio capability, e.g. "CONNECT 802.11a/n".
EAP-Message	This attribute encapsulates Extended Access Protocol [3] messages from the client so the NAS can authenticate them without understanding the particular EAP protocol. The NAS places any EAP messages received from the user into one or more EAP attributes and forwards them to the RADIUS Server as part of the Access-Request, which can return EAP messages in Access-Challenge, Access-Accept and Access-Reject packets. The client rather than the ZoneDirector generates these values.
State	Indicates the state of the EAP transaction. This value is included by the ZoneDirector but is not generated by it.
Acct-Session-ID	A unique accounting ID used to match start and stop records. This ID is also used in the accounting records.

Accounting Attributes (All Messages)

Attribute	Description
User-Name	The login name of the user to be authenticated.
Acct-Status-Type	Indicates whether this Accounting-Request marks the beginning of the user session (Start) or the end (Stop).
Acct-Authentic	Indicates how the user was authenticated, whether by RADIUS, the NAS itself, or another remote authentication protocol. Default value used by the ZoneDirector is "RADIUS".
Framed-IP-Address	The IP address of the user for this session.
Calling Station-Id	Allows the NAS to send client details in the Access-Request. A ZoneDirector will use the MAC address of the client. It is only used in Access-Request packets.
NAS-IP-Address	The IP Address of the ZoneDirector, which is requesting authentication of the user. NAS-IP-Address is only used in Access-Request packets.
NAS-Port	Indicates the physical port number of the NAS. It is only used in Access-Request packets.
Called-Station-Id	Allows the NAS to send information about the device the client is attempting to use. A ZoneDirector will use this to send the AP MAC and the SSID. It is only used in Access-Request packets.
NAS-Port-Type	Indicates the type of physical port on the NAS. It can be used instead of or in addition to the NAS-Port (5) attribute. It is only used in Access-Request packets. The default value used by the ZoneDirector is

|	
	"Wireless-802.11".
NAS-Identifier	A string identifying the NAS originating the Access-Request. It is only used in Access-Request packets. The default value sent by the ZoneDirector is the AP MAC or the BSSID of the WLAN a user is attempting to access.
Connect-Info	Indicates the type of user connection. The NAS may send this attribute in an Access-Request or Accounting-Request. The default value used by the ZoneDirector indicates the radio capability, e.g. "CONNECT 802.11a/n".
Acct-Session-Id	A unique accounting ID used to match start and stop records. This ID is also used in the accounting records.
Acct-Multi-Session-Id	A unique accounting ID used to match multiple related sessions. Each session will have a unique Acct-Session-Id and the same Acct-Multi-Session-Id.

Accounting Attributes (Specific to Interim-Update and Stop)

Attribute	Description
Acct-Session-Time	This attribute indicates how many seconds the user has received service for, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop.
Acct-Input-Octets	This attribute indicates how many octets have been received from the port over the course of this service being provided, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop.
Acct-Output-Octets	This attribute indicates how many octets have been sent to the port in the course of delivering this service, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop.
Acct-Input-Packets	This attribute indicates how many packets have been received from the port over the course of this service being provided to a Framed User, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop.
Acct-Output-Packets	This attribute indicates how many packets have been sent to the port in the course of delivering this service to a Framed User, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop.
Acct-Input-Gigawords	This attribute indicates how many times the Acct-Input-Octets counter has wrapped around 2^{32} over the course of this service being provided, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop or Interim-Update. NOTE: This value is only present when the Acct-Input-Octets value is greater than 1 Gigabyte.

Acct-Output-Gigawords	This attribute indicates how many times the Acct-Output-Octets counter has wrapped around 2^32 in the course of delivering this service, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop or Interim-Update. NOTE: This value is only present when the Acct-Input-Octets value is greater than 1 Gigabyte.
Acct-Event-Timestamp	This attribute is included in an Accounting-Request packet to record the time that this event occurred on the NAS, in seconds since January 1, 1970 00:00 UTC.

Accounting Attributes (Specific to stop only)

Attribute	Description
Acct-Terminate-Cause	This attribute indicates how the session was terminated, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop. Values are: user request, lost carrier, lost service, idle timeout, session timeout and admin reset.

RADIUS Server Directives

The ZoneDirector can use the following information as returned by the RADIUS server.

Access-Accept Message

Attribute	Description
Acct-Interim-Interval	Contains the number of seconds between each interim update to be sent from the NAS for this session. NOTE: Ignored if local policy on interim interval already exists (from ZoneDirector).
Session-Timeout	Sets the maximum number of seconds of service to be provided to the user before termination of the session or prompt. This attribute is available to be sent by the server to the client in an Access-Accept or Access-Challenge.

WISPr Attributes

Overview

Hotspots often make use of WISPr-specific RADIUS attributes to track operations. These can be used to generate billing information, limit bandwidth usage, disconnect clients, etc. All of these functions require additional information to be sent in the RADIUS messages between the ZoneDirector/AP and the RADIUS server.

The following events trigger accounting requests:

- Accounting-On when an AP joins
- Accounting-Off when an AP leaves or restarts
- Accounting-Start when a client associates
- Accounting-Stop when a client disassociates
- Associated clients will trigger an Interim-Update during the duration of their session

ZoneDirector

In addition to previously mentioned RADIUS attributes, Ruckus ZoneDirectors also support the following WISPr-specific attributes .

Authentication-specific Attributes

Attribute	Description
Framed-IP-Address	HTTP port of the ZoneDirector (9997 or 9998) as a UAM.
Location-Name	WISPr location name (optional) as configured in the ZoneDirector hotspot service.
Location-Id	WISPr location ID (optional) as configured in the ZoneDirector hotspot service.
WISPr-Redirection-URL	URL requested for redirection of client
Vendor-Specific	Indicates the used of an extended set of attributes supported by a specific vendor.
Vendor ID	Identifies the vendor that uses these attributes. The Ruckus ID is 14122.

Unless specifically called out, all previously mentioned attributes are also supported. For a complete list, please refer to Appendix B: Attribute Value Pairs.

Accounting-specific Attributes

Attribute	Description
Framed-IP-Address	HTTP port of the ZoneDirector (9997 or 9998) as a UAM.
Location-Name	WISPr location name (optional) as configured in the ZoneDirector hotspot service.
Location-ID	WISPr location ID as configured in the ZoneDirector hotspot service.

Standalone AP

In addition to previously mentioned RADIUS attributes, Ruckus standalone APs also support the following WISPr-specific attributes.

Authentication-specific Attributes

Attribute	Description
Framed-IP-Address	HTTP port of the AP (3990 or 3992) as a UAM.
WISPr-Location-Name	WISPr location name
WISPr-Location-ID	WISPr location ID
WISPr-Redirection-URL	URL requested for redirection of client

Accounting-specific Attributes

Attribute	Description
NAS-IP-Address	IP address of the AP-defined UAM server – this might *not* be the same address the RADIUS server sees the AP communicating with it
Framed-IP-Address	HTTP port of the AP (3990)

Unless specifically called out, all previously mentioned attributes are also supported. For a complete list, please refer to Appendix B: Attribute Value Pairs.

Ruckus RADIUS Attributes

Overview

Ruckus-specific information may be sent as part of the Access-Accept packet from the RADIUS server. All of these functions require additional information be sent in the RADIUS messages between the ZoneDirector/AP and the RADIUS server. The basic AVP definitions are included in the Ruckus RADIUS dictionary and must be included on the RADIUS server.

ZoneDirector

Ruckus ZoneDirectors support the following Ruckus-specific RADIUS attributes.

Authentication-specific Attributes

Attribute	Description
Ruckus-User-Groups	User role assignment – the role must already exist on the ZoneDirector – sent in the Access-Accept by the RADIUS server
Ruckus-Grace-Period	Specifies a grace period before re-authentication is required (WISPr or captive portal only). Range is 1 to 14400 minutes. Sent in the Access-Accept by the RADIUS server
Ruckus-SSID	Station WLAN name, sent from ZoneDirector to the RADIUS server as part of the Access-Request (information only)

Accounting-specific Attributes

Attribute	Description
Ruckus-Sta-RSSI	Station RSSI sent from ZoneDirector to the RADIUS server (Interim-Update, Stop)
Ruckus-SSID	Station WLAN name, sent from ZoneDirector to the RADIUS server (Start, Interim-Update and Stop)

SCG

Ruckus SCG controllers support the following Ruckus-specific RADIUS attributes.

Authentication-specific Attributes

Attribute	Description
Ruckus-WlanID	WLAN ID number sent from SCG to the RADIUS server as part of the Access-Request message to identify the WLAN interface
Ruckus-SCG-CBlade-IP	IP address of the C blade used by the SCG for this request
Ruckus-SCG-DBlade-IP	IP address of the D blade used by the SCG for this request
Ruckus-Session-Type	Sent by the RADIUS server to the SCG to indicate the forwarding policy to be used for the UE
Ruckus-Acct-Status	Sent by the RADIUS server to the SCG to indicate if the authenticator should send an accounting packet for this UE
Ruckus-SSID	Station WLAN name, sent from SCG to the RADIUS server as part of the Access-Request (information only)

Accounting-specific Attributes

Attribute	Description
Ruckus-Sta-RSSI	Station RSSI sent from SCG to the RADIUS server (Interim-Update, Stop)
Ruckus-SSID	Station WLAN name, sent from SCG to the RADIUS server (Start, Interim-Update and Stop)

Appendix A: Further Reading

FreeRADIUS

FreeRADIUS Beginner's Guide – by Dirk van der Walt (ISBN-10: 1849514089)

Getting Started with FreeRADIUS

http://www.packtpub.com/article/getting-started-with-freeradius

FreeRADIUS Home Web Site

http://freeradius.org/

Deploying FreeRADIUS: A website with excellent step-by-step directions

http://deployingradius.com/documents/configuration/active_directory.html

Tools & Troubleshooting

Decoding RADIUS with Wireshark

http://wiki.wireshark.org/Radius

RADIUS Attribute Types and Values

http://www.iana.org/assignments/radius-types/radius-types.xml

EAP Testing (eapol_test)

http://deployingradius.com/scripts/eapol_test/

FreeRADIUS Debug Log Parser

http://networkradius.com/freeradius.html

FreeRADIUS Troubleshooting

http://wiki.freeradius.org/Troubleshooting

RADIUS Packet Format

http://en.wikipedia.org/wiki/RADIUS

Appendix B: Attribute Value Pairs

Packet Structure

A RADIUS packet (shown below) consists of a code that indicates the message type, packet identifier to match sessions, length, authenticator and AVPs.
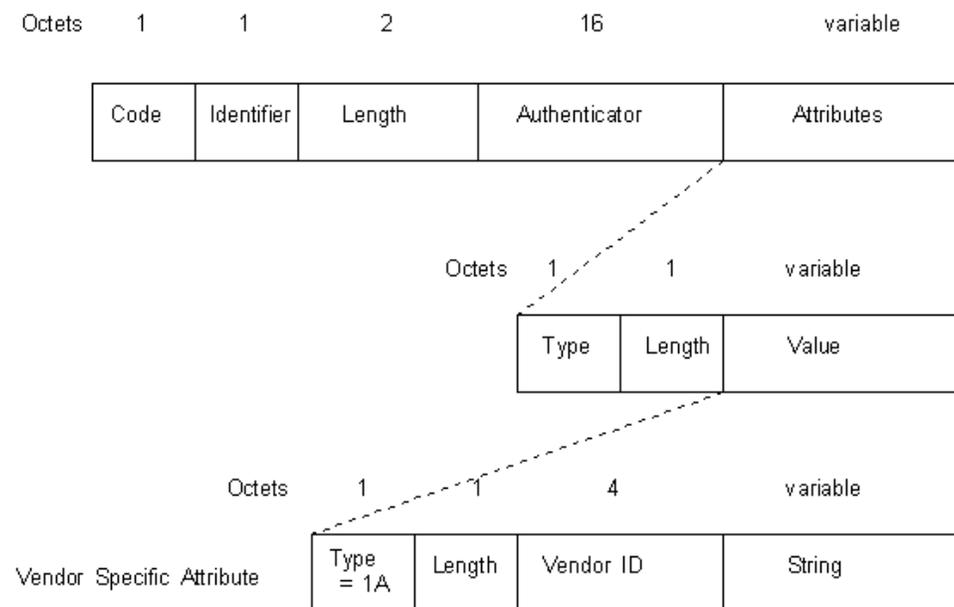

Figure 4 - RADIUS Packet Structure

- The Identifier field aids in matching requests and replies.
- The Length field indicates the length of the entire RADIUS packet including the Code, Identifier, Length, Authenticator and optional Attribute fields.
- The Authenticator is used to authenticate the reply from the RADIUS server, and is used in encrypting passwords; its length is 16 bytes.

Code	Assignment
1	Access-Request
2	Access-Accept
3	Access-Reject
4	Accounting-Request
5	Account-Response
11	Access-Challenge
12	Status-Server (experimental)
13	Status-Client (experimental)
255	Reserved

Authentication Attribute Value Pairs (AVP)

The last part of a RADIUS packet consists of the attribute value pairs (AVPs). These include a code indicating the type, the attribute name and its corresponding value. AVPs used by Ruckus products are shown in the attached spreadsheet.

RADIUS
attributes_v3.xlsx

Access-Accept Message Values Used by the ZoneDirector

The ZoneDirector may make use of some values returned by the RADIUS server. These include the following:

Type	Attribute Name	Usage	Comment
64	Tunnel-Type	Dynamic VLAN assignment	Must be set to "VLAN" (13)

65	Tunnel-Medium-Type	Dynamic VLAN assignment	Must be set to "802" (6)
81	Tunnel-Private-Group-Id	Dynamic VLAN assignment	VLAN ID number (1 – 4094)
85	Acct-Interim-Interval	Set interval for accounting updates	Ignored if local policy exists
27	Session-Timeout	Time before logging off a client	
29	Termination-Action		Session timeout becomes a disconnect or re-authentication event if value is set to Radius-Request (1)

Access-Accept Message Values Used by Standalone APs

A standalone AP may make use of some values returned by the RADIUS server. These include the following:

Type	Attribute Name	Usage	Comment
64	Tunnel-Type		Must be set to "VLAN" (13)
65	Tunnel-Medium-Type		Must be set to "802" (6)
81	Tunnel-Private-Group-Id		VLAN ID number (1 – 4094)
85	Acct-Interim-Interval	Set interval for accounting updates	Ignored if local policy exists
27	Session-Timeout	Time before logging off a client	
29	Termination-Action		Session timeout becomes a disconnect or re-authentication event if value is set to Radius-Request (1)

Accounting Attribute Value Pairs (AVP)

The last part of a RADIUS packet consists of the attribute value pairs (AVPs). These include a code indicating the type, the attribute name and its corresponding value. AVPs used by

Ruckus products are shown in the attached spreadsheet in the Authentication Attribute Value Pairs (AVP) (above).

Appendix C: Ruckus RADIUS Dictionary

This dictionary may be used with a RADIUS server to support extended attributes that are meaningful when Ruckus equipment is used.

```
###################################################################
# -*- text -*-
#
#       dictionary.ruckus
#
#       place the following  line into the "dictionary" file of your
#       FreeRadius installation
#       $INCLUDE dictionary.ruckus
#
#       For use with FreeRadius and ZoneDirector
#
#       rm, 02.11.2012
#
#       Vendor-ID:   25053
#
VENDOR         Ruckus                           25053
BEGIN-VENDOR  Ruckus

# Value Format:      group_attr1,group_attr2,...
ATTRIBUTE     Ruckus-User-Groups  1      string
ATTRIBUTE     Ruckus-Sta-RSSI             2      integer
ATTRIBUTE     Ruckus-SSID        3      string
ATTRIBUTE     Ruckus-WlanID      4      integer
ATTRIBUTE     Ruckus-Location             5      string
ATTRIBUTE     Ruckus-Grace-Period 6      integer
ATTRIBUTE     Ruckus-SCG-CBlade-IP        7      integer
ATTRIBUTE     Ruckus-SCG-DBlade-IP        8      integer
ATTRIBUTE     Ruckus-Session-Type 125    integer
ATTRIBUTE     Ruckus-Acct-Status  126    integer
END-VENDOR    Ruckus
###################################################################
```