

RADIUS Attributes

HOW TO GUIDE



March 2015

Revision 3

© 2015 ZIH Corp. All rights reserved. Zebra and the Stylized Zebra Head are trademarks of ZIH Corp, registered in many jurisdictions worldwide. All other trademarks are property of their respective owners.

Table of Contents:

1. RADIUS Authentication Attributes:	4
1.1 IETF Standard Attributes:	5
1.2 Zebra Vendor-Specific Attributes:	7
2. RADIUS Accounting Attributes:	13
3. Dynamic Authorization Extensions:	17
4. RADIUS Dictionary Files:	18
4.1 Cisco Secure Access Control Server:	18
4.2 FreeRADIUS:	20
4.3 Radiator RADIUS Server:	21
4.4 Steel Belted RADIUS:	22
5. Reference Documentation:	23

1. RADIUS Authentication Attributes:

The RADIUS protocol follows client-server architecture and uses the User Datagram Protocol (UDP) as described in RFC 2865. The RF Switch sends user information to the RADIUS server in an Access-Request message and after receiving a reply from the server acts according to the returned information.

The RADIUS server receives user requests for access from the client, attempts to authenticate the user, and returns the configuration information and policies to the client. The RADIUS server may be configured to authenticate an Access-Request locally or against SQL, Kerberos, LDAP, or Active Directory.

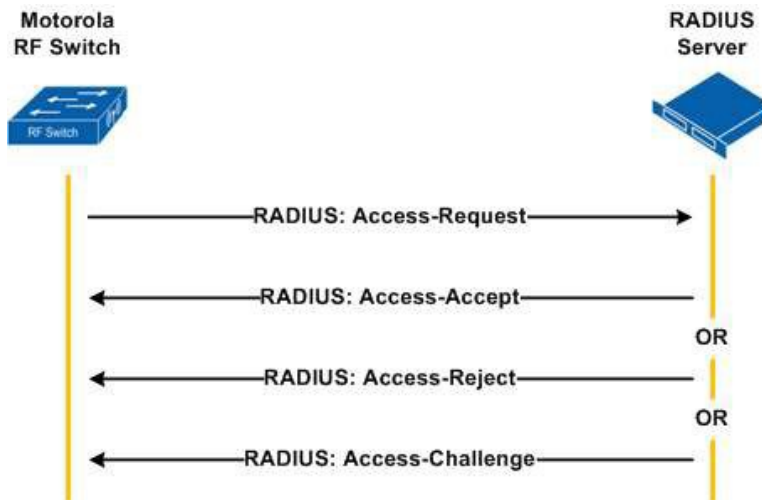


Figure 1.0 – Radius Authentication & Authorization

During authentication the RADIUS server then returns one of three responses to the NAS RF Switch:

- 1) Access-Reject – The user is unconditionally denied access to the requested network resource. Failure reasons may include an invalid credentials or an inactive account.
- 2) Access-Challenge – Requests additional information from the user such as a secondary password, PIN, token or card. Access-Challenge is also used in more complex authentication when a secure tunnel is established between the user and the Radius Server such as authentication using Extensible Authentication Protocol (EAP).
- 3) Access-Accept – The user is permitted access. The Access-Request often includes additional configuration information for the user using return attributes.

RADIUS services can be enabled on the RF Switch for management user authentication as well as WLAN user authentication. RADIUS services are required for WLANs implementing 802.1X EAP and Hotspot services but may also be enabled for MAC based authentication.

1.1 IETF Standard Attributes:

The following table outlines the standard authentication attributes that have been implemented on the RF Switch in accordance to RFC 2865. Additional extensions have also been implemented following the recommendations in RFC 2868 and RFC 2869.

Attribute Name	Type	RFC	Description
User-Name	1	RFC 2865	The <i>User-Name</i> attribute is forwarded in the <i>Access-Request</i> and indicates the name of the user to be authenticated.
User-Password	2	RFC 2865	The <i>User-Password</i> attribute is forwarded in the <i>Access-Request</i> and indicates the password of the user to be authenticated, or the user's input following an <i>Access-Challenge</i> .
CHAP-Password	3	RFC 2865	The <i>CHAP-Password</i> attribute is forwarded in the <i>Access-Request</i> and indicates the PPP Challenge-Handshake Authentication Protocol (CHAP) response to a challenge.
NAS-IP-Address	4	RFC 2865	The <i>NAS-IP-Address</i> attribute is forwarded in the <i>Access-Request</i> and indicates the IP Address of the RF Switch requesting user authentication.
NAS-Port	5	RFC 2865	The <i>NAS-Port</i> attribute is forwarded in the <i>Access-Request</i> and indicates the association index of the user on the RF Switch.
Service-Type	6	RFC 2865	The <i>Service-Type</i> attribute is forwarded in the <i>Access-Request</i> and indicates the type of service the user has requested, or the type of service to be provided. The attribute value is always set to <i>Framed-User</i> by the RF Switch.
Framed-MTU	12	RFC 2865	The <i>Framed-MTU</i> attribute is forwarded in the <i>Access-Request</i> and indicates the Maximum Transmission Unit (MTU) to be configured for the user. The attribute value is always set to <i>1400</i> by the RF Switch.
State	24	RFC 2865	The <i>State</i> attribute is available to be forwarded in the <i>Access-Challenge</i> and must be sent unmodified from the client to the server in the <i>Access-Request</i> reply to that challenge, if any.
Called-Station-Id	30	RFC 2865	The <i>Called-Station-Id</i> attribute is forwarded in the <i>Access-Request</i> and indicates the BSSID and ESSID that the authenticating user is associated with. The RF Switch will forward the attribute value using the following formatting: <i>XX-XX-XX-XX-XX-XX:ESSID</i> .
Calling-Station-Id	31	RFC 2865	The <i>Calling-Station-Id</i> attribute is forwarded in the <i>Access-Request</i> and indicates the MAC address of the authenticating user. It is only used in <i>Access-Request</i> packets. The RF Switch will forward the attribute value using the following formatting: <i>XX-XX-XX-XX-XX-XX</i> .
NAS-Identifier	32	RFC 2865	The <i>NAS-Identifier</i> attribute is forwarded in the <i>Access-Request</i> and indicates the hostname or user

defined identifier of the RF Switch.

CHAP-Challenge	60	RFC 2865	The <i>CHAP-Challenge</i> attribute is forwarded in the <i>Access-Request</i> and indicates the CHAP Challenge sent by the RF Switch to a PPP Challenge-Handshake Authentication Protocol (CHAP) user.
NAS-Port-Type	61	RFC 2865	The <i>NAS-Port-Type</i> attribute is forwarded in the <i>Access-Request</i> and indicates the type of physical connection for the authenticating the user. The attribute value is always set to <i>Wireless-802.11</i> by the RF Switch.
Connection-Info	77	RFC 2869	The <i>Connection-Info</i> attribute is forwarded in the <i>Access-Request</i> and indicates the data-rate and radio type of the authenticating user. The RF Switch will forward the attribute value using the following formatting: <i>CONNECT XXMbps 802.11X</i> .
NAS-Port-Id	87	RFC 2869	The <i>NAS-Port-Id</i> attribute is forwarded in the <i>Access-Request</i> and indicates the ESSID that the authenticating user is associated with.
CHAP-Challenge	60	RFC 2865	The <i>CHAP-Challenge</i> attribute is forwarded in the <i>Access-Request</i> and contains the CHAP Challenge sent by the RF Switch to a PPP Challenge-Handshake Authentication Protocol (CHAP) user.
EAP-Message	79	RFC 2869	The <i>EAP-Message</i> attribute is forwarded in the <i>Access-Request</i> , <i>Access-Challenge</i> , <i>Access-Accept</i> and <i>Access-Reject</i> and encapsulates Extended Access Protocol (EAP) packets.
Message-Authenticator	80	RFC 2869	The <i>Message-Authenticator</i> attribute is forwarded in the <i>Access-Request</i> and may be used to prevent spoofing of CHAP, ARAP or EAP <i>Access-Request</i> packets.
Tunnel-Private-Group-ID	81	RFC 2868	The <i>Tunnel-Private-Group-ID</i> attribute is forwarded in the <i>Access-Accept</i> and indicates the numerical VLAN ID to be assigned to the authenticating user. The attribute value must be set to a numerical value between 1 and 4094.

Table 1.1 – IETF Standard Authentication Attributes

1.1.1 Tunnel-Private-Group-ID:

The *Tunnel-Private-Group-ID* attribute may be forwarded in the *Access-Accept* to indicate the dynamic VLAN membership of an 802.1X or RADIUS MAC authenticated user. Note that the VLAN value returned from the RADIUS server will override any static VLAN(s) defined in the WLAN profile.

Attribute Name	Attribute Number	Attribute Value
Tunnel-Private-Group-ID	81	1 – 4094 (Assigned VLAN-ID)

Table 1.1.1 – Attribute Details

1.2 Zebra Vendor-Specific Attributes:

The following table outlines the Zebra vendor-specific attributes (VSAs) authentication attributes that have been implemented on the RF Switch in accordance to RFC 2865.

Attribute Name	Type	Vendor ID	Attribute Number	Formatting
Symbol-Admin-Role	26	388	1	Integer
Symbol-Current-ESSID	26	388	2	String
Symbol-Allowed-ESSID	26	388	3	String
Symbol-WLAN-Index	26	388	4	Integer
Symbol-QoS-Profile	26	388	5	Integer
Symbol-Allowed-Radio	26	388	6	String
Symbol-Expiry-Date-Time	26	388	7	String
Symbol-Start-Date-Time	26	388	8	String
Symbol-Posture-Status	26	388	9	String
Symbol-Downlink-Limit	26	388	10	String
Symbol-Uplink-Limit	26	388	11	Integer
Symbol-User-Group	26	388	12	String
Symbol-Login-Source	26	388	100	Integer

Table 1.2 – Zebra VSAs

1.2.1 Symbol-Admin-Role:

The *Symbol-Admin-Role* attribute maybe forwarded in a *Access-Accept* and indicates the permissions a management user is granted on an RF Switch when RADIUS management user authentication is enabled.

The *Symbol-Admin-Role* attribute can be used to assign one or more management roles to a user. When multiple roles are assigned, multiple *Symbol-Admin-Role* attributes and values must be returned to the RF Switch.

Attribute Name	Vendor ID	Attribute Number	Attribute Format
Symbol-Admin-Role	388	1	Integer

Integer Value	Associated Roles	Description
1	Monitor	The <i>Monitor</i> role is assigned to personnel requiring read-only access to an RF Switch.
2	Help Desk Manager	The <i>Help Desk Manager</i> role is assigned to personnel responsible for troubleshooting and debugging problems. The Help Desk Manager role provides access to troubleshooting utilities, execution of service commands, logs and can reboot the switch.
4	Network Administrator	The <i>Network Administrator</i> role is assigned to personnel responsible for configuration of wired and wireless parameters such as IP configuration, VLANs, Firewall, WLANs, Radios, IDS and hotspot.
8	System Administrator	The <i>System Administrator</i> role is assigned to personnel responsible for configuring general switch settings such as NTP, boot parameters, licenses, images, auto install, clustering and access control.
16	Web User Administrator	The <i>Web User Administrator</i> role is assigned to non skilled personnel responsible for adding guest user accounts for Hotspot authentication.
32	Security	The <i>Security</i> role is assigned to personnel Responsible for changing Wireless LAN keys
64	Device Provisioning Admin	The <i>Device Provisioning Administrator</i> has privileges to update device firmware. Such updates run the risk of overwriting and losing a device's existing configuration unless the configuration is properly archived.
32768	Super User	The <i>Super User</i> role is assigned to personnel requiring full administrative privileges.

Table 1.2.1 – Symbol-Admin-Role Attribute Details

1.2.2 Symbol-Current-ESSID:

The *Symbol-Current-ESSID* attribute is forwarded in the *Access-Request* and indicates the ESSID the authenticating user is associated with.

Attribute Name	Vendor ID	Attribute Number	Attribute Format
Symbol-Current-ESSID	388	2	String

Format: *ESSID-Name*

Example: *Hotspot*

Table 1.2.2 – Attribute Details

1.2.3 Symbol-Allowed-ESSID:

The *Symbol-Allowed-ESSID* attribute maybe forwarded in the *Access-Accept* and indicates one or more ESSIDs that the user is permitted to associate with.

During authorization the RF Switch will check the returned ESSID(s) against the current ESSID the authenticating user is associated with. If the returned ESSID(s) match the user is permitted access. If the returned ESSID(s) do not match the user will be denied access.

The *Symbol-Allowed-ESSID* attribute can be used to permit access to one or more ESSIDs. When multiple ESSIDs are permitted multiple *Symbol-Allowed-ESSID* attributes and values must be returned to the RF Switch.

Attribute Name	Vendor ID	Attribute Number	Attribute Format
Symbol-Allowed-ESSID	388	3	String

Format: *ESSID-Name*

Example: *Sales*

Table 1.2.3 – Attribute Details

1.2.4 Symbol-WLAN-Index:

The *Symbol-WLAN-Index* attribute is forwarded in the *Access-Request* and indicates the WLAN index number of the WLAN the authenticating user is associated with.

Attribute Name	Vendor ID	Attribute Number	Attribute Format
Symbol-WLAN-Index	388	4	Integer

Format: *Index-Number*

Example: 2

Table 1.2.4 – Attribute Details

1.2.5 Symbol-QoS-Profile:

The *Symbol-QoS-Profile* attribute maybe forwarded in the *Access-Accept* and indicates the static WMM Access Category (AC) to be assigned to the authenticating user. Once assigned traffic forwarded from the AP to the user will be prioritized using the assigned QoS value.

Attribute Name	Vendor ID	Attribute Number	Attribute Format
Symbol-QoS-Profile	388	5	Integer

Supported Values: 4 (*Voice*), 3 (*Video*), 2 (*Background*), 1 (*Best Effort*)

Example: 1

Table 1.2.5 – Attribute Details

1.2.6 Symbol-Allowed-Radio:

The *Symbol-Allowed-Radio* attribute maybe forwarded in the *Access-Accept* and indicates one or more radios that the authenticating user is permitted to associate with.

The *Symbol-Allowed-Radio* returned value must match one or more key words defined in the radio description fields for the user to be permitted access. For example if the RADIUS server returns the string *1st-Floor*, the RF Switch will only permit access to radios with *1st-Floor* defined in the description field such as *1st-Floor-Conference-Room*, *1st-Floor-Cafateria* etc. The user in this example would be denied access to radios with the description *2nd-Floor-Conference-Room* or *AP300-1*.

Attribute Name	Vendor ID	Attribute Number	Attribute Format
Symbol-Allowed-Radio	388	6	String

Format: *Radio-Index-Number*

Example: *1st-Floor*

Table 1.2.6 – Attribute Details

1.2.7 Symbol-Expiry-Date-Time:

The *Symbol-Expiry-Date-Time* attribute maybe forwarded in the *Access-Accept* and indicates the date and time the authenticating user is no longer authorized to access the network.

During authorization the RF Switch will check the returned date and time values against the current date and time on the RF Switch. If the returned date and time is *before* the current date and time on the RF Switch the user will be permitted access. If the returned date and time is *after* the current date and time on the RF Switch the user will be denied access.

Attribute Name	Vendor ID	Attribute Number	Attribute Format
Symbol-Expiry-Date-Time	388	7	String

Format: *MM/DD/YYYY-HH:MM*

Example: *01/02/2009-17:00*

Table 1.2.7 – Attribute Details

1.2.8 Symbol-Start-Date-Time:

The *Symbol-Start-Date-Time* attribute maybe forwarded in the *Access-Accept* and indicates the date and time the authenticating user is initially permitted to access the network.

During authorization the RF Switch will check the returned date and time values against the current date and time on the RF Switch. If the returned date and time is *after* the current date and time on the RF Switch the user will be permitted access. If the returned date and time is *before* than the current date and time on the RF Switch the user will be denied access.

Attribute Name	Vendor ID	Attribute Number	Attribute Format
Symbol-Start-Date-Time	388	8	String

Format: *MM/DD/YYYY-HH:MM*

Example: *01/01/2009-08:00*

Table 1.2.8 – Attribute Details

1.2.9 Symbol-Posture-Status:

The *Symbol-Posture-Status* attribute maybe forwarded in the *Access-Accept* and indicates the NAP compliance state of the authenticating user. This attribute is used with the Symantec LAN Enforcer endpoint inspection solution.

Attribute Name	Vendor ID	Attribute Number	Attribute Format
Symbol-Posture-Status	388	9	String

Table 1.2.9 – Attribute Details

1.2.10 Symbol-Downlink-Limit:

The *Symbol-Downlink-Limit* attribute maybe forwarded in the *Access-Accept* and indicates the amount of bandwidth in Kbps that the authenticating user is permitted to receive from the AP. Traffic that exceeds the defined value will be dropped by the RF Switch.

Attribute Name	Vendor ID	Attribute Number	Attribute Format
Symbol-Downlink-Limit	388	10	Integer

Format: 0, 100-10,000 (0 = Disabled)

Example: 768

Table 1.2.10 – Attribute Details

1.2.11 Symbol-Uplink-Limit:

The *Symbol-Uplink-Limit* attribute maybe forwarded in the *Access-Accept* and indicates the amount of bandwidth in Kbps that the authenticating user is permitted to transmit to the AP. Traffic that exceeds the defined value will be dropped by the RF Switch.

Attribute Name	Vendor ID	Attribute Number	Attribute Format
Symbol-Uplink-Limit	388	11	Integer

Format: 0, 100-10,000 (0 = Disabled)

Example: 512

Table 1.2.11 – Attribute Details

1.2.12 Symbol-User-Group:

The *Symbol-User-Group* attribute maybe forwarded in the *Access-Accept* and indicates the group on the RF Switch that the authenticating user is to be associated with. The *Symbol-User-Group* attribute is used with the role base firewall to dynamically assign firewall policies to users based on group membership.

Attribute Name	Vendor ID	Attribute Number	Attribute Format
Symbol-User-Group	388	12	String

Format: *Group-Name*

Example: *Sales*

Table 1.2.12 – Attribute Details

1.2.13 Symbol-Login-Source:

The *Symbol-Login-Source* attribute may be forwarded in the *Access-Accept* and indicates the management interfaces the user is permitted to access on the RF Switch when RADIUS management user authentication is enabled.

During authorization the RF Switch will check the returned list of permitted interfaces against the current interface the user is authenticating through. If the interface is permitted the user will be permitted access to the RF Switch. If the interface is not permitted the user will be denied access to the RF Switch.

The *Symbol-Login-Source* attribute can be used to permit access to one or more management interfaces or all management interfaces. When multiple interfaces are assigned, multiple *Symbol-Login-Source* attributes and values must be returned to the RF Switch.

Attribute Name	Vendor ID	Attribute Number	Attribute Format
Symbol-Login-Source	388	100	Integer

Integer Value	Login Source	Description
16	HTTP	The <i>HTTP</i> login source permits management access using the Web-UI.
32	SSH	The <i>SSH</i> login source permits management access using SSH.
64	Telnet	The <i>Telnet</i> login source permits management access using Telnet.
128	Console	The <i>Console</i> login source permits management access using serial console.
240	All	The <i>All</i> login source permits management access using all management interfaces.

Table 1.2.13 – Attribute Details

2. RADIUS Accounting Attributes:

RADIUS accounting is used to send accounting information about an authenticated session to the RADIUS accounting server. Accounting information is sent to the server when a user connects and disconnects from a WLAN and may also be periodically forwarded during the session.

RADIUS accounting information can be used to track individual user's network usage for billing purposes as well as be used as a tool for gathering statistic for general network monitoring.

When network access is granted to the user by the RF Switch, an Accounting-Request message with the Acct-Status-Type field set to Start is forwarded by the RF Switch to the RADIUS server to signal the start of the user's network access. Start records typically contain the user's identification, network address, point of attachment and a unique session identifier.

Optionally periodic Accounting-Request messages with the Acct-Status-Type field set to Interim Update may be sent by the RF Switch to the RADIUS server to update it on the status of an active session. Interim records typically convey the current session duration and information on current data usage.

When the user's session is closed, the RF Switch forwards an Accounting-Request message with the Acct-Status-Type field set to Stop. This provides information on the final usage in terms of time, packets transferred, data transferred and reason for disconnect and other information related to the user's network access.

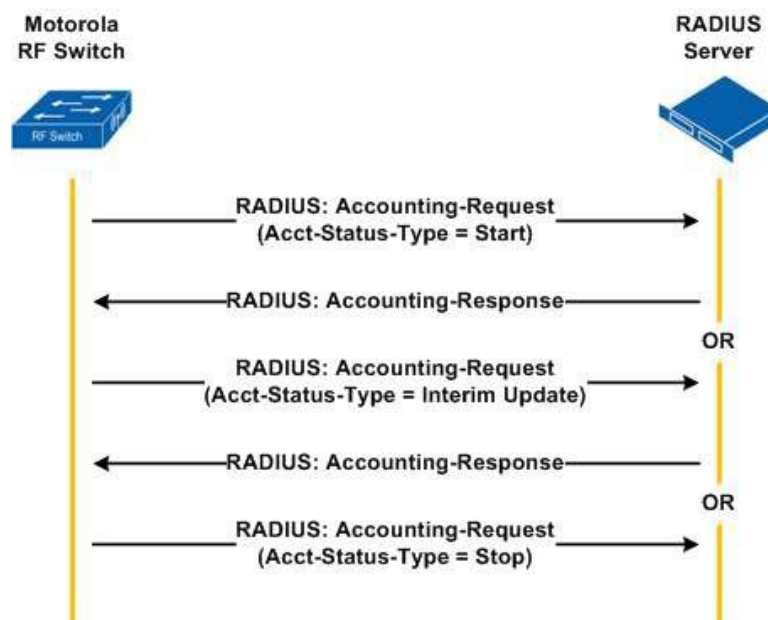


Figure 2.0 – RADIUS Accounting

RADIUS Accounting can be enabled / disabled on the RF Switch for each WLAN profile and administrators can select how the RF Switch forwards accounting information to the RADIUS server. For each WLAN profile the following accounting configuration is supported:

- 1) Start-Stop – The RF Switch will forward Accounting-Requests at the start and end of the user sessions.
- 2) Stop-Only – The RF Switch will forward Accounting-Requests at the end of the user sessions.
- 3) Start-Interim-Stop – The RF Switch will forward Accounting-Requests at the start and end of the user sessions as well as periodically during the lifetime of the sessions.

The following table outlines the standard RADIUS accounting attributes that have been implemented on the RF Switch in accordance to RFC 2866:

Attribute Name	Type	RFC	Description
User-Name	1	RFC 2865	The <i>User-Name</i> attribute is forwarded in the <i>Accounting-Request</i> and indicates the name of the user.
NAS-IP-Address	4	RFC 2865	The <i>NAS-IP-Address</i> attribute is forwarded in the <i>Accounting-Request</i> and indicates the IP Address of the RF Switch.
NAS-Port	5	RFC 2865	The <i>NAS-Port</i> attribute is forwarded in the <i>Accounting-Request</i> and indicates the association index of the user on the RF Switch.
Class	25	RFC 2865	The <i>Class</i> attribute is optionally forwarded in the <i>Access-Accept</i> and should be sent unmodified by the client to the accounting server as part of the <i>Accounting-Request</i> packet if accounting is supported.
Called-Station-Id	30	RFC 2865	The <i>Called-Station-Id</i> attribute is forwarded in the <i>Accounting-Request</i> and indicates the BSSID and ESSID that the user is associated with. The RF Switch will forward the attribute value using the following formatting: <i>XX-XX-XX-XX-XX-XX:ESSID</i> .
Calling-Station-Id	31	RFC 2865	The <i>Calling-Station-Id</i> attribute is forwarded in the <i>Accounting-Request</i> and indicates the MAC address of the user. The RF Switch will forward the attribute value using the following formatting: <i>XX-XX-XX-XX-XX-XX</i> .
NAS-Identifier	32	RFC 2865	The <i>NAS-Identifier</i> attribute is forwarded in the <i>Accounting-Request</i> and indicates the hostname or user defined identifier of the RF Switch.
Acct-Status-Type	40	RFC 2866	The <i>Acct-Status-Type</i> attribute is forwarded in the <i>Accounting-Request</i> and indicates whether the <i>Accounting-Request</i> marks the status of the accounting update. Supported values include <i>Start</i> , <i>Stop</i> and <i>Interim-Update</i> .
Acct-Delay-Time	41	RFC 2866	The <i>Acct-Delay-Time</i> attribute is forwarded in the <i>Accounting-Request</i> and indicates how many seconds the RF Switch has been trying to send the accounting record for. This value is subtracted from the time of arrival on the server to find the approximate time of the event generating this <i>Accounting-Request</i> .
Acct-Input-Octets	42	RFC 2866	The <i>Acct-Input-Octets</i> attribute is forwarded in the <i>Accounting-Request</i> and indicates how many octets have been received from the user over the course of the connection. This attribute may only be present in <i>Accounting-Request</i> records where the <i>Acct-Status-Type</i> is set to <i>Stop</i> .
Acct-Output-Octets	43	RFC 2866	The <i>Acct-Output-Octets</i> attribute is forwarded in the <i>Accounting-Request</i> and indicates how many octets have been forwarded to the user over the course of the connection. This attribute may only be present in

Accounting-Request records where the *Acct-Status-Type* is set to *Stop*.

Acct-Session-Id	44	RFC 2866	The <i>Acct-Session-Id</i> attribute is forwarded in the <i>Accounting-Request</i> and provides a unique identifier to make it easy to match start, stop and interim records in an accounting log file.
Account-Authentic	45	RFC 2866	The <i>Account-Authentic</i> attribute is forwarded in the <i>Accounting-Request</i> and indicates how the user was authenticated. When RADIUS accounting is enabled the RF Switch will set this value to <i>RADIUS</i> .
Acct-Session-Time	46	RFC 2866	The <i>Acct-Session-Time</i> attribute is forwarded in the <i>Accounting-Request</i> and indicates how many seconds the user has received service for. This attribute may only be present in <i>Accounting-Request</i> records where the <i>Acct-Status-Type</i> is set to <i>Stop</i> .
Acct-Input-Packets	47	RFC 2866	The <i>Acct-Input-Packets</i> attribute is forwarded in the <i>Accounting-Request</i> and indicates how many packets have been received from the user over the course of the connection. This attribute may only be present in <i>Accounting-Request</i> records where the <i>Acct-Status-Type</i> is set to <i>Stop</i> .
Acct-Output-Packets	48	RFC 2866	The <i>Acct-Output-Packets</i> attribute is forwarded in the <i>Accounting-Request</i> and indicates how many packets have been forwarded to the user over the course of the connection. This attribute may only be present in <i>Accounting-Request</i> records where the <i>Acct-Status-Type</i> is set to <i>Stop</i> .
Acct-Terminate-Cause	49	RFC 2866	The <i>Acct-Terminate-Cause</i> attribute is forwarded in the <i>Accounting-Request</i> and indicates how the session was terminated. This attribute may only be present in <i>Accounting-Request</i> records where the <i>Acct-Status-Type</i> is set to <i>Stop</i> .
Event-Timestamp	55	RFC 2869	The <i>Event-Timestamp</i> attribute is forwarded in the <i>Accounting-Request</i> and indicates the time that the accounting event occurred on the RF Switch.
NAS-Port-Type	61	RFC 2865	The <i>NAS-Port-Type</i> attribute is forwarded in the <i>Accounting-Request</i> and indicates the type of physical connection for the user. This attribute value is always set to <i>Wireless-802.11</i> by the RF Switch.
Tunnel-Type	64	RFC 2868	The <i>Tunnel-Type</i> attribute is forwarded in the <i>Accounting-Request</i> indicates the tunneling protocol(s) used by the user. This attribute value is always set to type <i>13 (Virtual LANs)</i> .
Tunnel-Medium-Type	65	RFC 2868	The <i>Tunnel-Medium-Type</i> attribute is forwarded in the <i>Accounting-Request</i> and indicates which transport medium used by the user. This attribute value is always set to type <i>6 (802 includes all 802 media plus Ethernet "canonical format")</i> .
Tunnel-Private-Group-ID	81	RFC 2868	The <i>Tunnel-Private-Group-ID</i> attribute is forwarded in the <i>Accounting-Request</i> and indicates the numerical

			VLAN ID assigned to the user. This attribute value is always set to a numerical value between 1 and 4094.
NAS-Port-Id	87	RFC 2869	The <i>NAS-Port-Id</i> attribute is forwarded in the <i>Accounting-Request</i> and indicates the ESSID that the user is associated with.

Table 2.0 – IETF Standard Accounting Attributes

3. Dynamic Authorization Extensions:

The RADIUS authentication protocol does not support unsolicited messages sent from the RADIUS server to the RF Switch. However, there are many instances in which it is desirable for changes to be made to session characteristics without requiring the RF Switch to initiate the exchange.

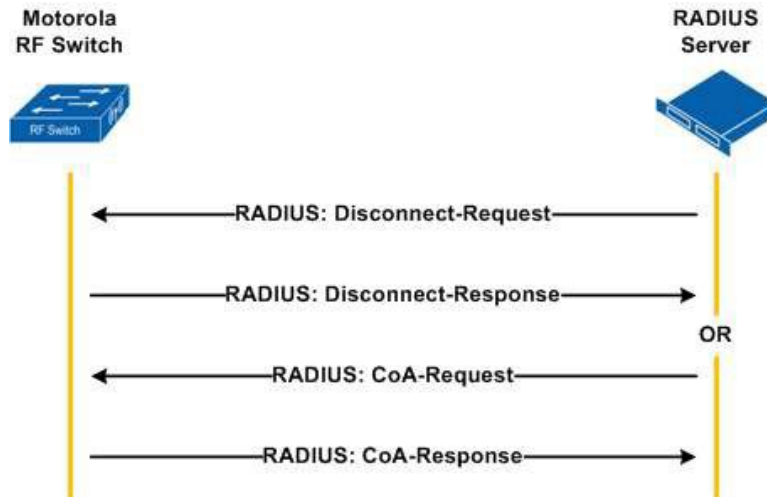


Figure 3.0 – Dynamic Authorization Extensions

To overcome these limitations several vendors have implemented additional RADIUS extensions support unsolicited messages sent from the RADIUS server to a RF Switch. These extensions support Disconnect and Change-of-Authorization (CoA) messages that can be used to terminate an active user session or change the characteristics of an active session.

- 1) Disconnect-Request – Causes a user session to be terminated. The Disconnect-Request packet identifies the NAS as well as the user session to be terminated by inclusion of the identification attributes shown in table 3.0.
- 2) CoA-Request – Causes session information to be dynamically updated on the RF Switch. Currently a CoA-Request packet may only be used to change the session-timeout and the idle-timeout of a user.

The following table outlines the dynamic authorization extension attributes that have been implemented on the RF Switch in accordance to RFC 3576.

Attribute Name	Type	RFC	Description
User-Name	1	RFC 2865	Name of the user.
Calling-Station-Id	31	RFC 2865	MAC address of the user.
Acct-Session-Id	44	RFC 2866	The identifier uniquely identifying the session on the NAS.

Table 3.0 – Dynamic Authorisation Extensions



The Called-Station-Id, NAS-Identifier, NAS-IP-Address and Service-Type attributes are also evaluated by the RF Switch if present.

4. RADIUS Dictionary Files:

4.1 Cisco Secure Access Control Server:

The following provides the necessary information to create a dictionary file that includes all the supported vendor specific attributes for Cisco Secure Access Control Server. The provided text can be copied into a file named *symbol.ini* and imported using the provided CSUtil utility.

```
;
; Zebra RF Switch Dictionary File for Cisco Secure ACS
; Last Updated: July 21st 2009
; Created By: Kevin Marshall
;

[User Defined Vendor]
Name=SYMBOL
IETF Code=388

VSA 1=Symbol-Admin-Role
VSA 2=Symbol-Current-ESSID
VSA 3=Symbol-Allowed-ESSID
VSA 4=Symbol-WLAN-Index
VSA 5=Symbol-QoS-Profile
VSA 6=Symbol-Allowed-Radio
VSA 7=Symbol-Expiry-Date-Time
VSA 8=Symbol-Start-Date-Time
VSA 9=Symbol-Posture-Status
VSA 10=Symbol-Downlink-Limit
VSA 11=Symbol-Uplink-Limit
VSA 12=Symbol-User-Group
VSA 100=Symbol-Login-Source

[Symbol-Admin-Role]
Type=INTEGER
Profile=OUT
Enums=Admin-Role

[Admin-Role]
1=Monitor
2=Helpdesk
4=NetworkAdmin
8=SysAdmin
16=WebAdmin
32768=SuperUser

[Symbol-Current-ESSID]
Type=STRING
Profile=IN

[Symbol-Allowed-ESSID]
Type=STRING
Profile=OUT
```

[Symbol-WLAN-Index]
Type=INTEGER
Profile=IN

[Symbol-QoS-Profile]
Type=INTEGER
Profile=IN

[Symbol-Allowed-Radio]
Type=STRING
Profile=OUT

[Symbol-Expiry-Date-Time]
Type=STRING
Profile=OUT

[Symbol-Start-Date-Time]
Type=STRING
Profile=OUT

[Symbol-Posture-Status]
Type=STRING
Profile=OUT

[Symbol-Downlink-Limit]
Type=INTEGER
Profile=OUT

[Symbol-Uplink-Limit]
Type=INTEGER
Profile=OUT

[Symbol-User-Group]
Type=STRING
Profile=OUT

[Symbol-Login-Source]
Type=INTEGER
Profile=OUT
Enums=Login-Source

[Login-Source]
16=HTTP
32=SSH
64=Telnet
128=Console
240=All

4.2 FreeRADIUS:

The following provides the necessary information to create a dictionary file that includes all the supported vendor specific attributes for FreeRADIUS. The provided text can be copied into a file named ***dictionary.symbol***.

```
#
# Zebra RF Switch Dictionary File for FreeRADIUS
# Last Updated: July 21st 2009
# Created By: Kevin Marshall
#

VENDOR          Symbol          388

ATTRIBUTE       Symbol-Admin-Role      1          integer      Symbol
VALUE           Symbol-Admin-Role      Monitor     1
VALUE           Symbol-Admin-Role      Helpdesk    2
VALUE           Symbol-Admin-Role      NetworkAdmin 4
VALUE           Symbol-Admin-Role      SysAdmin    8
VALUE           Symbol-Admin-Role      WebAdmin    16
VALUE           Symbol-Admin-Role      SuperUser   32768

ATTRIBUTE       Symbol-Current-ESSID   2          string        Symbol
ATTRIBUTE       Symbol-Allowed-ESSID   3          string        Symbol
ATTRIBUTE       Symbol-WLAN-Index      4          integer       Symbol
ATTRIBUTE       Symbol-QoS-Profile     5          integer       Symbol
ATTRIBUTE       Symbol-Allowed-Radio   6          string        Symbol
ATTRIBUTE       Symbol-Expiry-Date-Time 7          string        Symbol
ATTRIBUTE       Symbol-Start-Date-Time 8          string        Symbol
ATTRIBUTE       Symbol-Posture-Status  9          string        Symbol
ATTRIBUTE       Symbol-Downlink-Limit 10         integer       Symbol
ATTRIBUTE       Symbol-Uplink-Limit    11         integer       Symbol
ATTRIBUTE       Symbol-User-Group      12         string        Symbol

ATTRIBUTE       Symbol-Login-Source    100        integer       Symbol
VALUE           Symbol-Login-Source    HTTP        16
VALUE           Symbol-Login-Source    SSH         32
VALUE           Symbol-Login-Source    Telnet      64
VALUE           Symbol-Login-Source    Console     128
VALUE           Symbol-Login-Source    All         240
```

4.3 Radiator RADIUS Server:

The following provides the necessary information to create a dictionary file that includes all the supported vendor specific attributes for Radiator. The provided text can be copied into the main Radiator dictionary file.

```
#
# Zebra RF Switch Dictionary File for Radiator
# Last Updated: July 21st 2009
# Created By: Kevin Marshall
#

VENDORATTR 388 Symbol-Admin-Role 1 integer
VALUE Symbol-Admin-Role Monitor 1
VALUE Symbol-Admin-Role HelpDesk 2
VALUE Symbol-Admin-Role NetworkAdmin 4
VALUE Symbol-Admin-Role SystemAdmin 8
VALUE Symbol-Admin-Role WebAdmin 16
VALUE Symbol-Admin-Role SuperUser 32768

VENDORATTR 388 Symbol-Current-ESSID 2 string
VENDORATTR 388 Symbol-Allowed-ESSID 3 string
VENDORATTR 388 Symbol-WLAN-Index 4 integer
VENDORATTR 388 Symbol-QoS-Profile 5 integer
VENDORATTR 388 Symbol-Allowed-Radio 6 string
VENDORATTR 388 Symbol-Expiry-Date-Time 7 string
VENDORATTR 388 Symbol-Start-Date-Time 8 string
VENDORATTR 388 Symbol-Posture-Status 9 string
VENDORATTR 388 Symbol-Downlink-Limit 10 integer
VENDORATTR 388 Symbol-Uplink-Limit 11 integer
VENDORATTR 388 Symbol-User-Group 12 string

VENDORATTR 388 Symbol-Login-Source 100 integer
VALUE Symbol-Login-Source HTTP 16
VALUE Symbol-Login-Source SSH 32
VALUE Symbol-Login-Source Telnet 64
VALUE Symbol-Login-Source Console 128
VALUE Symbol-Login-Source All 240
```

4.4 Steel Belted RADIUS:

The following provides the necessary information to create a dictionary file that includes all the supported vendor specific attributes for Steel Belted RADIUS. The provided text can be copied into a file named *symbol.dct*.

```
#
# Zebra RF Switch Dictionary File for Steel Belted RADIUS
# Last Updated: July 21st 2009
# Created By: Kevin Marshall
#
@radius.dct

MACRO    Symbol-VSA(type,syntax)      26      [vid=388 type1=%type% len1=+2 data=%syntax%]

ATTRIBUTE Symbol-Admin-Role          Symbol-VSA(1, integer) R
VALUE     Symbol-Admin-Role          Monitor      1
VALUE     Symbol-Admin-Role          Helpdesk     2
VALUE     Symbol-Admin-Role          NetworkAdmin 4
VALUE     Symbol-Admin-Role          SystemAdmin  8
VALUE     Symbol-Admin-Role          WebAdmin     16
VALUE     Symbol-Admin-Role          SuperUser    32768

ATTRIBUTE Symbol-Current-ESSID        Symbol-VSA(2, string) C
ATTRIBUTE Symbol-Allowed-ESSID        Symbol-VSA(3, string) R
ATTRIBUTE Symbol-WLAN-Index           Symbol-VSA(4, integer) C
ATTRIBUTE Symbol-QoS-Profile          Symbol-VSA(5, integer) C
ATTRIBUTE Symbol-Allowed-Radio        Symbol-VSA(6, string) R
ATTRIBUTE Symbol-Expiry-Date-Time     Symbol-VSA(7, string) R
ATTRIBUTE Symbol-Start-Date-Time      Symbol-VSA(8, string) R
ATTRIBUTE Symbol-Posture-Status       Symbol-VSA(9, string) R
ATTRIBUTE Symbol-Downlink-Limit       Symbol-VSA(10, integer) R
ATTRIBUTE Symbol-Uplink-Limit         Symbol-VSA(11, integer) R
ATTRIBUTE Symbol-User-Group           Symbol-VSA(12, string) R

ATTRIBUTE Symbol-Login-Source         Symbol-VSA(100, integer) R
VALUE     Symbol-Login-Source         HTTP         16
VALUE     Symbol-Login-Source         SSH          32
VALUE     Symbol-Login-Source         Telnet       64
VALUE     Symbol-Login-Source         Console     128
VALUE     Symbol-Login-Source         All         240
```

5. Reference Documentation:

Description	Location
Zebra RFS Series Wireless LAN Switches WiNG System Reference Guide	http://support.symbol.com
Zebra RF Switch CLI Reference Guide	http://support.symbol.com

