Technical Guide

RADIUS

Feature Overview and Configuration Guide

Introduction

RADIUS (Remote Authentication Dial In User Service) is a networking protocol that provides centralized authentication, authorization, and accounting services for users who connect and use network services. The point at which the user connects to the network is known as the Network Access Server (NAS), while user authentication and account information is stored in a database on the RADIUS server. The RADIUS protocol is used to communicate between the Network Access Servers and the RADIUS server.

When a user connects to the network, the NAS challenges the user for authentication, and passes on the authentication to the RADIUS server to check. Based on the result of the check against the user database, the RADIUS server informs the NAS whether or not to allow the connected user access to the network.

A RADIUS server can do more than allow or deny access to the network. A RADIUS server can send back parameters to the connected users, such as an IP address for the user, or a VLAN for the user, or a privilege level for a session. RADIUS also provides an accounting service. Switches can inform the RADIUS server how long a user has been connected to the network, and how much traffic the user has sent and received while connected to the network.

The original use for RADIUS was for the authentication of users dialing into an ISP (Internet Service Provider). A PPP (Point-to-Point Protocol) connection would be established between the remote client and the ISP's access switch. The ISP's access switch would receive the client's username and password using PAP (Password Authentication Protocol) or using CHAP (Challenge Handshake Authentication Protocol) and pass on the client's username and password to the RADIUS server to authenticate the client. The RADIUS server's response to the authentication request would be sent back to the client as a PAP or CHAP allow or deny.

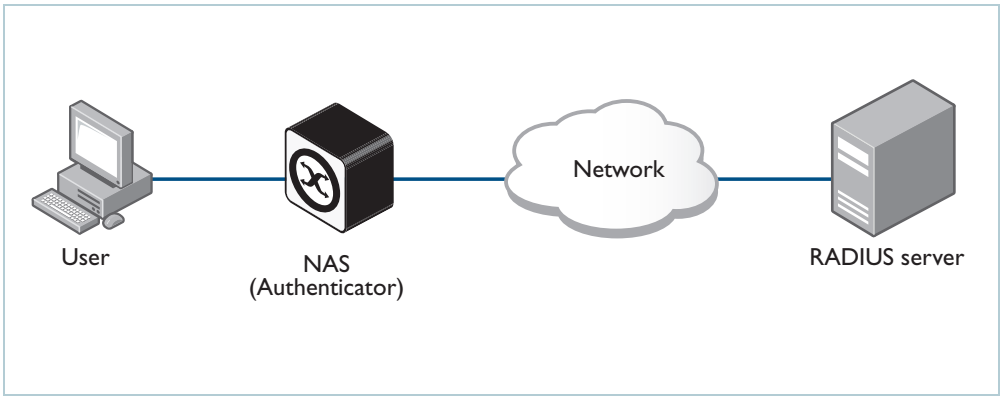
RADIUS has been adapted to network access authentication applications. Network access authentication using RADIUS follows a similar method to the PPP dial-up application for ISPs. For general network access authentication there is the RADIUS server where the database of user authentication data is stored and

a NAS (Network Access Server), which is the switch that user connects to first. The RADIUS server and the NAS communicate with each other through exchanging attributes. Usernames and passwords are treated as attributes in RADIUS packets to and from a RADIUS server and a NAS. The RADIUS server is configured with a list of valid NASs that are allowed to send authentication requests to the RADIUS server.

The RADIUS server will not accept authentication requests from a NAS that is not on the list of valid NASs. Each NAS has a shared secret, which is a shared key with the RADIUS server that is used to authenticate requests. The RADIUS server has access to a list of user authentication data, stored within the RADIUS server or accessed from another server.

Communication between the NAS and RADIUS server uses the RADIUS protocol. The RADIUS protocol uses UDP packets. There are two UDP ports used as the destination port for RADIUS authentication packets (ports 1645 and 1812). Note that port 1812 is in more common use than port 1645 for authentication packets. UDP ports (1646 and 1813) are used for RADIUS accounting separately from the ports used for RADIUS authentication.

Figure 10: Example showing a user to a NAS to a RADIUS server network connection



Products and software version that apply to this guide

This guide applies to all AlliedWare Plus™ products, running version **5.4.4** or later.

Feature support may change in later software versions. For the latest information, see the following documents:

- The product's Datasheet
- The product's Command Reference

These documents are available from the above links on our website at alliedtelesis.com.

The following features are supported since the following software versions:

- RADIUS Proxy - 5.4.8-0.x
- For security purposes, it is possible to specify a radius server with a named VRF. Placing a radius server within a VRF means that no actor that resides outside of the VRF can contact the radius server. - 5.5.2-1.1
- From version 5.5.5-1.1 onwards, you can configure RADIUS over TLS for TQR Series devices.

Contents

RADIUS Overview

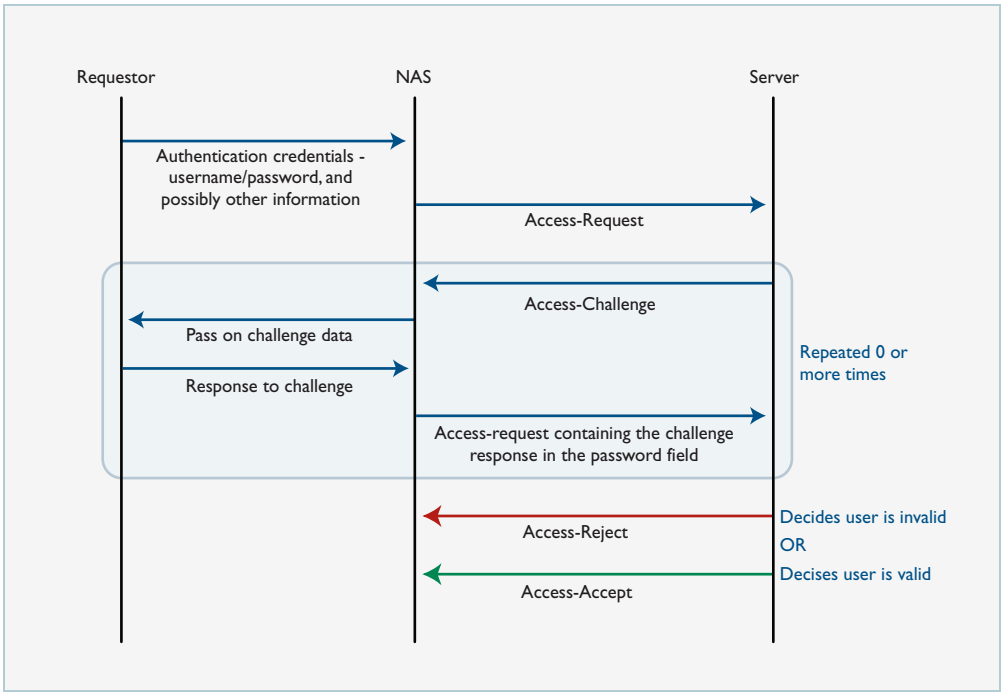
RADIUS packets

The RADIUS RFCs define the RADIUS packet types and attributes. RADIUS authentication is defined by RFC2058, RFC2138, RFC2865, and RFC2868. RADIUS accounting is defined by RFC2059, RFC2139, RFC2866, and RFC2867. These RADIUS RFCs define over fifty attributes and six packets types (**Access-Request, Access-Accept, Access-Reject, Accounting-Request, Accounting-Response, Access-Challenge**).

A RADIUS exchange is initiated by the NAS when a user requests access to the NAS. The NAS obtains the user authentication data adds them into a RADIUS **Access-Request** packet type and sends the RADIUS **Access-Request** packet to the RADIUS server.

- If a RADIUS server has not been configured for authentication request from a NAS then it will silently discard an **Access-Request** packet from it.
- If the RADIUS server accepts the request from the NAS it considers the authentication data provided in the **Access-Request** packet. The RADIUS server may verify the user from its own database or it may connect to other servers to verify.
- If the RADIUS server decides that the user is not allowed access to the NAS it responds to the NAS with an **Access-Reject** packet and the NAS will block the user.
- If the RADIUS server decides that the user is valid but needs more information to verify that the user is not an impostor, it may send an **Access-Challenge** packet to the NAS that the NAS forwards to the user. The NAS forwards the user response to the **Access-Challenge** packet in an **Access-Request** packet to the RADIUS server to accept or reject to allow or deny NAS user access.
- If the RADIUS server rejects the user it sends an **Access-Reject** packet to the NAS.
- If the RADIUS server accepts the user it sends an **Accept-Accept** packet to the NAS. The **Accept-Accept** packet to the NAS contains attributes that the NAS can apply.

Figure 11: Example showing an exchange from a requestor to a NAS to a RADIUS server



RADIUS attributes

Attributes are carried within RADIUS packets in the form of TLVs (Type Length Values). Every attribute has an attribute ID number in the Type field of the TLV. The Length field holds a one-byte number that represents then length of the TLV. The Value field holds the value of the attribute. Each attribute is identified by its RFC-defined name, followed by its attribute ID in parenthesis. For example:

- **User-name(1)**

  User-names are strings of at least three characters and have a maximum of 253 characters, which is the upper limit on all RADIUS attributes.

- **User-password(2)**

  User-passwords are encrypted using an MD5 hash of the password, the NAS's shared secret with the RADIUS server, and a request authenticator value. User-passwords can either be used at the initial authentication attempt or in response to an Access-Challenge packet type from the RADIUS server to the NAS.

- **CHAP-password(3)**

  CHAP-passwords are used if the NAS is using CHAP to authenticate the user, and doesn't receive the use the user's password but sends the CHAP response to the RADIUS server instead. The CHAP password is an encrypted string that is an MD5 hash of the password and challenge value sent by the user.

- **Framed-IP-Address(8)**

Used for dial-in user making PPP connections to the NAS who are dynamically allocated an IP address that they can use for the duration of their connect. The RADIUS server sends the Framed-IP-Address to the NAS to allocate.

- **Service-Type(6)**

  Used when the NAS is authenticating a user who wants to open a management session on the NAS, and is sent by the RADIUS server back to the NAS in an Access-Accept type packet to indicate the level of access the NAS gives a user. Service-Type(6) is mapped to a Privileged management session for AlliedWare Plus.

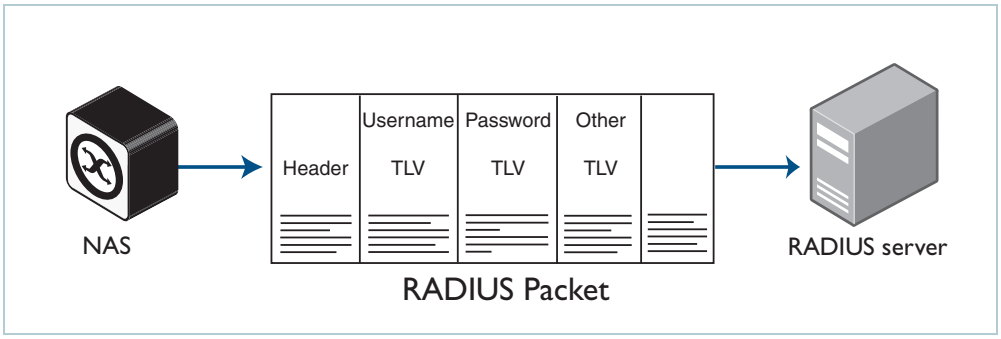
- **NAS-Port-Type(61)**

  Identifies the type of port on which the user is accessing the NAS. The NAS-Port-Type(61) attribute is sent by the NAS to the RADIUS server in Access-Request type packet, so the RADIUS server may use it to choose access type. For 802.1X sessions, the NAS-Port-Type sent by the NAS is Ethernet (15).

- **802.1X VLAN assignment uses:**

  Tunnel-Type(64), Tunnel-Medium-Type(65), Tunnel-Private-Group-ID(81), Egress-VLANID(56), and Egress-VLAN-Name(58) attributes (specified in RFC4675 used to specify 802.1Q tagged and untagged VLAN assignments with LLDP-MED/Voice-VLAN).

Figure 12: Example showing TLVs in a RADIUS packet from a NAS to a RADIUS server



For a full list of attributes see the "Defined RADIUS Attributes List" on page 36.

RADIUS security

RADIUS is used for network security and carries user authentication information, so can be a target for security attacks. To counter threats there are four elements to RADIUS security:

- **Shared secret**
- **Authenticator**
- **Password encryption**
- **RADIUS over TLS**

Shared secret

Every NAS and server are configured with a pre-shared key, called the **shared secret**, which is a key string, with no particular format of at least 16 characters.

The protocol has no method for choosing and sharing the secret between the NAS and the server. The secret must be manually generated and separately configured on the NAS and on the server.

The shared secret itself never appears in any RADIUS packets. It is used as an input to the algorithms used for creating encrypted values that are carried in the packets.

Authenticator

The authenticator is a random 16-byte value generated by the NAS. The NAS creates a new authenticator value for each **Access-Request** that it sends.

The response packets that come back from the server contain a value called the Response Authenticator. This is a value that is created by performing an MD5 hash on a string that is created by concatenating the packet type identifier, Session ID, Authenticator sent in the request packet, Attribute fields in the packet, Shared secret that the server shares with the NAS to which it is responding.

When the NAS receives the response packet, it performs the same hash on the same values, and verifies that it comes up with the same result. If not, then it must assume that the response packet has been spoofed, and silently discards it.

Password encryption

The value placed in the user-password TLV of an **Access-Request** packet is not simply an exact copy of the password sent from the requestor to the NAS.

The NAS concatenates together the shared secret and the authenticator that it has randomly generated for this request and then performs manipulations (MD5, XOR) on that concatenation, and the password to create the value to go into password TLV.

When the server validates the **Access-Request**, it retrieves the user's password from the user credentials database, and performs the same manipulation upon that password. If the result matches the value in the user-password field of the **Access-Request**, then the password sent by the requestor is deemed to be correct.

RADIUS over TLS

RadSec is an extension to the RADIUS authentication protocol that uses Transport Layer Security (TLS) as the transport protocol. It provides improved security over the standard RADIUS protocol by:

- ensuring that protocol messages are encrypted, preventing external entities from snooping usernames and passwords
- using X.509 certificate chains for identity validation and encrypted key exchange

AlliedWare Plus uses a **RadSecProxy** to act as an intermediary between local applications that use standard RADIUS UDP datagrams and external entities that use RadSec. RadSecProxy converts UDP datagrams into messages carried over TLS, and vice versa.

The TLS connection supports secure renegotiation, and if the connection is broken unintentionally then it recovers automatically after restoration of the connection. There is no need to set shared-secret between RadSec proxy and secure RADIUS server, since they are authenticated using X.509 certificates.

RadSecProxy on AlliedWare Plus can be configured as a client to communicate with an external secure RADIUS server via TLS, or as a server to provide secure RADIUS service for other devices.

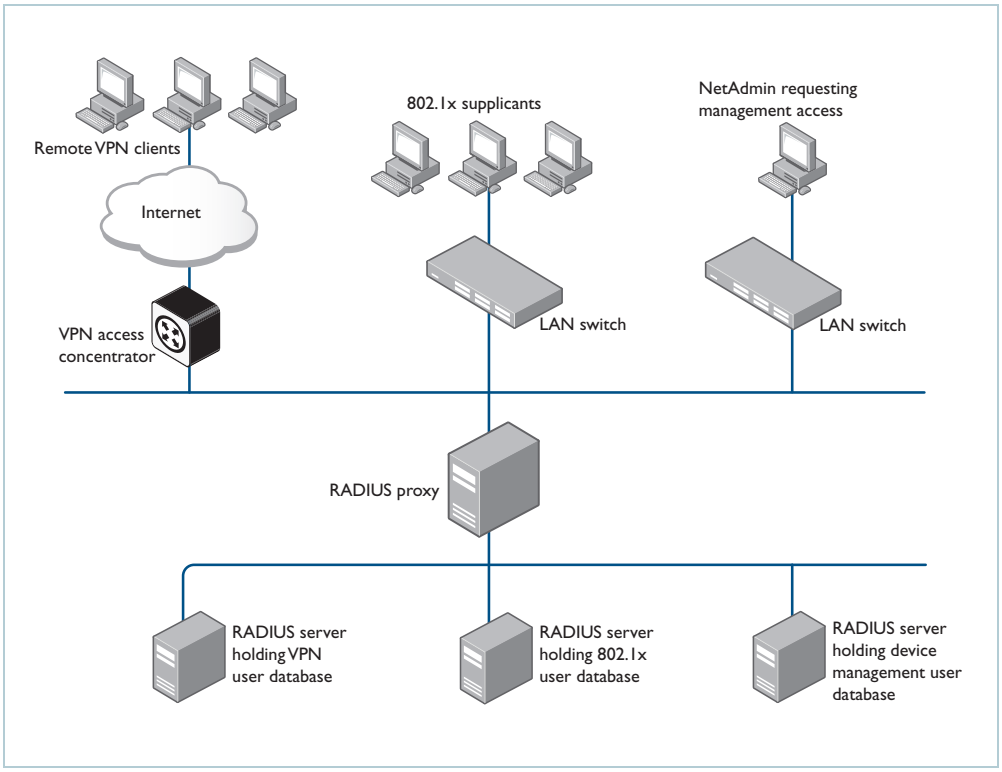
RADIUS proxy

It is possible to configure a RADIUS proxy server so that remote RADIUS servers hold the user database and validate NAS RADIUS requests.

- The NAS sends a RADIUS request to the RADIUS proxy server.
- The proxy server forwards the request to the first available RADIUS server.
- The RADIUS server processes the request and sends the response back to the proxy server.
- The proxy server then forwards the response to the NAS with an accept or reject.

There are a variety of situations where a RADIUS proxy is useful. For example, multiple RADIUS servers could be configured to each hold a different user database for a specific purpose e.g. one for authenticating switch management sessions, one for authenticating VPN connections, and one for authenticating 802.1X sessions. In this situation it is convenient to use a single IP address on all the NASs to point to the RADIUS proxy server. This server then forwards the request to the correct RADIUS server holding the relevant user database.

Figure 13: Example showing RADIUS proxy



RADIUS accounting

There are only two types of RADIUS accounting packet: **Accounting-Request** and **Accounting-Response**.

The **Accounting-Request** packets are always sent from the NAS to the server. The **Accounting-Response** packets are always sent from the server to the NAS, and are effectively ACKs of the **Accounting-Request** packets.

The **Accounting-Request** packets always carry the attribute **Acct-Status-Type**. The most commonly used values of this attribute are:

- **Start** – which denotes a packet marking that a session is beginning
- **Stop** – which denotes a packet marking that a session is ending
- **Interim update** – packets sent periodically during the session to give update reports on the statistics that are being collected.

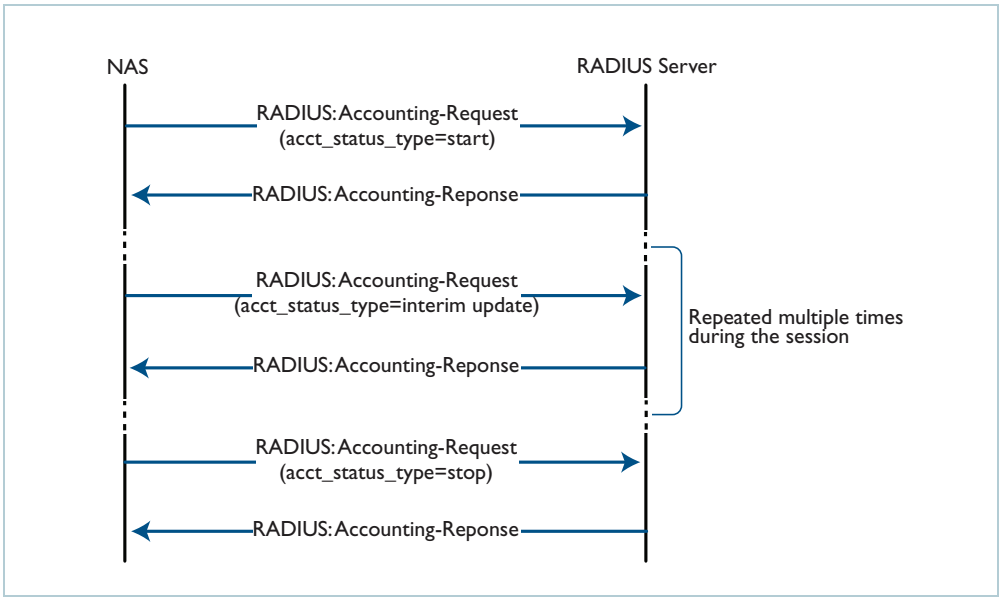
The statistics that can be exchanged in the session are:

- Input Octets
- Input Packets
- Output Octets
- Output Packets
- Session Duration

There is no requirement to exchange all these statistics – NAS implementations are at liberty to choose which statistics they will send. Each of these statistics has a corresponding attribute type. The attributes are sent in Interim-Update and Stop accounting request packets.

Each accounting session has a unique session ID, which is chosen by the NAS. The session ID is carried in an **Acct-Session-Id** attribute, that should be present in every packet involved in the session. The accounting packets typically do not use the same UDP port as the authentication packets. The default port for RADIUS accounting is 1813.

Figure 14: Example showing RADIUS accounting between a NAS and a RADIUS server



RADIUS Configuration

This section describes how to configure RADIUS with the available AAA commands.

RADIUS is often used in a variety of networks that need high security while maintaining access for remote users. RADIUS is suitable for the following networks that require access security:

- Networks with multiple-vendor access servers, each supporting RADIUS. For example, access servers from several vendors use a single RADIUS server-based security database.
- Networks in which a user may access a single service. Using RADIUS, you can control user access to a single host, or to a single utility such as Telnet.
- Networks that require accounting. You can use RADIUS accounting independent of RADIUS authentication. The RADIUS accounting functions allow data to be sent at the start and end of services, indicating the amount of resources (time, packets, bytes) used.

Switch configuration tasks

To configure RADIUS on your switch or access server, you must perform the following tasks:

- Use the **aaa authentication** command to define method lists for RADIUS authentication.
- Use authentication commands to enable the defined method lists to be used.

The following configuration tasks are optional:

- You can use the **aaa group server** command to group selected RADIUS hosts for specific services.
- You can use the **aaa accounting login** command to enable accounting for RADIUS connections.

This section describes how to set up RADIUS for authentication and accounting on your network, and includes the following sections:

- Switch to RADIUS server communication (Required), on page 13
- Configuring AAA server groups (Optional), on page 15
- Configuring AAA server groups with Deadtime (Optional) on page 16
- Specifying RADIUS authentication on page 17
- Specifying RADIUS accounting (Optional) on page 17

For RADIUS configuration examples using the commands in this guide, refer to the section "RADIUS Proxy Configuration" on page 18.

Switch to RADIUS server communication

The RADIUS host is normally a multiuser system running RADIUS server software from a software provider. Switch to RADIUS server communication has several components:

- Host name or IP address
- Authentication destination port
- Accounting destination port
- Timeout period
- Retransmission value
- Key string
- VRF

RADIUS security servers are identified on the basis of their host name or IP address, host name, VRF and specific UDP port numbers, or IP address and specific UDP port numbers. The combination of the IP address, VRF and UDP port number creates a unique identifier, allowing different ports/VRFs to be individually defined as RADIUS hosts providing a specific AAA service. This unique identifier enables RADIUS requests to be sent to multiple UDP ports or VRFs on a server at the same IP address.A RADIUS server and a switch use a shared secret text string to encrypt passwords and exchange responses.

To configure RADIUS using the AAA security commands, you must specify the host running the RADIUS server daemon and a secret text string that it shares with the switch, which you can specify using the **key** parameter in the **radius-server host** command.

The timeout, retransmission, and encryption key values are configurable globally for all RADIUS servers, on a per-server basis, or in some combination of global and per-server settings. To apply these settings globally to all RADIUS servers communicating with the switch, use the three global commands: **radius-server timeout**, **radius-server retransmit**, and **radius-server key**. To apply these values on a specific RADIUS server, use the **radius-server host** command

Note: You can configure both global and per-server timeout, retransmission, and key value commands simultaneously on the same Network Access Server. If both global and per-server functions are configured on a switch, the per-server timer, retransmission, and key value commands override global timer, retransmission, and key value commands

To configure per-server RADIUS server communication, use the following command in the Global Configuration mode:

MODE AND COMMAND	COMMAND PURPOSE
awplus(config)# radius-server host {<*hostname*>| <*ip-address*>} [auth-port <*port-number*>] [acct-port <*port-number*>] [timeout <*seconds*>] [retransmit <*retries*>] [key<*string*>]	Specifies the IP address or host name of the remote RADIUS server host and assigns authentication and accounting destination UDP port numbers. Use the **auth-port** <*port-number*> option to configure a specific UDP port on this RADIUS server to be used solely for authentication. Use the **acct-port** <*port-number*> option to configure a specific UDP port on this RADIUS server to be used solely for accounting. To configure the network access server to recognize more than one host entry associated with a single IP address, simply repeat this command as many times as necessary, making sure that each UDP port number is different. Set the timeout, retransmit, and encryption key values to use with the specific RADIUS host. If no timeout is set, the global value is used; otherwise, enter a value in the range 1 to 1000. If no retransmit value is set, the global value is used; otherwise enter a value in the range 1 to 1000. If no key string is specified, the global value is used.
awplus(config)# radius-server host {<*hostname*>| <*ip-address*>}[vrf <*name*>] [auth-port <*port-number*>] [acct-port <*port-number*>]| [timeout <*seconds*>] [retransmit <*retries*>] [key<*string*>]	To configure per-server RADIUS server communication, use the following command in the Global Configuration mode.

To configure global communication settings between the switch and a RADIUS server, use the following **radius-server** commands in the Global Configuration mode:

MODE AND COMMAND	COMMAND PURPOSE
awplus(config)# radius-server key <*key*>	Specifies the shared secret text string used between the switch and a RADIUS server (no default is set).
awplus(config)# radius-server retransmit <*retries*>	Specifies how many times the switch transmits each RADIUS request to the RADIUS server before giving up (the default is 3).
awplus(config)# radius-server timeout <*seconds*>	Specifies for how many seconds a switch waits for a reply to a RADIUS request before retransmitting the request.
awplus(config)# radius-server deadtime <*minutes*>	Specifies for how many minutes a RADIUS server that is not responding to authentication requests is passed over by requests for RADIUS authentication.

Configuring AAA server groups

Configuring the switch to use AAA server groups provides a way to group existing server hosts. This allows you to select a subset of the configured server hosts and use them for a particular service. A server group is used in conjunction with a global server-host list. The server group lists the IP addresses of the selected server hosts.

Server groups also can include multiple host entries for the same server, as long as each entry has a unique identifier. The combination of an IP address, VRF and a UDP port number creates a unique identifier, allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service.

Note: Radius Proxy does not support VRF.

To define a server host with a server group name, enter the following commands in the Global Configuration mode. The listed RADIUS server must exist in the Global Configuration mode:

MODE AND COMMAND	COMMAND PURPOSE
awplus(config)# radius-server host {<*hostname*>| <*ip-address*>} [auth-port <*port-number*>] [acct-port <*port-number*>] [timeout <*seconds*>] [retransmit <*retries*>] [key <*string*>]	Specifies and defines the IP address of the server host before configuring the AAA server-group.
awplus(config-if)# aaa group server <*group-name*>	Defines the AAA server group with a group name. This command puts the switch in server group sub configuration mode.

MODE AND COMMAND	COMMAND PURPOSE
awplus(config-sg)# server {<*hostname*>|<*ip-address*>} [auth-port <*port-number*>] [acct-port <*port-number*>]	Associates a particular RADIUS server with the defined server group. Each security server is identified by its IP address and UDP port number. Repeat this step for each RADIUS server in the AAA server group. Each server in the group must be defined previously using the radius-server host command.

Configuring AAA server groups with deadtime

After you have configured a server host with a server name, you can use the **deadtime (RADIUS server group)** command to configure each server per server group. Configuring deadtime within a server group allows you to direct AAA traffic to separate groups of servers that have different operational characteristics.

Configuring **deadtime** is no longer limited to a global configuration. A separate timer has been attached to each server host in every server group. When a server is found to be unresponsive after numerous retransmissions and time-outs, the server is assumed to be dead. The timers attached to each server host in all server groups are triggered. In essence, the timers are checked and subsequent requests to a server, once it is assumed to be dead, are directed to alternate servers, if configured. When the network access server receives a reply from the server, it checks and stops all configured timers, if running, for that server in all server groups.

If the timer has expired, only the server to which the timer is attached is assumed to be alive. This becomes the only server that can be tried for later AAA requests using the server groups to which the timer belongs.

Note: Since one server has different timers and may have different deadtime values configured in the server groups, the same server may in the future have different states, dead and alive, at the same time. To change the state of a server, you must start and stop all configured timers in all server groups.

The size of the server group will be increased because of the addition of new timers and the deadtime attribute. The overall impact of the structure depends on the number and size of the server groups and how the servers are shared among server groups in a specific configuration.

To configure deadtime within a server group, use the following commands beginning in the Global Configuration mode:

MODE AND COMMAND	COMMAND PURPOSE
awplus(config)# aaa group server radius group1	Defines a RADIUS type server group.
awplus(config-sg)# deadtime 1	Configures and defines a deadtime value in minutes.
awplus(config-sg)# exit	Exits server group configuration mode.

Specifying RADIUS authentication

After you have identified the RADIUS server and defined the RADIUS authentication key, you must define method lists for RADIUS authentication. Because RADIUS authentication is facilitated through AAA, you must enter the **aaa authentication login** command, specifying RADIUS as the authentication method.

Specifying RADIUS accounting

The AAA accounting feature enables you to track the services users are accessing as well as the amount of network resources they are consuming. Because RADIUS accounting is facilitated through AAA, you must issue the **aaa accounting login** command, specifying RADIUS as the accounting method.

Monitoring and maintaining RADIUS

To monitor and maintain RADIUS, use the following commands in Privileged Exec mode:

MODE AND COMMAND	COMMAND PURPOSE
`awplus# debug radius`	Displays information associated with RADIUS.
`awplus# show radius statistics`	Displays the RADIUS statistics for accounting and authentication packets.

RADIUS Proxy Configuration

It is possible to configure a RADIUS proxy server so that remote RADIUS servers hold the user database and validate NAS RADIUS requests.

- The NAS sends a RADIUS request to the RADIUS proxy server.
- The proxy server forwards the request to the first available RADIUS server.
- The RADIUS server processes the request and sends the response back to the proxy server.

The proxy server then forwards the response to the NAS with an accept or reject.

Basic Configuration

This example outlines a minimal RADIUS proxy configuration.

Step 1: **Change to RADIUS Proxy Configuration Mode**

```
awplus#configure terminal
awplus(config)#radius-server proxy-server
awplus(config-radproxy)#
```

Step 2: **Add upstream RADIUS server/s**

This is the server, or servers, that the proxy requests will be forwarded to.

To add two upstream servers, ***192.168.1.1*** and ***192.168.2.2***, with secret key strings ***string1*** and ***string2***, use the commands:

```
awplus(config-radproxy)#server 192.168.1.1 key secret1
awplus(config-radproxy)#server 192.168.2.2 key secret2
```

- You can configure more than one upstream server.
- The request will be sent to the first available server.
- If the first one is not available, the request will be sent to the second one.

Step 3: **Add permitted NAS client(s)**

Only RADIUS requests from these clients will be sent to the upstream server.

To add client ***10.37.236.11*** with shared key ***myKey,*** use the command:

```
awplus(config-radproxy)#nas 10.37.236.11 key myKey
```

Step 4: **Enable RADIUS proxy**

```
awplus(config-radproxy)#proxy enable
```

RADIUS proxy server using non-standard ports

If the upstream RADIUS server is listening on ports other than the standard 1812 for authentication and 1813 for accounting, you can configure the RADIUS proxy server to use these ports.

For example, upstream server ***192.168.1.1*** is listening on port ***2044*** for authorization and port ***2055*** for accounting requests. Enter the commands on the proxy server:

```
awplus#configure terminal
awplus(config)#radius-server proxy-server
awplus(config-radproxy)#server 192.168.1.1 key secret1 auth-port 2044 acct-port
2055
```

RADIUS proxy authorization and accounting ports

By default, the RADIUS proxy server uses ports 1812 and 1813 to listen for authorization and accounting requests. You can change these port numbers using the following commands:

```
awplus#configure terminal
awplus(config)#radius-server proxy-server
awplus(config-radproxy)#proxy auth-port 2044 acct-port 2055
```

RADIUS proxy rules

You can configure rules to match a RADIUS request based on a **realm** or a RADIUS packet **attribute**. If a match is found then the servers defined in the rule will be used as the upstream servers.

A **realm** can be any of the following formats:

- username@domain.com
- username%domain.com
- domain/username
- domain\username

Any RADIUS **attribute** from the request packet can be examined to determine the upstream server. Use the **help radius-attribute** command to get a list of all RADIUS attributes, see "Defined RADIUS Attributes List" on page 36

Example 1: Configure a rule with id ***10*** that matches a realm ***myuser@abcd.com***, ***myuser@xyz.com***, ***myuser@xyz.ac.nz*** to use the upstream server ***192.168.1.1***.

```
awplus#configure terminal
awplus(config)#radius-server proxy-server
awplus(config-radproxy)#rule 10 realm myuser@* server 192.168.1.1
```

Example 2: Configure the same rule, as per example 1, where the upstream server is listening on ports ***2044*** and ***2055***.

```
awplus#configure terminal
awplus(config)#radius-server proxy-server
awplus(config-radproxy)#rule 10 realm myuser@* server 192.168.1.254 auth-port
2044 acct-port 2055
```

Example 3: Configure a rule with id ***20*** that matches RADIUS attribute ***user-name*** as ***myuser*** to use the upstream server ***192.168.2.2***.

```
awplus#configure terminal
awplus(config)#radius-server proxy-server
awplus(config-radproxy)#rule 20 attribute user-name myuser server 192.168.2.2
```

RADIUS attribute help

The help **radius-attribute** command gives a list of all available attributes.

```
awplus#help radius-attribute
Standard Attributes:
 1      User-Name
 2      User-Password
 3      CHAP-Password
 4      NAS-IP-Address
 5      NAS-Port
 6      Service-Type
...
```

Working with RADIUS proxy groups

Step 1: **Create a RADIUS proxy group**

```
awplus#configure terminal
awplus(config)#radius-server proxy-server
awplus(config-radproxy)#group atlnz
awplus(config-radproxy-group)#
```

Step 2: **Add servers to the group**

Each server should already be defined using the **server** command.

```
awplus(config-radproxy-group)#server 192.168.1.1
awplus(config-radproxy-group)#server 192.168.2.2
awplus(config-radproxy-group)#exit
awplus(config-radproxy)
```

Step 3: **Configure a RADIUS proxy rule to use the group**

Configure a rule with id ***10*** that matches a realm ***myuser@abcd.com***, ***myuser@xyz.com***, ***myuser@xyz.ac.nz*** to use the group of upstream servers ***atlnz***.

```
awplus(config-radproxy)#rule 10 realm myuser@* group atlnz
```

Configure a source IP address

Use the **radius proxy source-interface** command to configure the source IP address of each outgoing RADIUS packet. The RADIUS packets will use the specified IP address or the IP address of the specified interface. If the interface is down, or there is no IP address on the interface, then the source IP address will be the IP address of the interface the packets leave on.

To set the source IP address to ***192.168.1.1*** for all outgoing RADIUS packets from the proxy server, use the following commands:

```
awplus#configure terminal
awplus(config)#radius-server proxy-server
awplus(config-radproxy)#source-interface 192.168.1.1
```

To use the IP address of the interface ***vlan1*** as the source IP for outgoing RADIUS packets from the proxy server, use the following commands:

```
awplus#configure terminal
awplus(config)#radius-server proxy-server
awplus(config-radproxy)#source-interface vlan1
```

Use the **no** variant of this command to remove the source interface configuration. The source IP address in outgoing proxy RADIUS packets will then be the IP address of the interface from which the packets are sent.

```
awplus#configure terminal
awplus(config)#radius-server proxy-server
awplus(config-radproxy)#no source-interface
```

RADIUS server timeout

An upstream RADIUS server is considered "dead" if it does not respond to a RADIUS request within a specified timeout period. By default this is set to 30 seconds. Set this timeout value using the **server timeout** command.

Use the following commands to set the server timeout value to 60 seconds

```
awplus#configure terminal
awplus(config)#radius-server proxy-server
awplus(config-radproxy)#server timeout 60
```

RADIUS server deadtime

The deadtime period is the amount of time a server is considered “dead” before its:

- status is changed to “alive” if status-check is disabled or
- a check status is initiated if status-check is enabled.

The default value is 300 seconds. Set this dead time value using the **server deadtime** command.

Use the following commands to change the deadtime to ***100*** seconds:

```
awplus#configure terminal
awplus(config)#radius-server proxy-server
awplus(config-radproxy)#server deadtime 100
```

RADIUS server status check

RADIUS proxy server can send a status check message to a dead server. This feature is disabled by default and must be enabled on a per server basis.

- If status check is set then a dead server’s status will change to ‘Alive’ if it responds favourably to a status check.
- If status check is not set, a dead server’s status changes to ‘Alive’ after the specified deadtime, irrespective of the actual state of the server.

This feature is only valid if the upstream server supports status check.

To enable status check on th upstream server ***192.168.1.1*** use the following command:

```
awplus#configure terminal
awplus(config)#radius-server proxy-server
awplus(config-radproxy)#server 192.168.1.1 key secret1 status-check
```

Monitoring RADIUS proxy server

show radius proxy-server

This command shows all configured upstream RADIUS servers and their status. A server can be in 1 of 3 states:

- Unknown,
- Alive,
- Dead.

When the RADIUS proxy starts all the servers will be in an 'Unknown' state. When the first RADIUS packet is received by the proxy server and sent to the first server, the status will be changed depending on the availability of that server.

```
awplus#show radius proxy-server
                              Auth  Acct  Auth           Acct
Server Host/IP Address        Port  Port  Status         Status
-------------------------------------------------------------------------
192.168.1.1                   1812  1813  Alive          Unknown
192.168.2.2                   1812  1813  Unknown        Unknown
192.168.10.20                 1812  1813  Unknown        Unknown
```

The above output shows that the proxy server received a RADIUS authorization request and sent it to the first configured server, ***192.168.1.1***, which is ‘Alive’.

If another request arrives and ***192.168.1.1*** is unavailable, then the server status will change to 'Dead' after the specified **timeout** period. The RADIUS proxy server will then send subsequent authorization requests to the next available server ***192.168.2.2***. The output will look like as below:

```
awplus#show radius proxy-server
                              Auth  Acct  Auth           Acct
Server Host/IP Address        Port  Port  Status         Status
-------------------------------------------------------------------------
192.168.1.1                   1812  1813  Dead           Unknown
192.168.2.2                   1812  1813  Alive          Unknown
192.168.10.20                 1812  1813  Unknown        Unknown
```

show radius proxy-server group

Use this command to see a list of all configured RADIUS proxy groups and their members.

```
awplus#show radius proxy-server group
[Proxy Server Group atlnz]
                              Auth  Acct  Auth           Acct
Server Host/IP Address        Port  Port  Status         Status
-------------------------------------------------------------------------
192.168.1.1                   1812  1813  Alive          Unknown
192.168.2.2                   1812  1813  Unknown        Unknown

[Proxy Server Group mygroup]
                              Auth  Acct  Auth           Acct
Server Host/IP Address        Port  Port  Status         Status
-------------------------------------------------------------------------
192.168.10.20                 1812  1813  Unknown        Unknown
```

show radius proxy-server statistics

List various RADIUS proxy counters

```
awplus#show radius proxy-server statistics
RADIUS Proxy Statistics for Clients:
                     Auth                 Acct
-------------------------------------------------------------
Requests             4                    0
Responses            4                    0
Accepts              3                    -
Rejects              1                    -
Challenges           0                    -
Dup                  0                    0
Invalid              0                    0
Malformed            0                    0
Bad_Authenticator    0                    0
Dropped              0                    0
Unknown_Types        0                    0
Last_Packet          0                    0


RADIUS Proxy Statistics for Server 192.168.1.1:1812,1813:
                     Auth                 Acct
-------------------------------------------------------------
Requests             7                    0
Responses            7                    0
Accepts              4                    -
Rejects              3                    -
Challenges           0                    -
Dup                  0                    0
Invalid              0                    0
Malformed            0                    0
Bad_Authenticator    0                    0
Dropped              0                    0
Unknown_Types        0                    0
Timeouts             0                    0
Last_Packet          0                    0
```

```
RADIUS Proxy Statistics for Server 192.168.2.2:1812,1813:
                     Auth                 Acct
-------------------------------------------------------------
Requests             0                    0
Responses            0                    0
Accepts              0                    -
Rejects              0                    -
Challenges           0                    -
Dup                  0                    0
Invalid              0                    0
Malformed            0                    0
Bad_Authenticator    0                    0
Dropped              0                    0
Unknown_Types        0                    0
Timeouts             0                    0
Last_Packet          0                    0


RADIUS Proxy Statistics for Server 192.168.10.20:1812,1813:
                     Auth                 Acct
-------------------------------------------------------------
Requests             0                    0
Responses            0                    0
Accepts              0                    -
Rejects              0                    -
Challenges           0                    -
Dup                  0                    0
Invalid              0                    0
Malformed            0                    0
Bad_Authenticator    0                    0
Dropped              0                    0
Unknown_Types        0                    0
Timeouts             0                    0
Last_Packet          0                    0
```

RADIUS Change of Authorization (CoA)

From version 5.5.1-1.1 onwards, AlliedWare Plus supports RADIUS Change of Authorization (CoA) to change a supplicant's VLAN or terminate a supplicant's session.

RADIUS CoA provides a mechanism to dynamically change a supplicant's session characteristics after they have been authenticated. RADIUS CoA is an extension to the RADIUS protocol and is defined in RFC5176.

For an explanation of CoA, step-by-step configuration instructions, and an example, see the AAA and Port Authentication Feature Overview and Configuration Guide.

RADIUS Configuration Examples

The following sections provide RADIUS configuration examples:

- RADIUS authentication on page 26
- Single RADIUS server configuration on page 27
- Multiple RADIUS server configuration on page 27
- RADIUS server group configuration on page 28
- RADIUS server configuration using server groups on page 28
- RADIUS over TLS configuration

RADIUS authentication

Example The following example shows how to configure the switch to authenticate using RADIUS.

Output 1: Sample RADIUS authentication to configure the switch to authenticate users

```
!
radius-server host 172.10.10.1
radius-server key radiuspass
username newuser password newpass
aaa authentication login admin
!
```

The lines in this example RADIUS authentication and accounting configuration are defined as follows:

- The **radius-server host** command defines the IP address of the RADIUS server host.
- The **radius-server key** command defines the shared secret text string between the network access server and the RADIUS server host.
- The **aaa authentication login** command defines a method list named **admin** for login authentication.

Example The following example shows how to configure the switch to authenticate logins using RADIUS.

Output 2: Sample RADIUS authentication to authenticate logins

```
!
aaa authentication login radius-login group radius
!
```

This sample RADIUS authentication configuration is defined as follows:

- The **aaa authentication login radius-login group radius** command configures the switch to use RADIUS for authentication at the login prompt.

Example The following example shows how to configure the authentication method to verify a username and password at login. In this example, if a username is entered at the username prompt, that username is used for authentication.

Output 3: Sample RADIUS authentication to verify a username and password

```
!
aaa authentication login default group radius
radius-server host 172.10.10.1 auth-port 1812 acct-port 1813
!
```

The lines in this sample RADIUS authentication configuration are defined as follows:

- The **aaa authentication login default group radius** command specifies that the username and password are verified by RADIUS.
- The **radius-server host 172.10.10.1 auth-port 1812 acct-port 1813** command specifies the IP address of the RADIUS server host, the UDP destination port for authentication requests, and the UDP destination port for accounting requests.

Single RADIUS server configuration

Example The following example shows how to configure server-specific timeout, retransmit, and key values for the RADIUS server with IP address 172.2.2.2.

Output 4: Single RADIUS server sample configuration

```
!
radius-server host 172.2.2.2 timeout 5 retransmit 5 key 10
!
```

Multiple RADIUS server configuration

Example The following example shows how to configure two RADIUS servers with specific timeout, retransmit, and key values. The **radius-server retransmit** command changes the global retransmission value to 4 for all RADIUS servers. The **radius-server host** command configures specific timeout, retransmission, and key values for the RADIUS server hosts with IP addresses **172.2.2.2** and **172.1.1.1**

Output 5: Multiple RADIUS server sample configuration

```
!
! Enable and configure radius authentication and accounting
! services on the switch:
!
aaa authentication login default group radius
aaa accounting default start-stop group radius
!
! Change the retransmission value for all RADIUS servers:
!
radius-server retransmit 4
!
! Configure per-server specific timeout, retransmission, and
! key values. Change the default auth-port and acct-port
! values.
!
radius-server host 172.2.2.2 auth-port 1645 acct-port 1646 timeout 3
retransmit 3 key radkey
!
! Configure per-server specific timeout and key values. This
! server uses the global retransmission value.
!
radius-server host 172.1.1.1 timeout 6 key rad123
!
```

RADIUS server group configuration

Example The following example shows how to create server group **group2** with three RADIUS server members, each with the same IP address but with unique authentication and accounting ports.

Output 6: RADIUS server group sample configuration using the same IP address

```
!
aaa group server radius group2
  server 172.1.1.1 auth-port 1645 acct-port 1646
  server 172.1.1.1 auth-port 1812 acct-port 1813
  server 172.1.1.1 auth-port 2000 acct-port 2001
!
```

RADIUS server configuration using server groups

The following example shows how to configure the network access server to recognize two different RADIUS server groups.

One of these groups, **group1**, has two different host entries on the same RADIUS server configured for the same services. The second host entry configured acts as fail over backup to the first one. Each group is individually configured for **deadtime**; **deadtime** for **group1** is one minute, and **deadtime** for **group2** is two minutes.

Output 7: Multiple RADIUS servers using server groups sample configuration

```
!
! The following command configures default RADIUS parameters:
!
aaa authentication login default group group1
!
! The following commands define the group1 RADIUS server group
! and associate servers with it and configures a deadtime of
! one minute:
!
aaa group server radius group1
  server 172.1.1.1 auth-port 1645 acct-port 1646
  server 172.2.2.2 auth-port 1812 acct-port 1813
  deadtime 1
!
! The following commands define the group2 RADIUS server group
! and associate servers with it and configures a deadtime of
! two minutes:
!
aaa group server radius group2
  server 172.2.2.2 auth-port 1812 acct-port 1813
  server 172.3.3.3 auth-port 2000 acct-port 2001
  deadtime 2
!
! The following commands configure the RADIUS attributes
! for each host entry associated with one of the defined
! server groups:
!
radius-server host 172.1.1.1 auth-port 1645 acct-port 1646
radius-server host 172.2.2.2 auth-port 1812 acct-port 1813
radius-server host 172.3.3.3 auth-port 2000 acct-port 2001
!
```

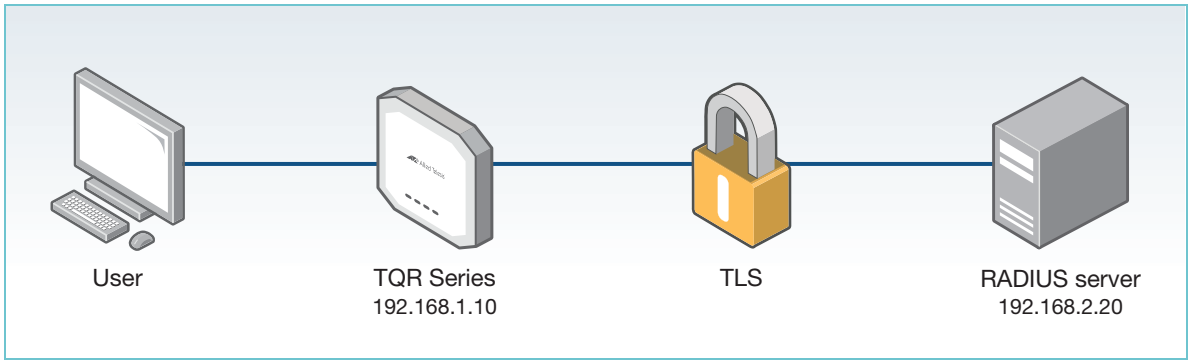
RADIUS over TLS configuration

RadSec example

From version 5.5.5-1.1 onwards, you can configure RADIUS over TLS for TQR Series devices. The following examples show how to configure a TQR Series device.

For the TQR Series, RadSec uses the command **radius-secure-proxy** to establish a TLS connection (because the server and NAS do not talk directly to each other). To configure Trustpoint, see the product's Command Reference.

Figure 15: Example showing a client and server on separate devices



Output 8: Example RADIUS over TLS for a TQR Series as a client

```
crypto pki trustpoint radsec
 enrollment terminal
!
radius-secure-proxy aaa
 server 192.168.2.20 name-check off
 server trustpoint radsec
```

Output 9: Example shows a TQR Series device configured as a RADIUS server

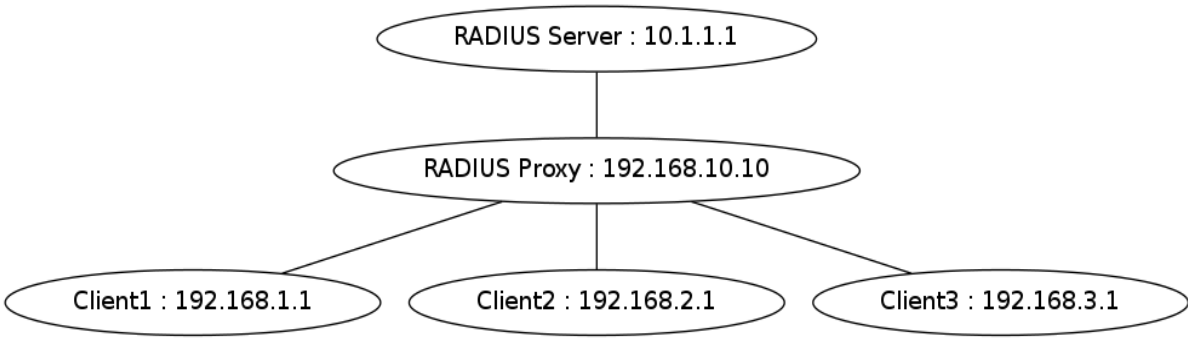
```
crypto pki trustpoint radsec
 enrollment terminal
!
radius-server local
 server enable
 server trustpoint local radsec
 nas 127.0.0.1 key dbSQ8EDlsS3xUeNxNmelt3ya+mDgdWCOegX15FooG8E= encrypted
 group admin
  vlan 10
  attribute Service-Type Administrative-User
 user manager encrypted password Ctr0hf2Bq//tGOwRBmZ1sVyuUWp775LFxfPG93x8WqQ=
group admin
!
radius-secure-proxy local-server
 no client name-check
 client 192.168.1.10
 client trustpoint radsec
```

RADIUS Proxy Configuration Examples

Simple proxy to a single RADIUS server

This example shows RADIUS proxy forwarding of all RADIUS requests from RADIUS Client1/2/3. The RADIUS proxy server sends back the response to each client.

Note: The RADIUS server configures the RADIUS proxy as a RADIUS server and does not know it is a proxy.



Local RADIUS server configuration on your AlliedWare Plus (AW+) device.

```
!
<IP: 10.1.1.1>
radius-server local
 server enable
 nas 192.168.10.10 key secret
 group admin
  attribute Service-Type Administrative-User
 user a password a group admin
 user b password b group admin
!
```

RADIUS proxy configuration.

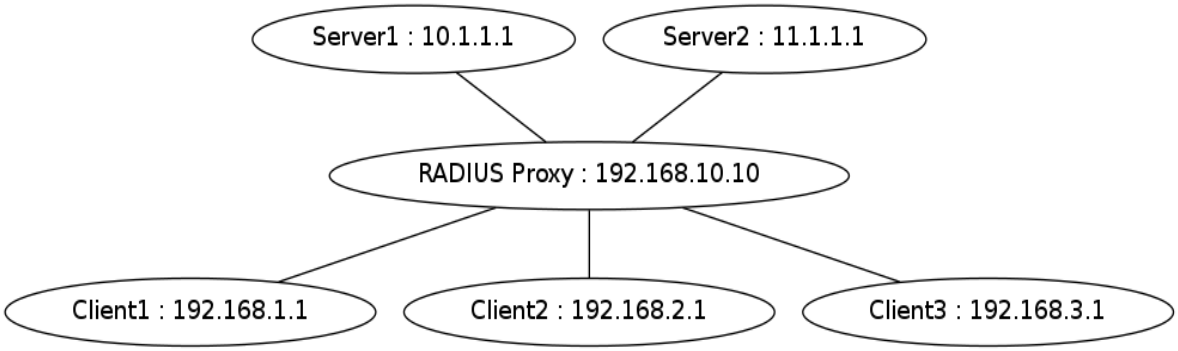
```
!
<IP: 192.168.10.10>
radius-server proxy-server
 server 10.1.1.1 key secret
 nas 192.168.1.1 key secretA
 nas 192.168.2.1 key secretB
 nas 192.168.3.1 key secretC
 proxy enable
!
```

RADIUS Client1 configuration with AW+ user login authentication and accounting.

```
!
<IP: 192.168.1.1>
radius-server host 192.168.10.10 key secretA
aaa authentication login default group radius
aaa accounting login default start-stop group radius
!
```

Rule-based proxy with multiple RADIUS servers

These examples show RADIUS proxy forwarding of RADIUS requests from RADIUS Client1/2/3 to a specified server based on a configured rule. The RADIUS proxy server sends back the response to each client.



Realm match

This example shows how to configure rules to choose a RADIUS server based on the realm of the RADIUS Request.

The following rules are configured:

- If the request is from the realm named ***abcd***, then send the request to RADIUS server 10.1.1.1. The realm name is stripped when the request is sent to the server.
- If the request is from the realm named ***xyz**** (i.e. a realm starting with ***xyz*** followed by any number of characters), then send the request to RADIUS server 10.1.1.1. The realm name is stripped when the request is sent to the server.
- If the request is from realms ****.com*** (e.g. ***abc.com***, ***123.com***), then send the request to RADIUS server 11.1.1.1. The realm name is not stripped when the request is sent to the server.
- If a request does not match any rule, then use the first alive server (i.e. use 10.1.1.1 if it's alive).

Note: The realm name appears in the User-Name attribute of a RADIUS Request packet. Valid formats for a realm are:

- username@realm
- username%realm
- realm/username
- realm\username

RADIUS proxy configuration.

```
!
radius-server proxy-server
 server 10.1.1.1 key secret
 server 11.1.1.1 key secret11
 nas 192.168.1.1 key secretA
 nas 192.168.2.1 key secretB
 nas 192.168.3.1 key secretC
 rule 1 realm abcd server 10.1.1.1
 rule 2 realm xyz* server 10.1.1.1
 rule 3 realm *.com nostrip server 11.1.1.1
 proxy enable
!
```

Attribute match

This example shows how to configure rules to choose a RADIUS server based on certain RADIUS attributes in the request packet.

The following rules are configured:

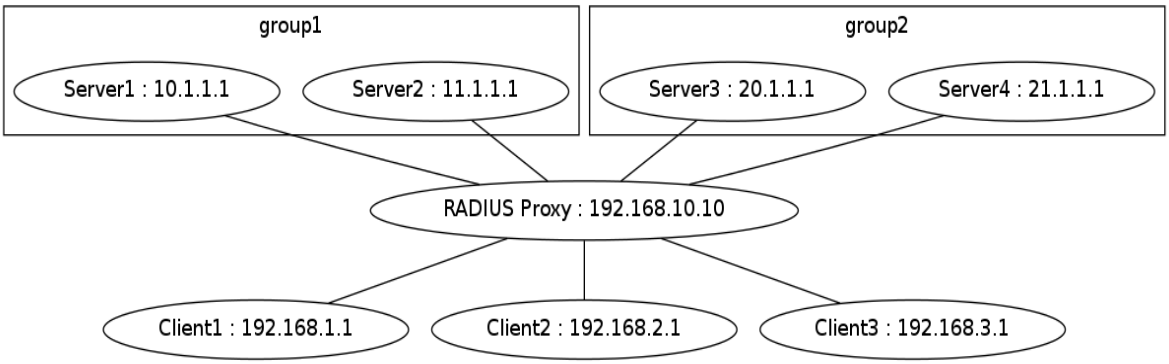
- If NAS-Identifier is ***XYZ***, then use RADIUS server 11.1.1.1
- If Called-Station-Id (SSID) is ***SSID: AP**X***, then use RADIUS server 11.1.1.1.
- If Called-Station-Id (SSID) starts with ***SSID: AP*** (e.g. "SSID: AP", "SSID: AP1"), then use RADIUS server 10.1.1.1.
- If Framed-IP-Address is ***192.168.100.****, then use RADIUS server 11.1.1.1.
- If a request does not match any rule, then use the first ‘Alive’ server.

RADIUS proxy configuration.

```
!
radius-server proxy-server
 server 10.1.1.1 key secret
 server 11.1.1.1 key secret11
 nas 192.168.1.1 key secretA
 nas 192.168.2.1 key secretB
 nas 192.168.3.1 key secretC
 rule 10 attribute NAS-Identifier XYZ server 11.1.1.1
 rule 20 attribute Called-Station-Id "SSID: AP\*\*X" server 11.1.1.1
 rule 30 attribute Called-Station-Id "SSID: AP*" server 10.1.1.1
 rule 40 attribute Framed-IP-Address 192.168.100.* server 11.1.1.1
 proxy enable
!
```

Rule-based proxy with multiple RADIUS server groups

These example shows RADIUS proxy forwarding of RADIUS requests from RADIUS Client1/2/3 to a specified server group based on a configured rule. The RADIUS proxy server sends back the response to each client.



The following rules are configured:

- If the User-Name attribute in the request starts with ***admin***, use the servers in the group ***group1***; use 10.1.1.1 if it's 'Alive' otherwise use 11.1.1.1.
- If the User-Name attribute in the request starts with ***test***, use the servers in the group ***group2***; use 20.1.1.1 if it's 'Alive' otherwise use 21.1.1.1.
- If a request does not match any rule, then use the first 'Alive' server (i.e. use 10.1.1.1 if it's 'Alive').

RADIUS proxy configuration.

```
!
radius-server proxy-server
 server 10.1.1.1 key secret
 server 11.1.1.1 key secret11
 server 20.1.1.1 auth-port 1645 acct-port 1646 key secret20
 server 21.1.1.1 auth-port 1645 acct-port 1646 key secret21
 group group1
  server 10.1.1.1
  server 11.1.1.1
 group group2
  server 20.1.1.1 auth-port 1645 acct-port 1646
  server 21.1.1.1 auth-port 1645 acct-port 1646
 nas 192.168.1.1 key secretA
 nas 192.168.2.1 key secretB
 nas 192.168.3.1 key secretC
 rule 100 attribute User-Name "admin*" group group1
 rule 101 attribute User-Name "test*" group group2
 proxy enable
!
```

Using Local RADIUS server for fallback

To provide a fallback RADIUS server, if other RADIUS servers are not reachable, add the Local RADIUS server to the end of the server list.

To do this:

1. Configure the Local RADIUS server with a different listening port to the RADIUS proxy to avoid conflict.
2. Add an administrative user ***manager*** to allow access to the network for troubleshooting on network failure.
3. Add the Local RADIUS server to the end of the RADIUS proxy's server list

RADIUS proxy configuration.

```
!
radius-server local
 server enable
 server auth-port 1234
 nas 127.0.0.1 key awplus-local-radius-server
 group admin
  attribute Service-Type Administrative-User
 user manager password manager-password group admin
!
radius-server proxy-server
 server 10.1.1.1 key secret
 server 11.1.1.1 key secret11
 server 127.0.0.1 auth-port 1234 key awplus-local-radius-server
 nas 192.168.1.1 key secretA
 nas 192.168.2.1 key secretB
 nas 192.168.3.1 key secretC
 proxy enable
!
```

Defined RADIUS Attributes List

This section contains a full list of valid attributes and pre-defined values that may be used in conjunction with the **attribute** command, to show or configure defined RADIUS attributes.

Table 11 lists all Standard attributes and values, Table 12 lists the Vendor-Specific attribute names and values.

More detailed information can be found in the following RFCs, defining the attributes and values for RADIUS server:

- RFC2865: Remote Authentication Dial In User Service (RADIUS)
- RFC2866: RADIUS Accounting
- RFC2867: RADIUS Accounting Modifications for Tunnel Protocol Support
- RFC2868: RADIUS Attributes for Tunnel Protocol Support
- RFC2869: RADIUS Extensions
- RFC3162: RADIUS and IPv6
- RFC3576: Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)
- RFC3580: IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines
- RFC4072: Diameter Extensible Authentication Protocol (EAP) Application
- RFC4372: Chargeable User Identity
- RFC4603: Additional Values for the NAS-Port-Type Attribute
- RFC4675: RADIUS Attributes for Virtual LAN and Priority Support
- RFC4679: DSL Forum Vendor-Specific RADIUS Attributes
- RFC4818: RADIUS Delegated-IPv6-Prefix Attribute
- RFC4849: RADIUS Filter Rule Attribute
- RFC5090: RADIUS Extension for Digest Authentication
- RFC5176: Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)
- RFC5447: Diameter Mobile IPv6: Support for Network Access Server to Diameter Server Interaction
- RFC5580: Carrying Location Objects in RADIUS and Diameter
- RFC5607: Remote Authentication Dial-In User Service (RADIUS) Authorization for Network Access Server (NAS) Management
- RFC5904: RADIUS Attributes for IEEE 802.16 Privacy Key Management Version 1 (PKMv1) Protocol Support

- RFC6519: RADIUS Extensions for Dual-Stack Lite
- RFC6572: RADIUS Support for Proxy Mobile IPv6
- RFC6677: Channel-Binding Support for Extensible Authentication Protocol (EAP) Methods
- RFC6911: RADIUS Attributes for IPv6 Access Networks
- RFC6929: Remote Authentication Dial-In User Service (RADIUS) Protocol Extensions
- RFC6930: RADIUS Attribute for IPv6 Rapid Deployment on IPv4 Infrastructures (6rd)
- RFC7055: A GSS-API Mechanism for the Extensible Authentication Protocol
- RFC7155: Diameter Network Access Server Application
- RFC7268: RADIUS Attributes for IEEE 802 Networks
- RFC7499: Support of Fragmentation of RADIUS Packets
- RFC7930: Larger Packets for RADIUS over TCP

Table 11: Standard RADIUS attributes

ATTRIBUTE ID AND NAME		VALUE TYPE/PRE-DEFINED VALUES
1	User-Name	string
2	User-Password	string
3	CHAP-Password	octets (Hexadecimal string followed by 0x)
4	NAS-IP-Address	ipaddr (IPv4 address)
5	NAS-Port	Integer
6	Service-Type	Integer. Valid values are: ■ Administrative-User (6) ■ Authenticate-Only (8) ■ Authorize-Only (17) ■ Callback-Administrative (11) ■ Callback-Framed-User (4) ■ Callback-Login-User (3) ■ Callback-NAS-Prompt (9) ■ Call-Check (10) ■ Framed-Management (18) ■ Framed-User (2) ■ Login-User (1) ■ NAS-Prompt-User (7) ■ Outbound-User (5)
7	Framed-Protocol	Integer. Valid values are: ■ ARAP (3) ■ Gandalf-SLML (4) ■ PPP (1) ■ SLIP (2) ■ X.75-Synchronous (6) ■ Xylogics-IPX-SLIP (5)
8	Framed-IP-Address	ipaddr (IPv4 address)
9	Framed-IP-Netmask	ipaddr (IPv4 address)

Table 11: Standard RADIUS attributes (continued)

ATTRIBUTE ID AND NAME		VALUE TYPE/PRE-DEFINED VALUES
10	Framed-Routing	integer. Valid values are: ■ Broadcast (1) ■ Broadcast-Listen (3) ■ Listen (2) ■ None (0)
11	Filter-Id	string
12	Framed-MTU	Integer
13	Framed-Compression	Integer. Valid values are: ■ IPX-Header-Compression (2) ■ None (0) ■ Stac-LZS (3) ■ Van-Jacobson-TCP-IP (1)
14	Login-IP-Host	IP Address
15	Login-Service	Integer. Valid values are: ■ LAT (4) ■ PortMaster (3) ■ Rlogin (1) ■ TCP-Clear (2) ■ TCP-Clear-Quiet (8) ■ Telnet (0) ■ X25-PAD (5) ■ X25-T3POS (6)
16	Login-TCP-Port	Integer. Valid values are: ■ Rlogin (513) ■ Rsh (514) ■ Telnet (23)
18	Reply-Message	string
19	Callback-Number	string
20	Callback-Id	string
22	Framed-Route	string
23	Framed-IPX-Network	IP address
24	State	octets (Hexadecimal string followed by 0x)
25	Class	octets (Hexadecimal string followed by 0x)
26	Vendor-Specific	Use the Vendor-specific Attribute Name. For valid values, see "Vendor-specific RADIUS attributes" on page 47.
27	Session-Timeout	Integer
28	Idle-Timeout	Integer
29	Termination-Action	Integer. Valid values are: ■ Default (0) ■ RADIUS-Request (1)
30	Called-Station-Id	string
31	Calling-Station-Id	string
32	NAS-Identifier	string
33	Proxy-State	octets (Hexadecimal string followed by 0x)

Table 11: Standard RADIUS attributes (continued)

ATTRIBUTE ID AND NAME		VALUE TYPE/PRE-DEFINED VALUES
34	Login-LAT-Service	string
35	Login-LAT-Node	string
36	Login-LAT-Group	octets (Hexadecimal string followed by 0x)
37	Framed-AppleTalk-Link	Integer
38	Framed-AppleTalk-Network	Integer
39	Framed-AppleTalk-Zone	string
40	Acct-Status-Type	Integer. Valid values are: ■ Accounting-Off (8) ■ Accounting-On (7) ■ Alive (3) ■ Failed (15) ■ Interim-Update (3) ■ Start (1) ■ Stop (2) ■ Tunnel-Link-Reject (14) ■ Tunnel-Link-Start (12) ■ Tunnel-Link-Stop (13) ■ Tunnel-Reject (11) ■ Tunnel-Start (9) ■ Tunnel-Stop (10)
41	Acct-Delay-Time	Integer
42	Acct-Input-Octets	Integer
43	Acct-Output-Octets	Integer
44	Acct-Session-Id	string
45	Acct-Authentic	Integer. Valid values are: ■ Diameter (4) ■ Local (2) ■ RADIUS (1) ■ Remote (3)
46	Acct-Session-Time	Integer
47	Acct-Input-Packets	Integer
48	Acct-Output-Packets	Integer

Table 11: Standard RADIUS attributes (continued)

ATTRIBUTE ID AND NAME		VALUE TYPE/PRE-DEFINED VALUES
49	Acct-Terminate-Cause	Integer. Valid values are: ■ Admin-Reboot (7) ■ Admin-Reset (6) ■ Callback (16) ■ Host-Request (18) ■ Idle-Timeout (4) ■ Lost-Carrier (2) ■ Lost-Service (3) ■ NAS-Error (9) ■ NAS-Reboot (11) ■ NAS-Request (10) ■ Port-Disabled (22) ■ Port-Error (8) ■ Port-Preempted (13) ■ Port-Reinit (21) ■ Port-Suspended (14) ■ Port-Unneeded (12) ■ Reauthentication-Failure (20) ■ Service-Unavailable (15) ■ Session-Timeout (5) ■ Supplicant-Restart (19) ■ User-Error (17) ■ User-Request (1)
50	Acct-Multi-Session-Id	string
51	Acct-Link-Count	Integer
52	Acct-Input-Gigawords	Integer
53	Acct-Output-Gigawords	Integer
55	Event-Timestamp	date (Not supported)
56	Egress-VLANID	Integer
57	Ingress-Filters	Integer. Valid values are: ■ Disabled (2) ■ Enabled (1)
58	Egress-VLAN-Name	string
59	User-Priority-Table	octets (Hexadecimal string followed by 0x)
60	CHAP-Challenge	octets (Hexadecimal string followed by 0x)

Table 11: Standard RADIUS attributes (continued)

ATTRIBUTE ID AND NAME		VALUE TYPE/PRE-DEFINED VALUES
61	NAS-Port-Type	Integer. Valid values are: ■ ADSL-CAP (12) ■ ADSL-DMT (13) ■ Async (0) ■ Cable (17) ■ Ethernet (15) ■ FDDI (21) ■ G.3-Fax (10) ■ HDLC-Clear-Channel (7) ■ IDSL (14) ■ ISDN (2) ■ ISDN-V110 (4) ■ ISDN-V120 (3) ■ PIAFS (6) ■ PPPoA (30) ■ PPPoEoA (31) ■ PPPoEoE (32) ■ PPPoEoQinQ (34) ■ PPPoEoVLAN (33) ■ SDSL (11) ■ Sync (1) ■ Token-Ring (20) ■ Virtual (5) ■ Wireless-802.11 (19) ■ Wireless-Other (18) ■ X.25 (8) ■ X.75 (9) ■ xDSL (16)
62	Port-Limit	Integer
63	Login-LAT-Port	string
64	Tunnel-Type	Integer. Valid values are: ■ AH (6) ■ ATMP (4) ■ DVS (11) ■ ESP (9) ■ GRE (10) ■ IP (7) ■ IP-in-IP (12) ■ L2F (2) ■ L2TP (3) ■ MIN-IP (8) ■ PPTP (1) ■ VLAN (13) ■ VTP (5)

Table 11: Standard RADIUS attributes (continued)

ATTRIBUTE ID AND NAME		VALUE TYPE/PRE-DEFINED VALUES
65	Tunnel-Medium-Type	Integer. Valid values are: ■ Appletalk (12) ■ Banyan-Vines (14) ■ BBN-1822 (5) ■ DecNet-IV (13) ■ E.163 (7) ■ E.164 (8) ■ E.164-NSAP (15) ■ F.69 (9) ■ HDLC (4) ■ IEEE-802 (6) ■ IP (1) ■ IPv4 (1) ■ IPv6 (2) ■ IPX (11) ■ NSAP (3) ■ X.121 (10)
66	Tunnel-Client-Endpoint	string
67	Tunnel-Server-Endpoint	string
68	Acct-Tunnel-Connection	string
69	Tunnel-Password	string
70	ARAP-Password	octets (Hexadecimal string followed by 0x)
71	ARAP-Features	octets (Hexadecimal string followed by 0x)
72	ARAP-Zone-Access	Integer. Valid values are: ■ Default-Zone (1) ■ Zone-Filter-Exclusive (4) ■ Zone-Filter-Inclusive (2)
73	ARAP-Security	Integer
74	ARAP-Security-Data	string
75	Password-Retry	integer
76	Prompt	integer. Valid values are: ■ Echo (1) ■ No-Echo (0)
77	Connect-Info	string
78	Configuration-Token	string
79	EAP-Message	octets (Hexadecimal string followed by 0x)
80	Message-Authenticator	octets (Hexadecimal string followed by 0x)
81	Tunnel-Private-Group-Id	string
82	Tunnel-Assignment-Id	string
83	Tunnel-Preference	Integer
84	ARAP-Challenge-Response	octets (Hexadecimal string followed by 0x)
85	Acct-Interim-Interval	Integer
86	Acct-Tunnel-Packets-Lost	Integer

Table 11: Standard RADIUS attributes (continued)

ATTRIBUTE ID AND NAME		VALUE TYPE/PRE-DEFINED VALUES
87	NAS-Port-Id	string
88	Framed-Pool	string
89	Chargeable-User-Identity	string
90	Tunnel-Client-Auth-Id	string
91	Tunnel-Server-Auth-Id	string
92	NAS-Filter-Rule	string
94	Originating-Line-Info	octets[2]
95	NAS-IPv6-Address	ipv6addr (IPv6 address)
96	Framed-Interface-Id	ifid (Not supported)
97	Framed-IPv6-Prefix	ipv6prefix (Not supported)
98	Login-IPv6-Host	ipv6addr (IPv6 address)
99	Framed-IPv6-Route	string
100	Framed-IPv6-Pool	string
101	Error-Cause	Integer. Valid values are: ■ Administratively-Prohibited (501) ■ Invalid-Attribute-Value (407) ■ Invalid-EAP-Packet (202) ■ Invalid-Request (404) ■ Missing-Attribute (402) ■ Multiple-Session-Selection-Unsupported (508) ■ NAS-Identification-Mismatch (403) ■ Proxy-Processing-Error (505) ■ Proxy-Request-Not-Routable (502) ■ Request-Initiated (507) ■ Residual-Context-Removed (201) ■ Resources-Unavailable (506) ■ Session-Context-Not-Found (503) ■ Session-Context-Not-Removable (504) ■ Unsupported-Attribute (401) ■ Unsupported-Extension (406) ■ Unsupported-Service (405)
102	EAP-Key-Name	string
123	Delegated-IPv6-Prefix	ipv6prefix
124	MIP6-Feature-Vector	octets (Hexadecimal string followed by 0x)
125	MIP6-Home-Link-Prefix	ipv6prefix
126	Operator-Name	string
127	Location-Information	octets (Hexadecimal string followed by 0x)
128	Location-Data	octets (Hexadecimal string followed by 0x)
129	Basic-Location-Policy-Rules	octets (Hexadecimal string followed by 0x)
130	Extended-Location-Policy-Rules	octets (Hexadecimal string followed by 0x)

Table 11: Standard RADIUS attributes (continued)

ATTRIBUTE ID AND NAME		VALUE TYPE/PRE-DEFINED VALUES
131	Location-Capable	Integer. Valid values are: ■ Civic-Location (1) ■ Geo-Location (2) ■ NAS-Location (8) ■ Users-Location (4)
132	Requested-Location-Info	Integer. Valid values are: ■ Civic-Location (1) ■ Future-Requests (16) ■ Geo-Location (2) ■ NAS-Location (8) ■ None (32) ■ Users-Location (4)
133	Framed-Management	Integer. Valid values are: ■ FTP (4) ■ Netconf (3) ■ RCP (7) ■ SCP (8) ■ SFTP (6) ■ SNMP (1) ■ TFTP (5)
134	Management-Transport-Protection	Integer. Valid values are: ■ Integrity-Confidentiality-Protection (3) ■ Integrity-Protection (2) ■ No-Protection (1)
135	Management-Policy-Id	string
136	Management-Privilege-Level	Integer
137	PKM-SS-Cert	octets (Hexadecimal string followed by 0x)
138	PKM-CA-Cert	octets (Hexadecimal string followed by 0x)
139	PKM-Config-Settings	octets (Hexadecimal string followed by 0x)
140	PKM-Cryptosuite-List	octets (Hexadecimal string followed by 0x)
141	PKM-SAID	short
142	PKM-SA-Descriptor	octets (Hexadecimal string followed by 0x)
143	PKM-Auth-Key	octets (Hexadecimal string followed by 0x)
144	DS-Lite-Tunnel-Name	string
145	Mobile-Node-Identifier	octets (Hexadecimal string followed by 0x)
146	Service-Selection	string
147	PMIP6-Home-LMA-IPv6-Address	ipv6addr
148	PMIP6-Visited-LMA-IPv6-Address	ipv6addr
149	PMIP6-Home-LMA-IPv4-Address	ipaddr
150	PMIP6-Visited-LMA-IPv4-Address	ipaddr

Table 11: Standard RADIUS attributes (continued)

ATTRIBUTE ID AND NAME		VALUE TYPE/PRE-DEFINED VALUES
151	PMIP6-Home-HN-Prefix	ipv6prefix
152	PMIP6-Visited-HN-Prefix	ipv6prefix
153	PMIP6-Home-Interface-ID	interface identifier
154	PMIP6-Visited-Interface-ID	interface identifier
155	PMIP6-Home-IPv4-HoA	ipv4prefix
156	PMIP6-Visited-IPv4-HoA	ipv4prefix
157	PMIP6-Home-DHCP4-Server-Address	ipaddr
158	PMIP6-Visited-DHCP4-Server-Address	ipaddr
159	PMIP6-Home-DHCP6-Server-Address	ipv6addr
160	PMIP6-Visited-DHCP6-Server-Address	ipv6addr
161	PMIP6-Home-IPv4-Gateway	ipaddr
162	PMIP6-Visited-IPv4-Gateway	ipaddr
163	EAP-Lower-Layer	Integer. Valid values are: ■ GSS-API (8) ■ IEEE-802.16e (4) ■ IEEE-802.1X-No-Preauth (2) ■ IEEE-802.1X-Preauth (3) ■ IKEv2 (5) ■ PANA-No-Preauth (7) ■ PANA-Preauth (9) ■ PPP (6) ■ Wired-IEEE-802.1X (1)
164	GSS-Acceptor-Service-Name	string
165	GSS-Acceptor-Host-Name	string
166	GSS-Acceptor-Service-Specifics	string
167	GSS-Acceptor-Realm-Name	string
168	Framed-IPv6-Address	ipv6addr
169	DNS-Server-IPv6-Address	ipv6addr
170	Route-IPv6-Information	ipv6prefix
171	Delegated-IPv6-Prefix-Pool	string
172	Stateful-IPv6-Address-Pool	string
173	IPv6-6rd-Configuration	tlv
173.1	IPv6-6rd-IPv4MaskLen	integer
173.2	IPv6-6rd-Prefix	ipv6prefix
173.3	IPv6-6rd-BR-IPv4-Address	ipaddr
174	Allowed-Called-Station-Id	string

Table 11: Standard RADIUS attributes (continued)

ATTRIBUTE ID AND NAME		VALUE TYPE/PRE-DEFINED VALUES
175	EAP-Peer-Id	octets
176	EAP-Server-Id	octets
177	Mobility-Domain-Id	integer
178	Preauth-Timeout	integer
179	Network-Id-Name	octets
180	EAPoL-Announcement	octets
181	WLAN-HESSID	string
182	WLAN-Venue-Info	integer
183	WLAN-Venue-Language	octets[3]
184	WLAN-Venue-Name	string
185	WLAN-Reason-Code	integer
186	WLAN-Pairwise-Cipher	integer
187	WLAN-Group-Cipher	integer
188	WLAN-AKM-Suite	integer
189	WLAN-Group-Mgmt-Cipher	integer
190	WLAN-RF-Band	integer
241	Extended-Attribute-1	extended
241.1	Frag-Status	Integer. Valid values are: ■ Fragmentation-Supported (1) ■ More-Data-Pending (2) ■ More-Data-Request (3) ■ Reserved (0)
241.2	Proxy-State-Length	integer
241.3	Response-Length	integer
241.4	Original-Packet-Code	integer
241.26	Extended-Vendor-Specific-1	evs
242	Extended-Attribute-2	extended
242.26	Extended-Vendor-Specific-2	evs
243	Extended-Attribute-3	extended
243.26	Extended-Vendor-Specific-3	evs
244	Extended-Attribute-4	extended
244.26	Extended-Vendor-Specific-4	evs
245	Extended-Attribute-5	long-extended
245.26	Extended-Vendor-Specific-5	evs
246	Extended-Attribute-6	long-extended
246.26	Extended-Vendor-Specific-6	evs

Table 12: Vendor-specific RADIUS attributes

VENDOR-SPECIFIC ATTRIBUTE NAME	VALUE TYPE/PRE-DEFINED VALUE
Access-Loop-Encapsulation	octets
Actual-Data-Rate-Downstream	integer
Actual-Data-Rate-Upstream	integer
Actual-Interleaving-Delay-Downstream	integer
Actual-Interleaving-Delay-Upstream	integer
ADSL-Agent-Circuit-Id	octets
ADSL-Agent-Remote-Id	octets
DSL-Forum-DHCP-Vendor-Specific	tlv
Attainable-Data-Rate-Downstream	integer
Attainable-Data-Rate-Upstream	integer
call-id	string
Cisco-Abort-Cause	string
Cisco-Account-Info	string
Cisco-Assign-IP-Pool	integer
Cisco-AVPair	string
Cisco-Call-Filter	integer
Cisco-Call-Type	string
Cisco-Command-Code	string
Cisco-Control-Info	string
Cisco-Data-Filter	integer
Cisco-Data-Rate	integer
Cisco-Disconnect-Cause	Integer. Valid values are: ■ No-Reason - 0 ■ No-Disconnect - 1 ■ Unknown - 2 ■ Call-Disconnect - 3 ■ CLID-Authentication-Failure - 4 ■ No-Modem-Available- 9 ■ No-Carrier - 10 ■ Lost-Carrier - 11 ■ No-Detected-Result-Codes - 2 ■ User-Ends-Session - 20 ■ Idle-Timeout - 21 ■ Exit-Telnet-Session - 22 ■ No-Remote-IP-Addr - 23 ■ Exit-Raw-TCP - 24 ■ Password-Fail - 25 ■ Raw-TCP-Disabled - 26 ■ Control-C-Detected - 27 ■ EXEC-Program-Destroyed - 28 ■ Close-Virtual-Connection - 29 ■ End-Virtual-Connection - 30

Table 12: Vendor-specific RADIUS attributes (continued)

VENDOR-SPECIFIC ATTRIBUTE NAME	VALUE TYPE/PRE-DEFINED VALUE
Cisco-Disconnect-Cause (continued)	■ Exit-Rlogin - 31 ■ Invalid-Rlogin-Option - 32 ■ Insufficient-Resources - 33 ■ Timeout-PPP-LCP - 40 ■ Failed-PPP-LCP-Negotiation - 41 ■ Failed-PPP-PAP-Auth-Fail - 42 ■ Failed-PPP-CHAP-Auth - 43 ■ Failed-PPP-Remote-Auth - 44 ■ PPP-Remote-Terminate - 45 ■ PPP-Closed-Event - 46 ■ NCP-Closed-PPP - 47 ■ MP-Error-PPP - 48 ■ PPP-Maximum-Channels - 49 ■ Tables-Full - 50 ■ Resources-Full - 51 ■ Invalid-IP-Address - 52 ■ Bad-Hostname - 53 ■ Bad-Port - 54 ■ Reset-TCP - 60 ■ TCP-Connection-Refused - 61 ■ Timeout-TCP - 62 ■ Foreign-Host-Close-TCP - 63 ■ TCP-Network-Unreachable - 64 ■ TCP-Host-Unreachable - 65 ■ TCP-Network-Admin-Unreachable - 66 ■ TCP-Port-Unreachable - 67 ■ Session-Timeout - 100 ■ Session-Failed-Security - 101 ■ Session-End-Callback - 102 ■ Invalid-Protocol - 120 ■ RADIUS-Disconnect - 150 ■ Local-Admin-Disconnect - 151 ■ SNMP-Disconnect - 152 ■ V110-Retries - 160 ■ PPP-Authentication-Timeout - 170 ■ Local-Hangup - 180 ■ Remote-Hangup - 185 ■ T1-Quiesced - 190 ■ Call-Duration - 195 ■ VPN-User-Disconnect - 600 ■ VPN-Carrier-Loss - 601 ■ VPN-No-Resources - 602 ■ VPN-Bad-Control-Packet - 603 ■ VPN-Admin-Disconnect - 604 ■ VPN-Tunnel-Shut - 605 ■ VPN-Local-Disconnect - 606 ■ VPN-Session-Limit - 607 ■ VPN-Call-Redirect - 608
Cisco-Email-Server-Ack-Flag	string
Cisco-Email-Server-Address	string
Cisco-Fax-Account-Id-Origin	string
Cisco-Fax-Auth-Status	string

Table 12: Vendor-specific RADIUS attributes (continued)

VENDOR-SPECIFIC ATTRIBUTE NAME	VALUE TYPE/PRE-DEFINED VALUE
Cisco-Fax-Connect-Speed	string
Cisco-Fax-Coverpage-Flag	string
Cisco-Fax-Dsn-Address	string
Cisco-Fax-Dsn-Flag	string
Cisco-Fax-Mdn-Address	string
Cisco-Fax-Mdn-Flag	string
Cisco-Fax-Modem-Time	string
Cisco-Fax-Msg-Id	string
Cisco-Fax-Pages	string
Cisco-Fax-Process-Abort-Flag	string
Cisco-Fax-Recipient-Count	string
Cisco-Gateway-Id	string
Cisco-Idle-Limit	integer
Cisco-IP-Direct	integer
Cisco-IP-Pool-Definition	string
Cisco-Link-Compression	integer
Cisco-Maximum-Channels	integer
Cisco-Maximum-Time	integer
Cisco-Multilink-ID	integer
Cisco-NAS-Port	string
Cisco-Num-In-Multilink	integer
Cisco-Policy-Down	string
Cisco-Policy-Up	string
Cisco-Port-Used	string
Cisco-PPP-Async-Map	integer
Cisco-PPP-VJ-Slot-Comp	integer
Cisco-Pre-Input-Octets	integer
Cisco-Pre-Input-Packets	integer
Cisco-Pre-Output-Octets	integer
Cisco-Pre-Output-Packets	integer
Cisco-PreSession-Time	integer
Cisco-PW-Lifetime	integer
Cisco-Route-IP	integer
Cisco-Service-Info	string
Cisco-Subscriber-Password	string
Cisco-Target-Util	integer
Cisco-Xmit-Rate	integer

Table 12: Vendor-specific RADIUS attributes (continued)

VENDOR-SPECIFIC ATTRIBUTE NAME	VALUE TYPE/PRE-DEFINED VALUE
dsp-id	string
gw-final-xlated-cdn	string
gw-final-xlated-cgn	string
gw-rxd-cdn	string
gw-rxd-cgn	string
h323-billing-model	string
h323-call-origin	string
h323-call-type	string
h323-conf-id	string
h323-connect-time	string
h323-credit-amount	string
h323-credit-time	string
h323-currency	string
h323-disconnect-cause	string
h323-disconnect-time	string
h323-gw-id	string
h323-incoming-conf-id	string
h323-preferred-lang	string
h323-prompt-id	string
h323-redirect-ip-address	string
h323-redirect-number	string
h323-remote-address	string
h323-return-code	string
h323-setup-time	string
h323-time-and-day	string
h323-voice-quality	string
incoming-req-uri	string
IWF-Session	octets
Maximum-Data-Rate-Downstream	integer
Maximum-Data-Rate-Upstream	integer
Maximum-Interleaving-Delay-Downstream	integer
Maximum-Interleaving-Delay-Upstream	integer
method	string
Minimum-Data-Rate-Downstream	integer
Minimum-Data-Rate-Downstream-Low-Power	integer
Minimum-Data-Rate-Upstream	integer
Minimum-Data-Rate-Upstream-Low-Power	integer

Table 12: Vendor-specific RADIUS attributes (continued)

VENDOR-SPECIFIC ATTRIBUTE NAME	VALUE TYPE/PRE-DEFINED VALUE
MS-Acct-Auth-Type	integer. Valid values are: ■ CHAP - 2 ■ EAP - 5 ■ MS-CHAP-1 - 3 ■ MS-CHAP-2 - 4 ■ PAP - 1
MS-Acct-EAP-Type	integer. Valid values are: ■ Generic-Token-Card - 6 ■ MD5 - 4 ■ OTP - 5 ■ TLS - 13
MS-AFW-Protection-Level	integer. Valid values are: ■ HECP-Response-Sign-And-Encrypt - 2 ■ HECP-Response-Sign-Only - 1
MS-AFW-Zone	integer. Valid values are: ■ MS-AFW-Zone-Boundary-Policy - 1 ■ MS-AFW-Zone-Protected-Policy - 3 ■ MS-AFW-Zone-Unprotected-Policy - 2
MS-ARAP-PW-Change-Reason	integer. Valid values are: ■ Admin-Requires-Password-Change - 3 ■ Expired-Password - 2 ■ Just-Change-Password - 1 ■ Password-Too-Short - 4
MS-BAP-Usage	integer. Valid values are: ■ Allowed - 1 ■ Not-Allowed - 0 ■ Required - 2
MS-CHAP2-CPW	octets
MS-CHAP2-Response	octets
MS-CHAP2-Success	octets
MS-CHAP-Challenge	octets
MS-CHAP-CPW-1	octets
MS-CHAP-CPW-2	octets
MS-CHAP-Domain	string
MS-CHAP-Error	string
MS-CHAP-LM-Enc-PW	octets
MS-CHAP-MPPE-Keys	octets
MS-CHAP-NT-Enc-PW	octets
MS-CHAP-Response	octets
MS-Extended-Quarantine-State	integer. Valid values are: ■ Infected - 2 ■ No-Data - 4 ■ Transition - 1 ■ Unknown - 3
MS-Filter	octets

Table 12: Vendor-specific RADIUS attributes (continued)

VENDOR-SPECIFIC ATTRIBUTE NAME	VALUE TYPE/PRE-DEFINED VALUE
MS-HCAP-Location-Group-Name	string
MS-HCAP-User-Groups	string
MS-HCAP-User-Name	string
MS-Identity-Type	integer. Valid values are: ■ Ignore-User-Lookup-Failure - 2 ■ Machine-Health-Check - 1
MS-IPv4-Remediation-Servers	octets
MS-IPv6-Filter	octets
MS-IPv6-Remediation-Servers	octets
MS-Link-Drop-Time-Limit	integer
MS-Link-Utilization-Threshold	integer
MS-Machine-Name	string
MS-MPPE-Encryption-Policy	integer. Valid values are: ■ Encryption-Allowed - 1 ■ Encryption-Required - 2
MS-MPPE-Encryption-Type	octets
MS-MPPE-Encryption-Types	integer. Valid values are: ■ RC4-40bit-Allowed - 1 ■ RC4-40or128-bit-Allowed - 6 ■ RC4-128bit-Allowed- 2
MS-MPPE-Recv-Key	octets
MS-MPPE-Send-Key	octets
MS-Network-Access-Server-Type	integer. Valid values are: ■ DHCP-Server - 3 ■ HCAP-Server - 6 ■ HRA - 5 ■ Remote-Access-Server - 2 ■ Terminal-Server-Gateway - 1 ■ Unspecified - 0 ■ Wireless-Access-Point - 4
MS-New-ARAP-Password	octets
MS-Old-ARAP-Password	octets
MS-Primary-DNS-Server	ipaddr
MS-Primary-NBNS-Server	ipaddr
MS-Quarantine-Grace-Time	integer
MS-Quarantine-IPFilter	octets
MS-Quarantine-Session-Timeout	integer
MS-Quarantine-SOH	octets
MS-Quarantine-State	integer. Valid values are: ■ Full-Access - 0 ■ Probation - 2 ■ Quarantine - 1

Table 12: Vendor-specific RADIUS attributes (continued)

VENDOR-SPECIFIC ATTRIBUTE NAME	VALUE TYPE/PRE-DEFINED VALUE
MS-Quarantine-User-Class	string
MS-RAS-Client-Name	string
MS-RAS-Client-Version	string
MS-RAS-Correlation	octets
MS-RAS-Vendor	integer
MS-RAS-Version	string
MS-RNAP-Not-Quarantine-Capable	integer. Valid values are: ■ SoH-Not-Sent - 1 ■ SoH-Sent - 0
MS-Secondary-DNS-Server	ipaddr
MS-Secondary-NBNS-Server	ipaddr
MS-Service-Class	string
MS-TSG-Device-Redirection	integer
MS-User-IPv4-Address	ipaddr
MS-User-IPv6-Address	ipv6addr
MS-User-Security-Identity	string
next-hop-dn	string
next-hop-ip	string
outgoing-req-uri	string
prev-hop-ip	string
prev-hop-via	string
release-source	string
remote-media-address	string
session-protocol	string
sip-conf-id	string
sip-hdr	string
subscriber	string