Technical Guide

Allied Telesis™

How To | Configure Administrative Login using RADIUS and TACACS+

Introduction

In a network with multiple switches and routers, it is convenient for a Network Administrator to use a centralized authenticating database, rather than configuring the local database on each individual device to authenticate users attempting to log in to the device. The two most popular protocols used for centralized authentication are RADIUS or TACACS+. AlliedWare Plus supports both of these protocols.

This How To note explains the process of configuring AlliedWare Plus to interact with both RADIUS and TACACS+ Servers for login authentication.

Note: This How To note covers only Login authentication; the use of RADIUS for port authentication (802.1x, MacAuth, WebAuth) is not covered.

Which software version does this document apply to?

This How To Note applies to AlliedWare Plus version **5.4.3** and above.

List of terms

VTY

Virtual Teletype (VTY) is the term used to refer to the 'virtual lines' via which telnet and SSH sessions connect to the switch. The parameters that are applied to telnet and SSH connections are configured under "line vty".

Login Authentication

For a user to gain access to the switch CLI (i.e. to log into the switch), they must provide a username and password that authenticates that they are authorized to have access to the CLI.

Accounting

Information pertaining to a user's connection to the switch can be transmitted to a server to be kept for audit purposes. The sort of information that is transmitted are things like:

- session start time
- session end time
- commands entered during the session

AlliedWare Plus™
OPERATING SYSTEM

Content

Additional reading

For more information and examples, see the "Two-step authentication" section in the AlliedWare Plus Technical Tips and Tricks.

http://www.alliedtelesis.com/support/documentation_keyword_tips.aspx

Configuring an AlliedWare Plus Switch to use RADIUS and/or TACACS+ for Login Authentication

As well as using the local user database to authenticate logins to the switch, RADIUS or TACACS+ can also be used. The basic steps to setting up AlliedWare Plus to use a RADIUS or TACACS+ Server for login authentication are reasonably straightforward.

Lets work through these step using RADIUS as an example.

1. Configure all of the RADIUS servers available to the switch.

First, configure all of the RADIUS servers available to the switch with the **radius-server host** command, (TACACS+ is configured in the same way, using the **tacacs-server host** command):

```
radius-server host {<host-name>|<ip-address>} [acct-port<065535>]
[auth-port <0-65535>] [key <key-string>] [retransmit <0-100>][timeout <1-1000>]
```

Example:

```
awplus(config)#radius-server host 192.168.1.1 key secret1
awplus(config)#radius-server host 192.168.2.1 key secret2
awplus(config)#radius-server host 192.168.3.1 key secret3
awplus(config)#radius-server host 192.168.4.1 key secret4
```

In the examples above, port numbers have not been configured, so the switch will use the default port numbers for RADIUS authentication (port 1812) and accounting (port 1813). The ports configured need to match the ports on which the RADIUS server is listening.

If the server was set up to use different port numbers than the default values, then the command configuring the RADIUS server on AlliedWare Plus would have to specify those non-default port numbers. Any port number between 0 and 65535 is possible.

A **key** is used to identify the client switch to the server. The server is configured with a key for each client switch that may send authentication requests to it. So, the switch needs to know which key it should use to identify itself to each server. Hence, there is a key included in each server definition that is configured on the switch.

Note: In RADIUS-speak, the client switch is referred to as a NAS (Network Access Server).

2. Configure the switch to use RADIUS authentication for logins.

```
aaa authentication login {default|<list-name>} {[local] [group
   {radius|tacacs+|<group-name>}]}
```

For example:

```
awplus(config)#aaa authentication login default group radius
```

The **list-name** default means that both the console and VTY (Virtual Teletype) connections (telnet and SSH) will automatically use this authentication method for login to the switch.

The group-name **radius** is predefined, and represents the group that consists of all RADIUS servers that have been configured with the **radius-server host** command. Similarly, the group name **tacacs+** is predefined, and includes all TACACS+ Servers that have been configured with the **tacacs-server host** command. Creating other groups that are subsets of the full set of configured servers is covered below in the section "Configuring a Group List" on page 6.

The TACACS+ commands to create a similar configuration as the one we have created above for RADIUS are:

```
awplus(config)#tacacs-server host a.b.c.d key tacacs+-key
awplus(config)#aaa authentication login default group tacacs+
```

With this simple 2-step configuration, the AlliedWare Plus switch will start using RADIUS or TACACS+ Servers for authentication of users wishing to gain management access to the device's CLI.

How the switch tries each configured RADIUS or TACACS+ Server in turn

The purpose of configuring the switch with multiple RADIUS servers is for resiliency – so that if one RADIUS server becomes unavailable, the switch can use the other RADIUS servers. When a user attempts to log in, the switch sends an authentication request to the first authentication server in the group.

- If the first server in the list is reachable, and it contains a username and password matching the authentication request, the user is authenticated and the login succeeds.
- If the authentication server denies the authentication request because of an incorrect username or password, the user login fails.
- If the switch receives no response at all from the first RADIUS server, then it will resend its request to that server. If, after a few retries, the switch is just getting no response from the first server, it will move on to trying the next server.

The number of times it will attempt to contact a RADIUS server before moving on to the next configured server, is configurable with the command:

```
radius-server retransmit <retries>
```

This command can be configured globally, and apply to all RADIUS servers that the switch knows about. Similarly, a retransmit value can be configured individually on specific server definitions by using the **retransmit** parameter on the **RADIUS-server host** command. If a global value and server-specific values have been configured, the server-specific values take precedence.

The default number of times is **3 attempts**.

The amount of time the switch waits for a reply each time it sends a request to a RADIUS server is configured using the command:

```
radius-server timeout <seconds>
```

This command can be configured globally, and apply to all RADIUS servers that the switch knows about. Similarly, a timeout value can be configured individually on specific server definitions by using the **timeout** parameter on the **RADIUS-server host** command. If a global value and server-specific values have been configured, the server-specific values take precedence.

The default time the switch waits for a reply is **5 seconds**.

The RADIUS client considers a RADIUS server to be dead if it fails to respond to a request after the configured number of retransmit attempts have been made. To improve RADIUS response times when some servers may be unavailable, a **deadtime** can be used to skip dead servers using the command:

```
radius-server deadtime <minutes>
```

The default deadtime is **0 minutes**.

This default of 0 minutes means, that by default, 'Dead' RADIUS servers are not skipped, they will be retried. To tell the switch to skip a non-responsive server for a while, a deadtime needs to be configured. The deadtime is a global setting. There is no command for setting the deadtime on a per-server basis.

Once the deadtime has expired, the switch will once again try to send requests to the server in question. If it is still unresponsive, then it will again be marked **Dead** for the duration of the deadtime.

TACACS+ has a similar process of working through the configured servers until it finds one that responds. With TACACS+, the retransmit time or deadtime are not configurable, only the timeout is configurable.

Note: If the requested username is not present on a given RADIUS or TACACS+ Server, then the server will reject the login request. There is no circumstance in which the switch will retry servers until it finds one that has the requested username. As soon as a server replies with either an **access-accept** or **access-reject**, the switch does not try any other servers.

What if no RADIUS server responds to a switch's request?

If no RADIUS server at all responds to the switch's request, it is possible to have another fall back option. This is achieved by specifying multiple authentication methods - one to be used first, then another if that first method gets no response.

For example, we can tell the switch to first try RADIUS authentication, then the local user database:

```
awplus(config)#aaa authentication login default group radius
    local
```

- This command effectively gives the switch a list of methods to use for authentication. Hence, it is referred to as a **method list**.
- If any of the configured RADIUS servers are reachable, and do not authenticate the user, then the login will fail – the local user database will not be tried.

If no RADIUS servers are reachable, then the local user database will be tried.

Note: Using remote authentication is the common configuration, however, in the case where a network is down (and **only** when the network is down) the local database is used to provide a 'login of last resort'.

Configuring a method list using the 'list-name' command

If the 'default' list-name is used, as in the example above, then this authentication method list will automatically apply to the console port as well as all VTY lines – telnet and SSH.

If, however, you want a different authentication method to be used on the console to that which will be used on the VTY lines, you can configure a separate 'list-name' and method for each, i.e:

```
awplus(config)#aaa authentication login CONSOLE local
awplus(config)#aaa authentication login TTY group radius
```

Then, under each line, configure the login authentication list-name:

To set the authentication for users accessing the console to use the method list 'CONSOLE' (i.e. to use the local user database), proceed as follows:

```
awplus(config)#line console 0
awplus(config-line)#login authentication CONSOLE
```

To set the authentication for telnet/SSH users to use the method list 'TTY' (i.e. to use the configured RADIUS servers), the commands are:

```
awplus(config)#line vty 0 32*
awplus(config-line)#login authentication TTY
```

*To make sure that connections after the first 5 have the same authentication setting, you should really set all up to the max VTY

You can also configure the switch to use TACACS+ by creating a method list that uses TACACS+, and configuring that method list on the console or the VTY lines.

Configuring a Group List

Up until now, all the examples we have looked at have used the RADIUS group 'radius', which simply represents all the configured RADIUS servers. It is possible to define groups that are a subset of the configured RADIUS servers.

```
aaa group server radius <group-name>
```

A subset of RADIUS to be used by the switch for login authentication can be specified using the aaa group server radius command:

Example: We have four RADIUS Servers configured with the radius-server host command:

```
awplus(config)#radius-server host 192.168.1.1
awplus(config)#radius-server host 192.168.2.1
awplus(config)#radius-server host 192.168.3.1
awplus(config)#radius-server host 192.168.4.1
```

But, we would only like to use two of them at the moment.

To achieve this:

1. Create a server group.

```
awplus(config)#aaa group server radius GROUP1
```

2. Specify the RADIUS servers to include in the group (Group1).

```
awplus(config-sg)#server 192.168.1.1
awplus(config-sg)#server 192.168.2.1
```

3. Configure aaa authentication.

Configure aaa authentication using this group (Group1), rather than the pre-defined group 'radius'

```
awplus(config)#aaa authentication login default group GROUP1
```

Setting the source address from which RADIUS requests are sent

The source IP address that the switch uses on its RADIUS requests can be configured. Normally it would be the address on the interface over which the RADIUS server is reached. However, if the command below is configured, then the specified IP address (or the primary IP address on the specified interface) will be used as the source address.

```
ip radius source-interface {<interface>|<ip-address>}
```

RADIUS/TACACS+ login accounting

The switch can be configured to send information on the start and finish of a login session using the aaa accounting login command. A method list **list-name** and **group-name** can be used in the same way as RADIUS or TACACS+ authentication if desired. By default, AlliedWare Plus does not send any accounting messages for login sessions. Accounting is only performed if it is explicitly configured.

```
aaa accounting login {default|<list-name>}
{start-stop|stop-only|none} {group {radius|tacacs+|<group-
   name>}}
```

There are only two types of RADIUS or TACACS+ accounting packet:

- **Accounting-Response**: always sent from the server to the NAS, and are effectively ACKs of the Accounting-Request packets.
- **Accounting-Request**: always sent from the NAS to the server and carry the attribute **Acct-Status-Type**.

The most commonly used values of the Acct-Status-Type 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**: which are packets sent periodically during the session to give update reports on the statistics that are being collected. Interim updates are only sent if the **aaa accounting update** command is configured.

The statistics that can be exchanged in the session are:

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

The switch will send an Accounting-Request with Acct-Status-Type=Start immediately after authentication.

It will send an Accounting-Request with Acct-Status-Type=Stop when the user logs out. The switch will send interim updates during the session if configured to do so.

TACACS+ command accounting

In addition to login accounting, TACACS+ also supports command accounting. The purpose of command accounting is to provide an audit trail of the commands that have been executed on the switch, which can be enabled per privilege level using the command:

```
aaa accounting commands <1-15> default stop-only group tacacs+
```

(Where <1-15> is the privilege level you wish to configure command accounting for.)

Command accounting needs to be explicitly configured individually for each privilege level. When TACACS+ command accounting is enabled for a particular privilege level all commands that are successfully executed at that privilege will be sent to the accounting server. Invalid commands, commands that are not executed, and command output is not sent to the accounting server.

Only the default method list is supported for TACACS+ command accounting, which means it can only be enabled or disabled globally. TACACS+ command accounting only supports the **stop-only** parameter, meaning commands are only sent to the accounting server once they have executed.

Viewing the RADIUS Configuration

The **show radius** command gives you all of the information on the RADIUS configuration, including the status of the servers.The initial status of the configured RADIUS servers will show as **unknown**.

When a user attempts to login, the switch will send a RADIUS Access-Request to the first configured server in the Group. If, after retransmitting this Request the number of times specified by the **radius-server retransmit** count, it does not receive a reply it will mark the status of this server as 'Dead' and try the next server configured in the Group.

- If a deadtime is configured, it will not retry any 'Dead' servers for the period configured.
- If the switch receives a reply to its RADIUS Access-Request from a server it will mark it as 'Alive'.
- If the first server constantly replies, then the other servers will never be tried, and will stay in the 'unknown' state.

```
awplus#sh radius
RADIUS Global Configuration
  Source Interface     : not configured
  Secret Key           :
  Timeout              : 5 sec
  Retransmit Count     : 3
  Deadtime             : 0 min

Server Host : 192.168.2.1
  Authentication Port : 1812
  Accounting Port     : 1813
  Secret Key          : secret2
Server Host : 192.168.1.1
  Authentication Port : 1812
  Accounting Port     : 1813
Secret Key          : secret1
Server Host : 192.168.3.1
  Authentication Port : 1812
  Accounting Port     : 1813
  Secret Key          : secret3
Server Host : 192.168.4.1
  Authentication Port : 1812
  Accounting Port     : 1813
  Secret Key          : secret4

Server Host/     Auth  Acct  Auth           Acct
IP Address       Port  Port  Status         Status
------------------------------------------------------------
192.168.2.1      1812  1813  Alive          Unknown
192.168.1.1      1812  1813  Unknown        Unknown
192.168.3.1      1812  1813  Unknown        Unknown
192.168.4.1      1812  1813  Unknown        Unknown
```

Confirming the status of TACACs+ servers

There is also a **show tacacs+** command which shows you the status of configured TACACS+ Servers:

```
awplus#show tacacs+
TACACS+ Global Configuration
  Timeout              : 5 sec

Server Host/     Server
IP Address       Status
------------------------
10.1.1.1         Alive
192.12.22.1      Alive
awplus#
```

User Access and Privilege Levels

When a user is configured in the local user database, they can be configured with a privilege level depending on how much access to the switch is appropriate for them. The privilege level configured for a user denotes the highest privilege level that the user can access without having to enter an **enable** password.

A user at:

- privilege level 1 can access the majority of show commands,
- privilege level 7 can access the majority of show commands including platform show commands.
- privilege level 15 can access configuration commands as well as all show commands in Privileged Exec mode.

A RADIUS or TACACS+ Server can be used to assign privilege levels to a user when they are authenticated. A TACACS+ Server is also able to be used for enable password authentication, i.e. authenticate the password entered for the **enable** command. The AlliedWare Plus RADIUS client does not support this.

Note: If TACACS+ enable password authentication is configured, an AlliedWare Plus device will not attempt to determine a user's privilege level following login authentication, as this will be determined during enable password authentication.

A user can see their current privilege level with the **show privilege** command:

```
awplus>show privilege
Current privilege level is 1
awplus>enable
awplus#show privilege
Current privilege level is 15
```

Configuring the AlliedWare Plus Switch to act as a RADIUS Server

An AlliedWare Plus switch can be used to provide authentication to client switches users via RADIUS. Please check that your feature license supports the number of users required.

To configure an AlliedWare Plus switch to act as a RADIUS server, the following commands are used:

1. Enable the local RADIUS server.

```
awplus(config)#radius-server local
awplus(config-radsrv)#server enable
```

This will automatically configure the following additional RADIUS configuration:

```
crypto pki trustpoint local
!
crypto pki enroll local
radius-server local
 server enable
 nas 127.0.0.1 key awplus-local-radius-server
```

2. Add client devices.

Then, also under the local RADIUS server configuration, we need to add any client devices (NAS) which are going to be sending RADIUS Access-Requests to it. In the following example, we have used the command radius-server host 192.168.2.1 key secret2 to add the switch 192.168.2.254. The key (secret2) must match the key configured on the client.

```
awplus(config-radsrv)#nas 192.168.2.254 key secret2
```

3. Define groups with three different user privilege levels.

```
group priv15
  attribute Service-Type Administrative-User*
group priv7
  attribute Cisco-AVPair shell:priv-lvl=7
  attribute Service-Type NAS-Prompt-User**
group priv1
  attribute Service-Type NAS-Prompt-User
```

*Service-Type **6** is the type number for an Administrative-User, and can be used instead of **Administrative-User**.

Service-Type **7 is the type number for an NAS-Prompt-User, and can be used instead of **NAS-Prompt-User**.

4. Add users and assign them to the appropriate group for their privilege level.

```
user user15 password password15 group priv15
```

- Authenticated user15 users with privilege level 15 have access to all commands.

  These users are assigned privilege level 1 initially and can enter the **enable** command to gain access to privilege level 15. No enable password is required, whether an enable password is configured on the local switch or not.

```
user user7 password password7 group priv7
```

- Authenticated users with privilege level 7 are assigned privilege level 1 initially, and can enter the **enable 7** command to gain access to privilege level 7.
- Authenticated users with privilege level 7 to 14 have access to privilege level 1 commands and all show commands.

```
user user1 password password1 group priv1
```

- The user 'user1', when authenticated, is assigned privilege level 1.
- Users with privilege levels 1 to 6 have access to privilege 1 level commands only.
- The authenticated user can only enter the **enable 1** command, which will still only provide a privilege level of 1.

Notes:

1. In fact the following group configuration can be used to assign any privilege level, including level 15, to a user:

```
attribute Cisco-AVPair shell:priv-lvl=<1-15>
attribute Service-Type NAS-Prompt-User
```

2. Administrative-user and NAS-Prompt-User are the only values of 'Service-Type' that an AlliedWare Plus NAS will recognise. If an AlliedWare Plus NAS receives a RADIUS Access-accept from the RADIUS server with any other Service-Type, the NAS will treat this as being the same as having received an Access-Reject, so the user will be denied login access.

3. For any level user, from privilege level 1 to 15 who is authenticated, if they enter the **enable** password (if configured), then they will be assigned to privilege level 15. But, if no enable password is configured, then only users assigned to privilege level 15 on authentication can gain access to privilege level 15.

4. To restrict a level 1 user from simply typing ENA to raise their access level, set a long random enable password on the switch. If the user gets level 15 from the Radius server, then they can enable without needing the password, If a user gets level 1 from the Radius, then they can't enable to 15 without knowing the password.

   Note that if local users are configured as a "last resort" access, then the enable password will also be needed in this case, making for a more secure "double" password requirement.

Using a TACACS+ Server for Authentication and Accounting

The current implementation of the TACACS+ client in AlliedWare Plus supports the following features:

- Authentication for the user access request sessions
- Authentication of enable password on a per-user basis
- Accounting to provide an audit trail of user exec sessions.
- Accounting of CLI commands executed within a user exec session, configurable on a per privilege level basis.

The attributes that AlliedWare Plus will process in the authentication response are:

- **idletime** - sets how long the switch will wait, after the last user input into the shell session.
- **timeout** - sets an absolute upper limit on the duration of the shell session, after which the user will be forcibly logged out, before forcibly closing the session and logging the user out.
- **privilege level**- sets the user's privilege level in the range 1 to 15, with 15 being the highest.

Note: If TACACS+ enable password authentication is configured an AlliedWare Plus device will not attempt to determine a user's privilege level following login authentication, as this will be determined during enable password authentication.

Configuring TACACS+ for authentication and accounting

Here is a summary of how to use TACACS+ authentication and accounting under AlliedWare Plus.

Example:

1. Configure all of the TACACS+ Servers available to the switch, and specify the shared key.

```
awplus(config)#tacacs-server host 192.168.1.1 key secret1
```

2. Tell the switch to use TACACS+ authentication for logins.

```
awplus(config)#aaa authentication login default group tacacs+
```

A method-list-name) and group-list can be configured in the same way as with RADIUS, if required.

3. Configure the switch to use TACACS+ enable password authentication

With TACACS+, we are also able to have the switch's enable password authenticated by the TACACS+ Server. If you wish to use TACACS+ for enable password authentication, it is advisable to also use the same TACACS+ Server for login authentication as well.

```
awplus(config)#aaa authentication enable default group tacacs+
```

AlliedWare Plus supports only a default method list for enable password authentication, which means it is applied globally to all users accessing the switch via the console, or via telnet/SSH.

A user is configured on a TACACS+ Server with a maximum privilege level. When they enter the **enable <privilege level>** command on the switch, they are prompted for an enable password which is authenticated against the TACACS+ Server. If the password is correct, and the specified privilege level is equal to or less than the user's maximum privilege level, then they are granted access to that level. If the user attempts to access a privilege level that is higher than their maximum configured privilege level, then the authentication attempt will be rejected and they will remain at their current privilege level.

4. If Accounting is required, configure the default method list for TACACS+ login accounting

```
awplus(config)#aaa accounting login default start-stop group
   tacacs+
```

The default login accounting method list will be applied to all exec sessions, without the need for additional configuration. Alternatively method lists (list-name) can be configured and applied separately to console and VTY lines. Specifying the **start-stop** parameter means that a **start** packet will be sent when a user exec session begins, and a **stop** packet will be sent when the user exec session closes. Alternatively **stop-only** can be specified to only send a TACACS+ accounting **stop** packets when user exec sessions close.

TACACS+ will also send update messages if **aaa accounting update** is configured.

Command Accounting is configurable per privilege level if required, and then only commands at the specified privilege level will be accounted to the TACACS+ Server.

Configure TACACS+ command accounting for privilege level 1,7, and 15.

```
awplus(config)#aaa accounting commands 1 default stop-only
   group tacacs+
```

```
awplus(config)#aaa accounting commands 7 default stop-only
   group tacacs+
```

```
awplus(config)#aaa accounting commands 15 default stop-only
   group tacacs+
```

C613-16179-00 REV A

Allied Telesis™ the solution : the network

North America Headquarters | 19800 North Creek Parkway | Suite 100 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
EMEA & CSA Operations | Incheonweg 7 | 1437 EK Rozenburg | The Netherlands | T: +31 20 7950020 | F: +31 20 7950021

alliedtelesis.com