TACACS+

FEATURE OVERVIEW AND CONFIGURATION GUIDE

Introduction

This guide provides information about the AlliedWare Plus™ implementation of TACACS+ and how to configure it on your switch.

TACACS+ (Terminal Access Controller Access-Control System Plus) provides a method for securely managing multiple network devices from a single management service.

TACACS+ is a TCP-based access control protocol, utilizing TCP port 49, that allows a device to forward a user's username and password to an authentication server to determine whether access can be allowed. In addition to this authentication service, TACACS+ can also provide authorization and accounting services.

Products and software version that apply to this guide

This guide applies to AlliedWare Plus products that support TACACS+, running version **5.4.4** or later.

To see whether your product supports TACACS+, see the following documents:

- The product's Datasheet
- The AlliedWare Plus 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:

- TACACS+ command authorization - 5.4.6-2.1

Content

TACACS+ Overview

The purpose of TACACS+ is to provide a service for the Authentication, Authorization, and Accounting (AAA) of users' interactions with networking equipment.

The service involves:

- Servers that hold Authentication credentials (usernames and passwords), make Authorization decisions and collect Accounting statistics.
- Client devices that communicate with the servers to access their AAA services.
- A protocol via which to carry out the communication.

Authentication involves identifying a user, typically by requiring the user to supply a valid username and password before access is granted. Following authentication, the user must gain authorization to perform tasks. For example, after logging into a device, a user may try to issue configuration commands. The authorization process determines whether the user has the authority to issue these commands. Authorization is always preceded by authentication.

Accounting is the process of keeping an audit trail of information about a session: start time, end time, what commands were executed during the session, etc

One of the features of TACACS+ is the ability to separate authentication, authorization, and accounting so that these functions can be provided independently on separate servers.

The AlliedWare Plus TACACS+ implementation

The AlliedWare Plus TACACS+ implementation provides authentication, authorization, and accounting. Note that:

- Authorization cannot be performed independently of the authentication process.
- Authentication and authorization must be configured on the same server.
- Method lists of specific TACACS+ servers cannot be configured, only the set of all TACACS+ servers may be used.

With the AlliedWare Plus TACACS+ implementation, all traffic that passes between the TACACS+ client and the TACACS+ servers on the network is encrypted. TACACS+ encrypts the entire payload of packets, which means that it encrypts the user's password between the client and the server.

A TACACS+ client is available on your device. You need a system running TACACS+ server software from a software provider to use the TACACS+ functionality on your device.

Prioritization of TACAS+ servers

TACACS+ servers are queried in the order they are added. So, for example, if servers performing command authorization are configured before servers performing other authorization, authentication, or accounting roles, the command authorization servers will be queried first. This can be used to configure TACACS+ servers to perform different AAA roles.

Authentication

The TACACS+ protocol can forward many types of username and password information. The AlliedWare Plus TACACS+ implementation supports username and password login authentication, as well as enable password authentication. This information is encrypted over the network with MD5 (Message Digest 5).

When TACACS+ login authentication is enabled on the switch with the **aaa authentication login** command and at least one TACACS+ server is configured and reachable, all user login authentications are authenticated against the TACACS+ server. No local login or other means of authentication is allowed or accepted by the switch unless the switch has been configured to use another authentication method as a backup, and the TACACS+ server is not reachable.

When TACACS+ enable password authentication is enabled on the switch with the **aaa authentication enable default group tacacs+** command and at least one TACACS+ server is configured and reachable, all user attempts to access a higher privilege level using the **enable (Privileged Exec mode)** command are authenticated against the TACACS+ server.

If TACACS+ enable password authentication is enabled and the TACACS+ server is not reachable, then the user is only granted access to the desired privilege level if a backup authentication method is also configured.

Authorization

In the AlliedWare Plus TACACS+ implementation, authorization cannot be performed independently of the authentication process. Authorization is concerned with what users are allowed to do once they have gained access to the managed device. This involves the passing of Attribute Value pairs (AV pairs) from the TACACS+ server to the managed device. An AV pair is made up of two pieces of information: the attribute that identifies the parameter to be set, and the value that specifies the value to assign to that parameter. These AV pairs are configured on a per-user or per-group basis on the TACACS+ server.

The AV pairs that are supported by the AlliedWare Plus TACACS+ implementation are:

- **Privilege level**

  Privilege levels range from 1 to 15, with 15 being the highest.

- **Timeout**

  The value assigned to this attribute specifies the length of time that the session can exist. After this value has expired, the session will either be disconnected, or have the privilege of the user reduced. The valid range of timeout values is 0 to 65535 (minutes).

- **Idletime**

  If no input or output traffic is received or sent in the period specified by the value for this attribute, the session is disconnected. The valid idletime range is 0 to 65535 (minutes).

Command authorization

TACACS+ command authorization provides centralized control of the commands available to a user of an AlliedWare Plus device. Once enabled, with the **aaa authorization commands** command:

- The command string and username are encrypted and sent to the first available configured TACACS+ server (the first server configured) for authorization.
- The TACACS+ server decides if the user is authorized to execute the command and returns the decision to the AlliedWare Plus device.
- Depending on this decision the device will then either execute the command or notify the user that authorization has failed.

If multiple TACACS+ servers are configured, and the first server is unreachable or does not respond, the other servers will be queried, in turn, for an authorization decision.

By default, TACACS+ authorization applies to commands issued in exec mode only. Authorization of configuration mode commands is enabled using the **aaa authorization config-commands** command.

Note: Authorization of configuration commands is required for a secure TACACS+ command authorization configuration as it prevents the feature from being disabled to gain access to unauthorized exec mode commands.

You can configure multiple TACACS+ servers for redundancy. In addition, a local fall-back may be configured in case all the TACACS+ servers become unreachable. Commands are then authorized based on the user's privilege level; the same behavior as if command authorization had not been configured. If a local fall-back is not enabled and the servers become unreachable, then all commands, except **logout**, **exit**, and **quit**, will be denied.

Note: The commands **logout**, **exit**, and **quit** are accepted without performing command authorization. This is so a user can close a session even if command authorization fails.

Accounting

TACACS+ accounting usually takes place after authentication and authorization. However, because TACACS+ separates these three functions, neither authentication nor authorization are required for accounting to function. TACACS+ accounting provides the following two distinct functions:

- a record of services used for billing purposes
- an audit trail for user exec sessions

The AlliedWare Plus TACACS+ accounting implementation supports an audit trail for user exec sessions only. This includes the ability to configure accounting for user logins and logouts, and accounting of any commands executed by the user while they are logged into the switch.

TACACS+ accounting includes three different types of accounting records:

- **start** records that indicate a service is about to start
- **stop** records that indicate a service has just ended
- **update** records that indicate a service is still in progress

Configuration

The TACACS+ server is normally a multiuser system running TACACS+ server software from a software provider. TACACS+ servers are identified on the basis of their host name or IP address. A TACACS+ server and a device use a shared secret text string to encrypt passwords and exchange responses. To configure TACACS+, you must specify the host running the TACACS+ server software and a secret text string that it shares with the switch.

Configure TACACS+

Follow the steps below to configure TACACS+ for login authentication, enable password authentication, and accounting:

Step 1. **Specify a remote TACACS+ server and the shared secret key**	
`awplus#` `configure terminal`	Enter Global Configuration mode.
`awplus(config)#` `tacacs-server host {<host-name>|<ip-address>} [key [8]<key-string>]`	Specify the IP address or host name of the remote TACACS+ server host and the shared secret key to use with the specified TACACS+ server. Specify 8 if you are entering a password as a string that has already been encrypted instead of entering a plain text password. As many as four TACACS+ servers can be configured and consulted for authentication and accounting. The first server configured is regarded as the primary server and if the primary server fails then the backup servers are consulted in turn.
`awplus(config)#` `tacacs-server key [8] <key-string>`	Specify the global shared secret text string used between the switch and **all** TACACS+ servers. Specify **8** if you are entering a password as a string that has already been encrypted instead of entering a plain text password. If no secret key is explicitly specified for a TACACS+ server with the **tacacs-server host** command, the global secret key will be used.
Step 2. **Specify the timeout value**	
`awplus(config)#` `tacacs-server timeout <seconds>`	Specify for how many seconds a switch waits for a reply to a TACACS+ request before considering the TACACS+ server dead.

Step 3. **Define the method list for TACACS+ login authentication**	

`awplus(config)#`
 	
`aaa authentication login {default|<list-name>} {[local] [group {radius| tacacs+|<group-name>}]}`
	This method list defines the AAA server type used for login authentication. The server types are always used in the order specified with this command. If the first server in the method list is unreachable, the switch sends the request to the next server in the list. If the authentication server denies the authentication request because of an incorrect username or password then the user login fails.

Step 4. Define the method list for TACACS+ enable password authentication	

`awplus(config)#`
 	
`aaa authentication enable default group tacacs+ [local] [none]`
	This method list defines the authentication method used to determine the privilege command level a user can access. Specify **local** to use the locally configured enable password and **none** to grant access to Privileged Exec mode with no authentication, if the TACACS+ server goes offline, or is not reachable during enable password authentication.

Step 5. Define the method for TACACS+ login accounting	

`awplus(config)#`
 	
`aaa accounting login {default|<list-name>} {start-stop|stop-only| none} {group {radius| tacacs+|<group-name>}}`
	You can only define one method for login accounting, either RADIUS or TACACS+. Specify **start-stop** to send both start and stop login accounting records, **stop-only** to send only stop login accounting records, or **none** to disable the sending of login accounting records.

Step 6. Configure TACACS+ command accounting	

`awplus(config)#`
 	
`aaa accounting commands <1-15> default stop-only group tacacs+`
	TACACS+ command accounting is configured per privilege level and only commands of the specified privilege level are accounted. Therefore, if you require that all commands are accounted to the TACACS+ server, you must configure command accounting for each privilege level separately. Commands are accounted to the TACACS+ server after they have successfully executed.

Step 7. Troubleshooting TACACS+	

`awplus(config)#`
 	
`show tacacs+`
	Display the current TACACS+ server configuration and status.

`awplus#`
 	
`debug aaa authentication`
	Enable debug output for TACACS+ authentication.

`awplus#`
 	
`debug aaa authorization`
	Enable debug output for TACACS+ authorization.

`awplus#`
 	
`debug aaa accounting`
	Enable debug output for TACACS+ accounting.

TACACS+ configuration example

Example The following example shows how to configure the switch to authenticate and account using TACACS+.

Output 1: Example TACACS+ authentication and accounting configuration

```
!
tacacs-server host 172.10.10.1
tacacs-server key tacacspass
aaa authentication login admin group tacacs+ local
aaa authentication enable default group tacacs+ local
aaa accounting login admin start-stop group tacacs+
aaa accounting commands 1 default stop-only group tacacs+
aaa accounting commands 7 default stop-only group tacacs+
aaa accounting commands 15 default stop-only group tacacs+

line console 0
login authentication admin
accounting login admin
!
```

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

- The **tacacs-server host** command defines the IP address of the TACACS+ server host.
- The **tacacs-server key** command defines the global shared secret text string between the network access server and the TACACS+ server host.
- The **aaa authentication login** command defines a method list named **admin** to use first the TACACS+ servers and then the local user database for user login authentication.
- The **aaa authentication enable default group tacacs+** command defines a method list to use first the TACACS+ servers and then the local enable passwords, set with the **enable password** command, for user enable password authentication.
- The **aaa accounting login** command defines a method named **admin** to use TACACS+ servers for login accounting.
- The **aaa accounting commands** command specifies the privilege level of the commands that will be accounted.
- The **login authentication** command specifies that this method list will be used for authenticating users logging in on the asynchronous console port.
- The **accounting login** command specifies that this method list will be used for accounting users logging in on the asynchronous console port.

Configure TACACS+ command authorization

There are two key steps to configuring TACACS+ command authorization:

1. Create method lists that define the TACACS+ servers and optional local fall-back service. These method lists will be used to authorize certain sets of commands.

   AlliedWare Plus defines three sets of commands, that are indexed by a **level** value:

   Level = 1: All commands that can be accessed by a user with privilege level between 1 and 6 inclusive

   Level = 7: All commands that can be accessed by a user with privilege level between 7 and 14 inclusive

   Level = 15: All commands that can be accessed by a user with privilege level 15

   Method lists can contain two methods:

   - A set of TACACS+ servers. Currently only one possible set of servers can be specified, namely the set of all TACACS+ servers currently configured on the unit.
   - A local fall-back. This is the method that is applied if no TACACS+ servers are reachable. The only available option is **none**, which means no authorization is applied, so all commands are allowed. If this option is not specified, and if all TACACS+ servers are unreachable, all commands except **exit**, **quit**, and **logout** will fail authorization, and will not be executed.

2. Apply method lists to types of access.

   The method lists can be configured on console and TTY lines. So when users connect to the device via the on-board console port (line console 0), the method list configured on console 0 will be applied to authorizing their commands. Similarly, when users connect by Telnet or SSH, the method list configured on the vty lines will be applied to authorizing their commands.

If a method list is created with the name **default** it is automatically applied to all access lines that have not had another named method list applied to them.

Additionally, you may want command authorization to apply to commands in config mode. If so, this can be enabled with the command **aaa authorization config-commands**.

Follow the steps below to configure TACACS+ command authorization:

Step 1. Configure the device connection to the server	
`awplus#` `configure terminal`	Enter Global Configuration mode.
`awplus(config)#` `tacacs-server host {<host-name>|<ip-address>} [key [8]<key-string>]`	Specify the IP address or host name of the remote TACACS+ server host and the shared secret key to use with the specified TACACS+ server. Specify **8** if you are entering a password as a string that has already been encrypted instead of entering a plain text password. As many as four TACACS+ servers can be configured and consulted for authentication and accounting. The first server configured is regarded as the primary server and if the primary server fails then the backup servers are consulted in turn.
Step 2. Define the method list for TACACS+ command authorization	
`awplus(config)#` `aaa authorization commands <level> {<list-name>|default} group tacacs+ [none]`	Define a named method list that will be used for TACACS+ command authorization. Note that while multiple authorization method lists can be defined only the set of all configured TACACS+ servers is currently supported on AlliedWare Plus. **level**: this is the set of commands the method list will be used to authorize. **group tacacs+**: this is the set of all configured TACACS+ servers. **none**: when specified, will provide a local fall-back to command authorization. If authorization servers become unavailable then the device will accept all commands normally allowed for the privilege level of the user. The default list can be configured if **default** is specified instead of a list-name. This default configuration list applies to all console/virtual terminal connections that do not have a method list applied (see Step 3).
Step 3. Apply method list to access lines	
`awplus(config-line)#` `authorization commands <level> [<list-name>|default]`	Once a method list is defined it can be applied to a line or set of lines (console/virtual terminal connections). The **default** list is applied to all lines do not have a method list applied.
Step 4. Enable authorization of configuration commands	
`awplus(config)#` `aaa authorization config-commands`	Optionally, authorization of configuration command can be enabled. If it is not enabled then all configuration commands are accepted by default including command authorization configuration commands.
Step 5. Set the source IP interface for TACACS+ communication	
`awplus(config)#` `ip tacacs source-interface {<interface-name>|<ip-address>`	By default, TACACS+ packets use the source IP address of the egress interface. This command configures a specific IP address or interface to be used for the source IP of all TACACS+ packets.

TACACS+ command authorization configuration example

Example

Once a TACACS+ server is configured a basic TACACS+ command authorization configuration is as follows:

Output 2: Sample TACACS+ command authorization configuration

```
awplus# configure terminal
awplus(config)# tacacs-server host 10.10.10.2 key secretKey
awplus(config)# aaa authorization commands 15 TAC15 group tacacs+
awplus(config)# line vty 0 5
awplus(config-line)# authorization commands 15 TAC15
awplus(config-line)# exit
awplus(config)# aaa authorization config-commands
```

The lines in this example TACACS+ achieve the following:

- The **configure terminal** command enters global configuration mode.
- The **tacacs-server host 10.10.10.2 key secretKey** command defines the TACACS+ server at 10.10.10.2 with the globally shared secretKey.
- The **aaa authorization commands 15 TACS15 group tacacs+** command defines a method list named TACS15 to authorize privilege level 15 commands.
- The **line vty 0 5** command enters line configuration mode.
- The **authorization commands 15 TACS15** command applies the TACS15 method list to all access lines 0 - 5.
- The **exit** command switches back to global configuration mode.
- The **aaa authorization config-commands** command enables authorization on the configuration commands.

The TACACS+ status can be viewed with the **show tacacs+** command.

Output 3: Example output from show tacacs+

```
awplus# show tacacs+
TACACS+ Global Configuration
  Source Interface    : not configured
  Timeout             : 5 sec

 Server Host/      Server
 IP Address        Status
 ------------------------
 10.10.10.2        Alive
```

Information regarding applied method lists can be viewed with the **show aaa server group** command.

Output 4: Example output from **show aaa server group**

```
awplus# show aaa server group
User           List Name          Method                   Acct-Event
======== ==== ================== ================== ====== ==========
login    auth default            -                  local  -
-------- ---- ------------------ ------------------ ------ ----------
cmd-1    auth -                  -                  -      -
-------- ---- ------------------ ------------------ ------ ----------
cmd-7    auth -                  -                  -      -
-------- ---- ------------------ ------------------ ------ ----------
cmd-15   auth TAC15              tacacs+            group  -
-------- ---- ------------------ ------------------ ------ ----------
login    acct -                  -                  -      -
-------- ---- ------------------ ------------------ ------ ----------
dot1x    auth -                  -                  -      -
-------- ---- ------------------ ------------------ ------ ----------
dot1x    acct -                  -                  -      -
-------- ---- ------------------ ------------------ ------ ----------
auth-mac auth -                  -                  -      -
-------- ---- ------------------ ------------------ ------ ----------
auth-mac acct -                  -                  -      -
-------- ---- ------------------ ------------------ ------ ----------
auth-web auth -                  -                  -      -
-------- ---- ------------------ ------------------ ------ ----------
auth-web acct -                  -                  -      -
-------- ---- ------------------ ------------------ ------ ----------
openvpn  auth -                  -                  -      -
-------- ---- ------------------ ------------------ ------ ----------
```

C613-22048-00 REV B

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