# *Configuring AAA Services*

**Cisco devices can use two kinds of AAA services,**

**Remote Authentication Dial In User Service (RADIUS)**

**and**

**Terminal Access Controller Access-Control System Plus (TACACS+).**

## Defining RADIUS and TACACS+

**The two most frequently used AAA protocols are RADIUS and TACACS+. Either one can be used in a Cisco router environment:**

**RADIUS is an open-source standard maintained by the Internet Engineering Task Force (IETF)**

**TACACS+ is a Cisco proprietary protocol that was implemented as an enhancement over RADIUS. In particular TACACS+ includes the ability to separate authorization from authentication and accounting.**

# Comparison of RADIUS and TACACS+

| RADIUS | TACACS+ |
|---|---|
| Uses UDP as the transport. | Uses TCP as the transport. |
| Encrypts only the password. | Encrypts the entire body of the packet, excluding the header. |
| Combines authentication and authorization. | Separates the authentication from the authorization and accounting functions. |
| Limited support for certain protocols. | Full multiprotocol support. |
| Vendor implementations often differ (even though it is an open standard). Interoperability can be an issue. | Specific to Cisco equipment. |
| Traffic is minimal due to limited command support. | Traffic can be significantly higher than with RADIUS because TACACS+ supports more commands and capabilities. |

# RADIUS

**RADIUS uses specific message types to establish communication between the device (in this case our router) and the RADIUS server itself.**

**There are four message types:**

*1.* ***ACCESS-REQUEST:*** This message commonly contains the **username** and **password** and can contain other attributes (see the description of attribute-value pairs after this list) and is **the initial message sent from the router to the RADIUS server.**

2. *ACCESS-ACCEPT*: This is the message provided by the RADIUS server that indicates that the username and password were correct.

3. *ACCESS-REJECT*: This is the message provided by the RADIUS server that indicates that the username and password were incorrect.

4. *ACCESS-CHALLENGE*: This message is provided when an additional form of authentication is employed, such as a token or a personal identification number (PIN).

## Operation of RADIUS in depth

1. The client initiates the conversation by attempting to access the router.
2. That request prompts a username query from the router.
3. The client sends the username to the router.
4. The router requests the password.
5. The client then provides the password to the router.
6. The router takes the username and password information provided and sends it in an ACCESS-REQUEST message to the RADIUS server.

7. If the username and password are correct, the RADIUS server will provide an ACCESS-ACCEPT message back to the router and access is granted. If, on the other hand, the username and password combination are incorrect, the RADIUS server will pass back an ACCESS-REJECT message and the router will end the conversation.

## TACACS+

**Terminal Access Controller Access-Control System Plus (TACACS+) was created by Cisco to achieve a higher degree of control over the authentication process.**

1. User makes a request to log in to a router.
2. The router requests the username from the TACACS+ server.
3. The TACACS+ server provides a username prompt to the router.
4. The router provides the username prompt to the user.
5. The user inputs the username at the prompt.

6. The router then forwards the username to the TACACS+ server.

7. The router requests a password prompt from the TACACS+ server.

8. The TACACS+ server provides a password prompt to the router.

9. The password prompt is then provided to the user from the router.

10. The user inputs a password at the prompt.

11. The router forwards the password to the TACACS+ server.

12. The TACACS+ server sends one of four response messages: ACCEPT, REJECT,ERROR, CONTINUE.

## Configuring Authentication

**Here you will learn how to use a local database to authenticate users.**

## AAA Local User Authentication

1. Turn on AAA services using the aaa new-model command as shown here:

**Router1(config)# aaa new-model**

2. Add a user name and password using the following syntax:

**Router1(config)# username username password password**

3. Define the login default for AAA as a local database. Use the following syntax:

**Router1(config)# aaa authentication login default local**

## Using Method Lists

The following methods are available for authenticating the user:

**Local** -The local username database is being used to authenticate the user.

**Enable** - The enable password is being used to authenticate the user.

**RADIUS** - A RADIUS server is being used to authenticate the user.

**TACACS+** - A TACACS+ server is being used authenticate the

user.

**Line** - A line password is being used to authenticate the user.

## Configuring Authorization

**Router1(config) #** aaa authorization?

```
auth-proxy       For Authentication Proxy Services
cache            For AAA cache configuration
commands         For exec (shell) commands.
config-commands  For configuration mode commands.
```

```
configuration    For downloading configurations from AAA server
console          For enabling console authorization
exec             For starting an exec (shell).
ipmobile         For Mobile IP services.
network          For network services. (PPP, SLIP, ARAP)
reverse-access   For reverse access connections
template         Enable template authorization
```

**There is an option to provide an EXEC shell to someone who has already authenticated.**

**aaa authorization exec test2 if-authenticated**

# Configuring Accounting

The syntax of aaa accounting is as follows:

```
aaa accounting {auth-proxy | system | network | exec | connection | commands
level} {default | list-name} {vrf vrf-name} {start-stop | stop-only | none}
{broadcast} group group-name
```

# Configuring TACACS+

There are three basic steps to configuring a router to use a TACACS+ server:

1. Configure AAA services globally using the aaa new-model command.
2. Configure the server or servers you are going to use by specifying their IP addresses.
3. Configure an encryption key that prevents someone from putting a rogue TACACS+ server on the network.

```
Router1# aaa new-model
Router1# tacacs-server host 172.16.100.100 single-connection
Router1# tacacs-server host 172.16.100.101 single-connection
Router1# tacacs-server key mys3cret
```