



Romel Cabling ▾



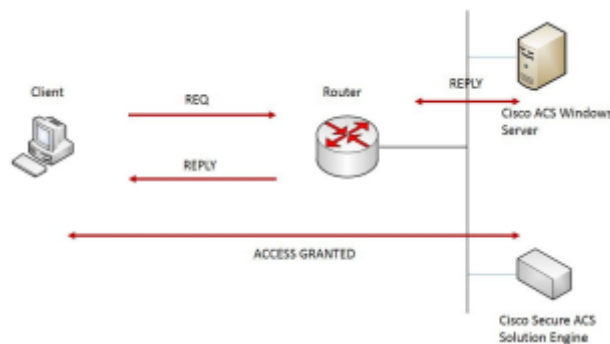
Home

Home > My courses > 121 - ITSP2B > 10 Implementing the AAA Framework: Implementing A... > Lesson Proper for Week 10

# Lesson Proper for Week 10

## IMPLEMENTING AUTHENTICATION USING EXTERNAL SERVICES

Due to the scaling of large networks, creating a user account on each router can be an inconvenience. If the account's details are adjusted on one device, the network engineer will need to replicate the changes to all other devices on the network individually. A convenient solution to adjust scaling and ensuring that all of the accounts and privileges are kept synchronized is to use a centralized AAA server such as a Cisco **Access Control Server (ACS)** or a Cisco **Identity Services Engine (ISE)**:



The user accounts are created on the ACS or ISE appliance. The routers and switches are configured to query the AAA server if they receive any login requests. The AAA server would also be responsible for providing privileges and getting logs of the activities of each user.

Examples of these security protocols are as follows:

- RADIUS
- TACACS+



## TACACS+

This is a Cisco proprietary third-generation protocol that facilitates the use of AAA services. This protocol is derived from TACACS and XTACACS, and supports authentication, authorization, and accounting. Multiple servers can be used to handle different services. For example, one server can be used to handle authentication and another server can be used to handle authorization for a router.

TACACS+ provides additional layers of security by encrypting the messages between the client and the AAA server.

Here are the some of the special features of TACACS+:

- TACACS+ supports authorization commands with some advanced authentication mechanisms like Data Encryption Standard and one-time password (OTP) keys
- TACACS+ supports all 16 privilege levels (0-15)
- TACACS+ allows the blocking of specific port services such as a TTY or VTY
- The TACACS+ AAA server can contain an internal database size up to 5,000 users
- A TACACS+ server acts as a proxy server which authenticates, authorizes, and accounts access details

## CONFIGURING TACACS+



The following are the steps involved to configure external authentication using TACACS+.

1. Creating a username and password:

```
| Router (config) # username ccnasecurity secret cisco
```

2. Enabling AAA on the device:

```
| Router (config) # aaa new-model
```

3. Configuring the TACACS+ server. The next step is to configure the router to point to the TACACS+ server that has been created. This can be achieved by two methods. The first is to create a pointer on the router by specifying the IP address of the TACACS+ server and the shared key:

```
| Router (config) # tacacs-server host 10.10.10.10 key secretkey
```

While the second is to create a group of TACACS+ servers and define the same:

```
| Router (config) # aaa group server tacacs+ Authforlogin  
Router (config-sg-tacacs+) #server 10.10.10.10
```

4. Defining a method list for AAA. The next step is to define a method list for AAA logins using the following parameters:

```
| Router (config) # aaa authentication login default group tacacs+ local
```

Where:

- The keyword `aaa authentication login` specifies that this is only used for login authentication
- The keyword `default` is used in case of a custom name or when only one default list can be created for each function of AAA
- The keyword `group tacacs+` specifies the user who is going to use the configured TACACS+ servers
- The keyword `local` specifies the secondary authentication method in case the TACACS+ server is not reachable

5. Attaching the configured AAA authentication on the line modes:

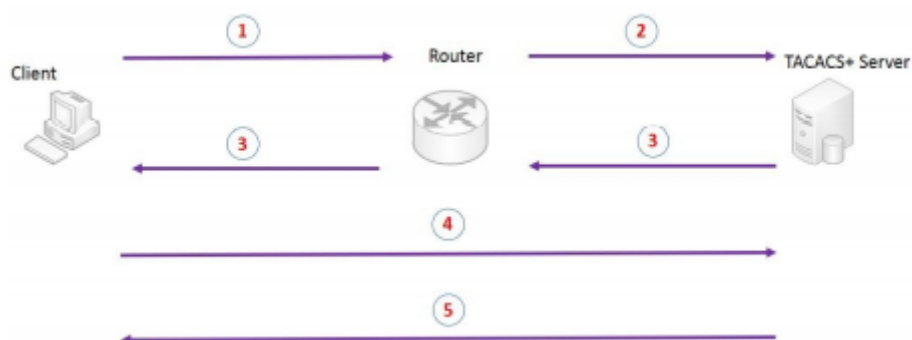
```
| Router (config) # line console 0  
Router (config-line) # login authentication default  
Router (config) # line vty 0 15  
Router (config-line) # login authentication default
```



The keyword `default` here substitutes the default method list available.

## USING AAA WITH TACACS+

Let's consider the example of a user connected to the router, and the TACACS+ server is requesting access to the router. The following are the steps involved in authenticating the user with TACACS+:



1. The **Client** sends a request message to the **Router**
2. The **Router** passes the request to the **TACACS+ Server** and requests for the login text
3. The **TACACS+ Server** prompts for the username and the password, and the **Router** passes the server request to the server
4. The **Client** sends the username and password to the router and the **Router** forwards the same to TACACS+
5. Then, the server replies with an ACCEPT or REJECT code

## **RADIUS**

This is an open standard protocol that works in a client and server model. In the implementation of Cisco, the RADIUS client is configured on the Cisco routers and sends authentication or authorization requests to a RADIUS server which is located centrally.

RADIUS can be implemented in various network environments that are in need of high security levels. Some of the environments where RADIUS can be used are as follows:

1. It can be implemented in networks that are built with different vendor products. RADIUS can act as a single server-based database.
2. In networks environments where smart cards are used.
3. It can be used in environments where administrators need to do accounting independently.
4. It can be used in networks where administrators want to set up pre-authentication profiles. Pre-authentication mainly helps ISP's to manage ports and shared resources depending on the agreed upon service agreements.

On the other hand, RADIUS cannot be used for some situations, and they are as follows:

1. RADIUS does not support some of the protocols like AppleTalk Remote Access (ARA), X.25 PAD connections, and NetBIOS
2. RADIUS does not work on the two-way authentication model
3. RADIUS binds the user client to only one service model and does not support a variety of services

## **CONFIGURING RADIUS**



The following are the steps involved in configuring external authentication using RADIUS:

1. Creating a username and password:

```
| Router (config) # username ccnasecurity secret cisco
```

2. Enabling AAA on the device:

```
| Router (config) # aaa new-model
```

3. Configuring the RADIUS server. The next step is to configure the router to point to the RADIUS server that has been created. This can be achieved by creating a pointer on the router by specifying the IP address of the RADIUS server and the shared key:

```
| Router (config) # radius-server host 10.10.10.10  
Router (config) # radius-server key thesecretkey
```

4. Defining a method list for AAA. The next step is to define a method list for AAA logins using the following parameters:

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

5. Attaching the configured AAA authentication on the line modes:

```
| Router (config) # line console 0  
Router (config-line) # login authentication default  
Router (config) # line vty 0 15  
Router (config-line) # login authentication default
```

◀ Preliminary Activity for Week 10

Jump to...



Analysis, Application, and Exploration for Week 10 ▶

## Navigation

Home

 Dashboard

Site pages

My courses

121 - CC106

121 - BPM101 / DM103

121 - OAELEC2

121 - ITE3

121 - MUL101

121 - ITSP2B

Participants

 Grades

General

01 Exploring Security Threats

02 Delving into Security Toolkits


03 Intrusion Prevention System





- 04 Understanding Security Policies I
- 05 Understanding Security Policies II
- 06 - Preliminary Examination
- 07 Deep Diving into Cryptography
- 08 Deep Diving into Cryptography: Types of Cipher
- 09 Implementing the AAA Framework
- 10 Implementing the AAA Framework: Implementing A...


 Preliminary Activity for Week 10

 **Lesson Proper for Week 10**

 Analysis, Application, and Exploration for Week 10

 Generalization for Week 10

 Evaluation for Week 10

 Assignment for Week 10

11 Securing the Control and Management Planes

12 - Midterm Examination

13 Protecting Layer 2 Protocols

14 Protecting the Switch Infrastructure

15 Exploring Firewall Technologies I

16 Exploring Firewall Technologies II

17 Cisco ASA

121 - WEB101 / CCS3218

Courses

---

## Fair Warning

**NOTICE:** Please be reminded that it has come to the attention of the Publishing Team of eLearning Commons that learning materials published and intended for ***free use only by students and faculty members within the eLearning Commons network were UNLAWFULLY uploaded in other sites without due and proper permission.***

**PROSECUTION:** Under Philippine law (Republic Act No. 8293), copyright infringement is punishable by the following: Imprisonment of between 1 to 3 years and a fine of between 50,000 to 150,000 pesos for the first offense. Imprisonment of 3 years and 1 day to six years plus a fine of between 150,000 to 500,000 pesos for the second offense.

**COURSE OF ACTION:** Whoever has maliciously uploaded these concerned materials are hereby given an ultimatum to take it down within 24-hours. Beyond the 24-hour grace period, our Legal Department shall initiate the proceedings in coordination with the National Bureau of Investigation for IP Address tracking, account owner identification, and filing of cases for prosecution.





**Enrollment registration is now Ongoing**  
**For 2nd Semester SY 2021 - 2022**  
*We are accepting new students, returnees and transferees.*





visit [www.bcp.edu.ph](http://www.bcp.edu.ph)

**"Be trained to be the best,  
Be linked to success"**

 [bcp-inquire@bcp.edu.ph](mailto:bcp-inquire@bcp.edu.ph)  (8)442-8601 | (8)518-8050

The banner features a blue-tinted image of a multi-story building with a 'BCP' sign on the roof. A large white diagonal banner contains the enrollment text. The bottom right corner includes a quote, a circular logo, and contact information.

## **Activities**

-  Assignments
-  Forums
-  Quizzes
-  Resources

Bestlink College of the Philippines  
College Department

Powered by [eLearning Commons](#)

