



**Romel Cabling** ▾



[Home](#)

[Home](#) > [My courses](#) > [121 - ITSP2B](#) > [09 Implementing the AAA Framework](#) > [Lesson Proper for Week 9](#)

## Lesson Proper for Week 9

The acronym AAA stands for authentication, authorization, and accounting.

- **Authentication:** This process ensures that when a user enters a username and password combination that it is validated if the user says who they are before access is granted on the system.
- **Authorization:** After the authentication phase is completed, the second step is to assign privileges to the user's account. The authorization aspects provides privileges for the user and determines what the user can or cannot do on the system.
- **Accounting:** This is about tracing and tracking the user once he/she logs into the system. Tracking is necessary for the administrator to understand the security measures taken and to perform investigation when a threat or an attack occurs.

The benefits of AAA are that it:

- Provides increased availability and scalability
- Increases control and flexibility
- Provides standard authentication methods

AAA is used to identify and verify the user on the management plane of the device. The use of AAA is that it creates a local database for usernames and passwords by means of running a configuration. If the administrators wants to allow multiple users to access the devices in the network, a centralized database which lists authorized users is



created to authenticate the users. This is what an access control server also performs. A list of allowed and authorized usernames and passwords are configured on the ACS server and configure the devices that should refer to any of its decisions about authentication or authorization on the ACS server.

AAA allows a network device that a user is requesting to access management via **TACACS** (short for **Terminal Access Controller Access Control System**), **RADIUS** (**Remote Authentication Dial-In User Service**), **LDAP** (**Lightweight Directory Access Protocol**), or Microsoft Active Directory. Even though every method has multiple disadvantages, one common advantage is that you can log the user's request centrally with the help of a database. The other advantage is that it helps to have a single sign-on as the credentials are stored in the central database and used by the network device to authenticate a login request.

The problem with external authentication is that if the database fails, the reachability to the server gets affected. This issue can be solved by migrating the database to a local user database. Once the user is authenticated, the next step is about authorizing and controlling the users and what they can access. This might require some tools like **Cisco Access Control Server (Cisco ACS)** or the Identity **Services Engine (ISE)**. After successful authorization that is permitting or denying a user from accessing certain resources, AAA also talks about archiving what users have accessed in their respective sessions. The Cisco IOS AAA client may reside on the router or on a **Network Access Server (NAS)** which performs the functions. This model does not scale for larger networks because there can be a large amount of stored data.

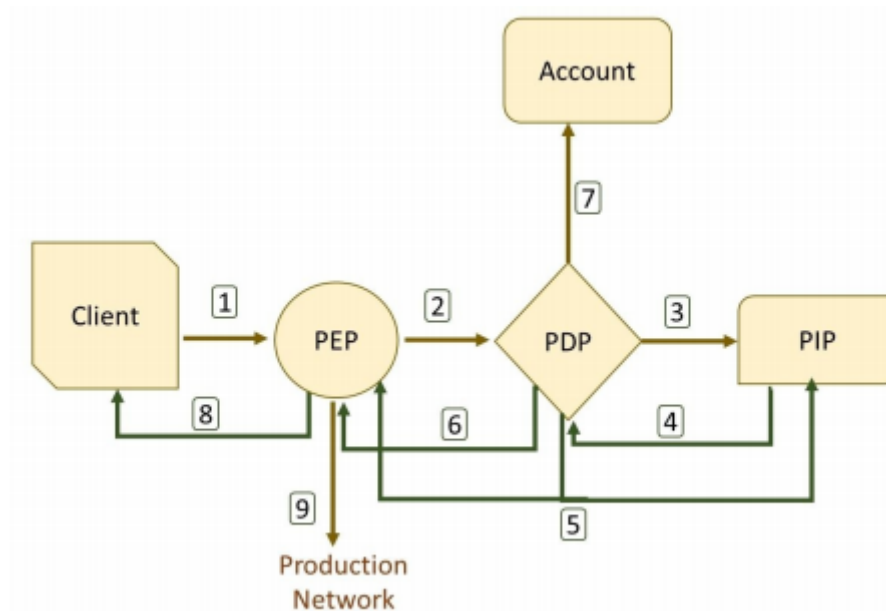
## COMPONENTS OF AAA

Authentication, authorization, and accounting are the functional components, but they also contain certain core components. It's important to understand the core components of AAA and their functions, which are as follows:

- **Client:** A device that attempts to access the network by authenticating itself or acting as substitute to validate the user.
- **Policy Enforcement Point (PEP):** It implements the requisites specified by client access. It is also referred to as the authenticator, VPN concentrator, **Wireless Access Point (WAP)**, and so on.
- **Policy Information Point (PIP):** It stores information and facilitates access decisions. A PIP could be a database containing device IDs, a user directory, or a one-time password, to name a few.
- **Policy Decision Point (PDP):** It is responsible for collecting access requests from the PEP and also assigning the PIP to collect more information that would help in making an access decision. It is responsible for making the final decision about the network.
- **Accounting and Reporting System:** This feature tracks the use of the network and recognizes the identity, location, and the resources accessed by the user.



The following diagram explains the components and operation of AAA:



First, the client establishes connectivity with the network, and is then asked to provide identification before sending the message to PEP. Next, the information received by PEP is sent to PDP whereupon the PDP collects information from PIP about the client and authenticates the information. The PIP validates the user's credentials and send a success or failure message. It also sends additional information such as the role, location, and so on about the client to the PDP for evaluation.

First, the client establishes connectivity with the network, and is then asked to provide identification before sending the message to PEP. Next, the information received by PEP is sent to PDP whereupon the PDP collects information from PIP about the client and authenticates the information. The PIP validates the user's credentials and send a success or failure message. It also sends additional information such as the role, location, and so on about the client to the PDP for evaluation.

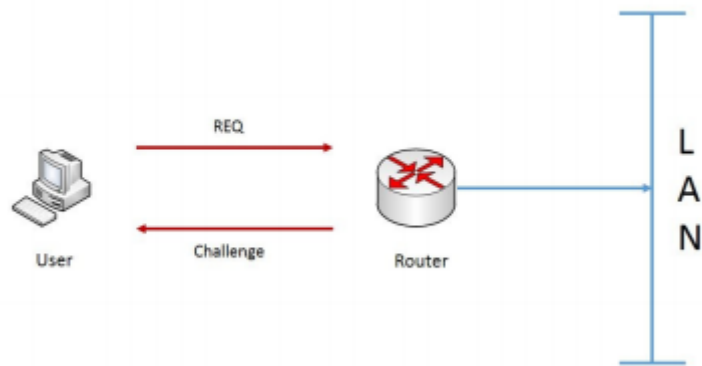
## IMPLEMENTING CISCO AAA - AUTHENTICATION

AAA can be implemented in two forms: either locally on a device or with TACACS+ or RADIUS.

### 1. Implementing authentication using local services

In this section, we going to take look at implementing authentication on the Cisco IOS router. This feature will enable the router to act as an authentication server with all of the user accounts that are created and stored on the device itself:





Whenever a user tries to log in, the router will query the local database to validate if the username and password combination exists and is accurate. If yes, this proves to the router that the user has validated their identity and is who they say they are.

The following are the steps to enable AAA using local services:

1. Enable AAA on the routers. On the CLI, use the following command. This command enables AAA and unlocks all other subcommands:

```

Router enable
Router # configure terminal
Router(config) # aaa new-model

```

2. Enable the username and password. The next step after you enable AAA is to create a username and password. The username and password can either be in the form of plain text or in encrypted form:

```

Router (config)# username ccnasecurity password cisco

```

3. The preceding command shows how to enable plain text. The following command shows how to create an encrypted password instead of plain text. This uses a MD5 hashing method for encryption:

```

Router (config)# username ccnasecurity secret cisco

```

3. Configure the device to use the local database:

```

Router (config) # aaa authentication login default local

```

4. This command creates a method list so that you can use the local authentication database. The preceding command can be explained as follows:



- **aaa:** Enables the AAA feature on the router:

```
Router(config)# aaa ?
accounting Accounting configurations parameters.
authentication Authentication configurations parameters.
authorization Authorization configurations parameters.
!! Output Omitted !!
```

- **authentication:** Specifies the set of configurations for authentication, authorization, or accounting:

```
Router(config)# aaa authentication ?
enable Set authentication list for enable.
login Set authentication lists for logins.
!! Output Omitted !!
```

- **login:** Prompts the username and password while trying to log in via console, TTY, VTY, and auxiliary. This command is only used for administration access:

```
Router(config)# aaa authentication login ?
WORD Named authentication list (max 31 characters, longer will be
rejected).
default The default authentication list.
```

- **default:** To make the router use the default method list:

```
Router(config)# aaa authentication login default ?
enable Use enable password for authentication.
group Use Server-group
line Use line password for authentication.
local Use local username authentication.
none NO authentication.
```

- **local:** This tells the router to use the local database as a reference:

```
Router(config)# aaa authentication login default local
```

◀ Preliminary Activity for Week 9

Jump to...



Analysis, Application, and Exploration for Week 9 ▶



## 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

 Preliminary Activity for Week 9

 **Lesson Proper for Week 9**

 Analysis, Application, and Exploration for Week 9

 Generalization for Week 9

 Evaluation for Week 9

 Assignment for Week 9

10 Implementing the AAA Framework: Implementing A...

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,



## 2nd Semester Enrollment



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

# Enrollment registration is now Ongoing





## For 2nd Semester SY 2021 - 2022

We are accepting new students, returnees and transferees.

"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

## Activities

-  Assignments
-  Forums
-  Quizzes
-  Resources

