Name of candidate:		
Roll no.:	**Year: BE**	**Semester: -VII**
Branch: IT	**Subject: Advance Security Lab**	
Experiment No.: 09	**Date of performance:**	**Date of submission:**
LO's Covered: LO5		

Rubrics for Practical

Indicator	**Poor**	**Average**	**Good**	**Excellent**
Timeline (2)	More than two weeks late (0)	Two weeks late (0)	One week late (1)	Early or on time (2)
Knowledge (4)	Not Able to answer any Question (0)	Able to answer a Question (2)	Able to answer few Questions (3)	Able to answer all questions (4)
Performance (4)	Able to partially perform the experiment (1)	Able to perform the experiment for certain extent (2)	Able to perform the experiment with support (3)	Able to perform the experiment considering all aspects (4)
Rubrics	**Timeline(2)**	**Knowledge(4)**	**Performance(4)**	**Total (10)**
Score				

Signature of faculty:

Experiment No. 09

Aim: Exploring AAA using RADIUS and TACACS+ in Packet tracer

Theory:
AAA stands for Authentication, Authorization, and Accounting.

Authentication

- Refers to confirmation that a user who is requesting a service is a valid user.
- Accomplished via the presentation of an identity and credentials.
- Examples of credentials include passwords, one-time tokens, digital certificates, and phone numbers (calling/called).

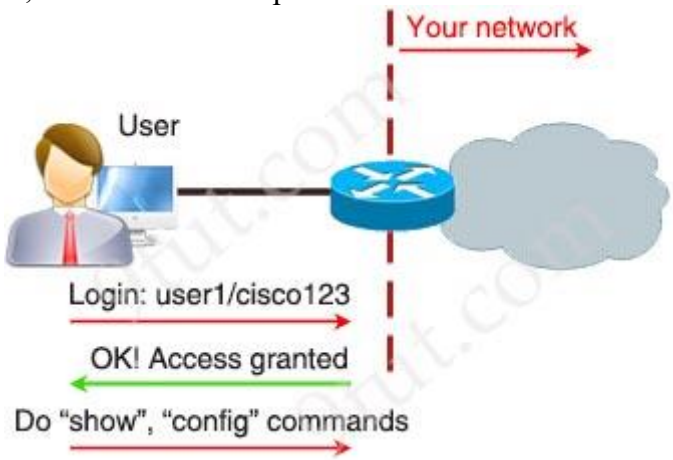
Authorization

- Refers to the granting of specific types of service (including "no service") to the users based on their authentication.
- May be based on restrictions, for example, time-of-day restrictions, or physical location restrictions, or restrictions against multiple logins by the same user.
- Examples of services include, IP address filtering, address assignment, route assignment, encryption, QoS/differential services, bandwidth control/traffic management, etc.

Accounting

- Refers to the tracking of the consumption of network resources by users.
- Typical information that is gathered in accounting include the identity of the user, the nature of the service delivered, when the service began, and when it ended.
- May be used for management, planning, billing, etc.

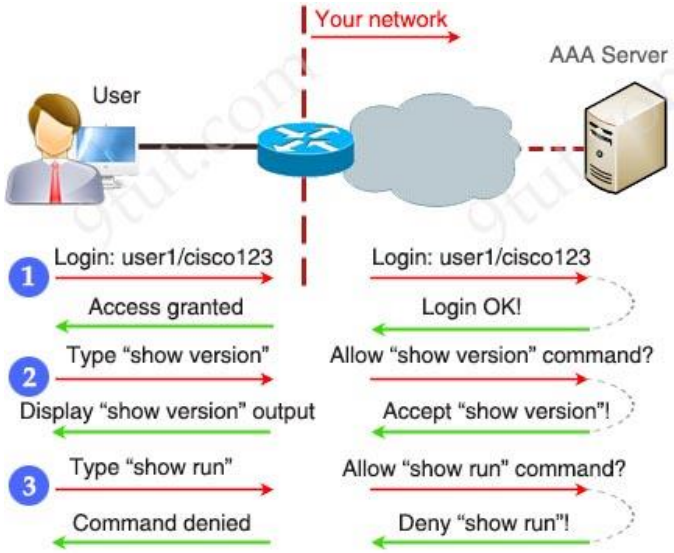
When your company grows bigger and bigger, there is a moment that you need to consider implementing security to your network. There are many ways to secure a network but AAA offers a complete solution. In this tutorial let's find out about this security feature.
Before diving into AAA, let's take an example of a user who wants to connect to our network.



This process uses a login and password on the access line. Although it is very easy to implement, but there are many disadvantages of using this method:

- Insecure login method
- Vulnerable to brute-force attacks
- No accountability
- Must be configured on each device manually
- Store usernames & passwords locally on each device
- Cannot limit which specific commands are not used

With AAA, now the process of a user connecting to our network is shown below:



With AAA, users must authenticate before getting an IP address to access the network. Otherwise, they can only use specific protocols to continue authenticating

For authentication we can do via local database, 802.1x standard (which was developed to provide a method to authenticate devices attempting to access a switchport/LAN) or via remote AAA servers. There are two popular client/server AAA protocols to communicate between remote AAA servers and authenticating devices:

- **RADIUS** (Remote Authentication Dial In User Service)
- **TACACS+** (Terminal Access Controller Access-Control System)

The comparison of two protocols is listed below:

	RADIUS	**TACACS+**
Transportation & Ports	**UDP** port 1812/1645 (Authentication) 1813/1646 (Accounting)	**TCP** port 49
Encryption	only passwords	entire payload of each packet (leaving only the TACACS+ header in cleartext)
Standards	Open standard	Cisco proprietary (but actually now it is an open standard defined by RFC1492)
Operation	**Authentication and authorization are combined** in one function	**authentication, authorization and accounting are separated**
Logging	No command logging	Full command logging (commands typed by users can be recorded on the servers)

AAA stands for Authentication, Authorization and Accounting.

- **Authentication:** Specify who you are (usually via login username & password)
- **Authorization**: Specify what actions you can do, what resource you can access
- **Accounting**: Monitor what you do, how long you do it (can be used for billing and auditing)

An example of AAA is shown below:

- **Authentication:** "I am a normal user. My username/password is **user_tom/learnforever**"
- **Authorization**: "**user_tom** can access **LearnCCNA** server via **HTTP** and **FTP**"
- **Accounting**: "**user_tom** accessed **LearnCCNA** server for **2 hours**". This user only uses "show" commands.

AAA Configuration

The following steps are required to configure AAA:

1. Enable the "new model" of AAA.
2. Configure the server(s) to be used for AAA (e.g. TACACS+ or RADIUS servers).
3. Define authentication and authorization method lists.
4. Enforce AAA authentication on the relevant lines (e.g. console and VTY lines).

Example:

In this example we will do an **Authentication configuration** so that the users are authenticated when telnet to the device:

1. Globally enables AAA on a device:

```
Switch(config)#aaa new-model
```

2. We are going to configure the server to be used for AAA and the key; note that the key used is the same key that was configured on the RADIUS server.

```
Switch(config)#radius-server host 192.168.1.2 key MySecretP@ssword
```

In the above command we don't specify the ports used for RADIUS authentication and accounting so it will use the default values of 1645 and 1646, respectively (or we can specify them via the "radius-server host 192.168.1.2 **auth-port** 1645 **acct-port** 1646 key MySecretP@ssword" command). The full syntax of above command is:

Switch(config)# **radius-server host** { *hostname* | *ip-address* } [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] [*alias* {hostname | ip address}]

3. We will activate authentication for logins to the device and specify that RADIUS is the preferred method but we should include the local user database as a fall back if RADIUS becomes unavailable. Note that users in the local database cannot be used if the user doesn't exist in RADIUS, it will only fall back if the RADIUS server is offline.

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

This command is broken down as follows:

- The '**aaa authentication**' part is simply saying we want to configure authentication settings.
- The '**login**' is stating that we want to prompt for a username/password when a connection is made to the device.
- The '**default**' means we want to apply for all login connections (such as tty, vty, console and aux). If we use this keyword, we don't need to configure anything else under tty, vty and aux lines. If we don't use this keyword then we have to specify which line(s) we want to apply the authentication feature. An example of not using the 'default' keyword is shown in step 4 below.
- The '**group radius local**" means all users are authenticated using RADIUS servers (the first method). If the RADIUS servers don't respond (unreachable), then the router's local database is used (the second method). But notice that if the RADIUS server is **reachable** while the user has not configured on it, it will **not** fallback and try to search in the local database. It will display**% Authentication failed** message.

Note: If we don't have the 'local' keyword (only 'aaa authentication login default group radius' command then the authentication will fail if the AAA server does not reply to the authentication request as there is no fallback authentication method)

For local authentication to work we need to create a local user. To create a new user, with password stored in plain text:

```
Switch(config)#username User1 password CCNA_cisco
```

But having passwords in plain text isn't a good idea! The below command is better to create a new user, with password stored in encrypted text:

```
Switch(config)#username test2 secret Pa55w0rd
```

specify the RADIUS server and a group to be used.

4. In step 3, if we don't use the 'default' login method list, for example:

```
Switch(config)#aaa authentication login MY_AUTHEN_GROUP group radius local
```

Then we have to configure the same group (MY_AUTHEN_GROUP in this case) to the specific line(s) with the "**login authentication** *list_name*" command. For example we want to apply to VTY lines (for telnet):

```
Switch(config)#line vty 0 4
Switch(config)# login authentication MY_AUTHEN_GROUP
```

Note:

- We can configure different usernames/passwords on the local device and the remote AAA server but for normal users we should configure same usernames/passwords on both devices so that the transition (in case the remote AAA server fails) is transparent to them.
- Use the **aaa authentication** global configuration command to define method lists for RADIUS authentication
- Use the **aaa authorization** global command to authorize specific user functions
- Use the **aaa accounting** command to enable accounting for RADIUS connections

So in conclusion this is all the config we need for a simple authentication using AAA:

```
Switch(config)#username test2 secret Pa55w0rd
Switch(config)#aaa new-model
Switch(config)#radius-server host 192.168.1.2 key MySecretP@ssword
Switch(config)#aaa authentication login MY_AUTHEN_GROUP group radius local
Switch(config)#line vty 0 4
Switch(config)# login authentication MY_AUTHEN_GROUP
```

A simple TACACS+ configuration for authentication would be:

```
aaa new-model
aaa authentication login default group tacacs+ local
tacacs-server host 10.10.10.1
tacacs-server key login@pass!
```

With this configured, when logging in, the password supplied will be attempted to be verified by the TACACS+ server before access is granted. If the server is unavailable/unreachable, then the switch will fall back to using the local authentication database.

Conclusion:

Post Lab:

1. Discuss Advantages and Disadvantages of AAA
2. Suppose we configure AAA as follows.

```
aaa authentication login NO_AUTH none

line console 0
login authentication NO_AUTH
```

   Which login credentials are required when connecting to the console port in this output?
3. Which login credentials are required when connecting to the VTY port in this output?

```
Router(config)# aaa authentication login default tacacs+ enable
```

1. Advantages:
   - Secure login (AAA server is not exposed to users and only some protocols are allowed to be sent initially)
   - Easy management at one or some centralized servers
   - Firewalls or other security devices can be placed before AAA servers to protect them
   - Can accept or reject specific commands
   - Every command typed by users can be logged for later analysis

   Disadvantages:
   - Require powerful server (to handle all the traffic and requests)

2. The console port is authenticated with NO_AUTH list. But this list does not contain any authentication method (it uses "none") so no authentication is required when connecting to the console port.
3. The router first attempts to use the TACACS+ method for authentication, then the *enable* method. Therefore, the enable password is used to authenticate users if the device cannot contact the TACACS+ server.