# AAA on Cisco Devices

Goal: Implement basic AAA and use it for authentication on CISCO Routers and Switches.

# Lab Topology:

A diagram of a computer network

Description automatically generated

Contents

[AAA on Cisco Devices 1](#_Toc169081492)

[Lab Topology: 1](#_Toc169081493)

[Task 1 – Open Packet Tracer file 2](#_Toc169081494)

[Task 2 – Basic Device 3](#_Toc169081495)

[Task 3 – Configuring AAA Server in Packet Tracer 3](#_Toc169081496)

[Step 1 - Open configuration tab of AAA Server 3](#_Toc169081497)

[Step 2 - Configure AAA account for R1 in AAA Server: 3](#_Toc169081498)

[Step 3 – Add AAA user to AAA server. 4](#_Toc169081499)

[Task 4 – Configure Local AAA Authentication for Console Access on R1 6](#_Toc169081500)

[Step 1 - Configure a local username on R1 6](#_Toc169081501)

[Step 2 - Configure local AAA authentication for console access on R1. 6](#_Toc169081502)

[Step 3 - Configure the line console to use the defined AAA authentication method. 6](#_Toc169081503)

[Step 4 - Verify the AAA authentication method. 6](#_Toc169081504)

[Task 5 – Configure Local AAA Authentication for vty Lines on R1 7](#_Toc169081505)

[Step 1 - Configure domain name and crypto key for use with SSH. 7](#_Toc169081506)

[Step 2: Configure the vty lines to use the defined AAA authentication method. 7](#_Toc169081507)

[Step 3: Verify the AAA authentication method. 7](#_Toc169081508)

[Task 6 - Configure Server-Based AAA Authentication Using RADIUS on R1 7](#_Toc169081509)

[Step 1: Configure the RADIUS server specifics on R1. 7](#_Toc169081510)

[Step 2: Configure AAA login authentication for console access on R1. 8](#_Toc169081511)

[Step 3 - Verify the AAA authentication method for Console lines. 8](#_Toc169081512)

[Step 4 - Verify the AAA authentication method for vty lines. 8](#_Toc169081513)

## Task 1 – Open Packet Tracer file

Download and open lab files:

LAB\_C3NetSec\_8\_PT\_AAA\_on\_Cisco\_Devices-V.1.0.pkt

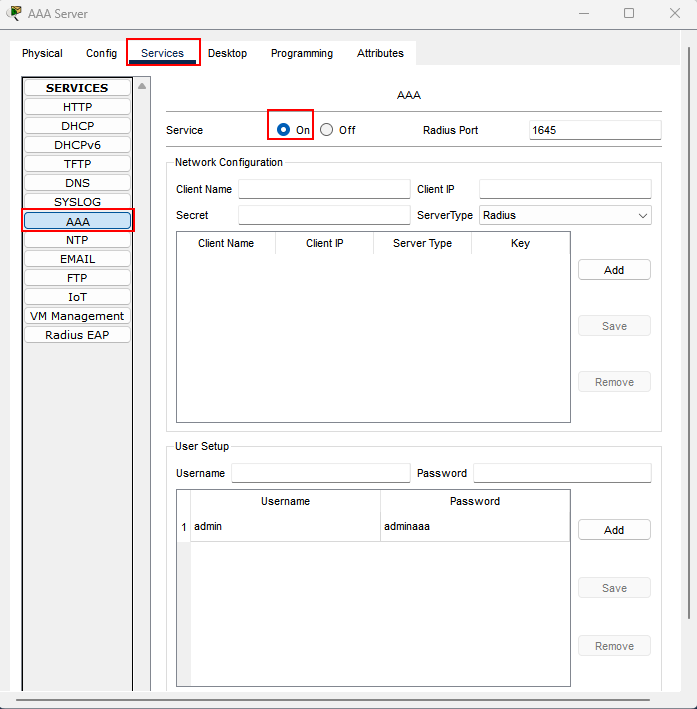
## Task 2 – Basic Device

Configure devices based on table below:

|  |  |  |
| --- | --- | --- |
| Device Name | Interface | IPv4 |
| R1 | Gig0/0/0 | 10.1.1.1/24 |
| SW1 | VLAN1 | 10.1.1.2/24 |
| AAA Server | Fa0 | 10.1.1.3/24 |
| PC1 | Fa0 | 10.1.1.4/24 |

## Task 3 – Configuring AAA Server in Packet Tracer

### Step 1 - Open configuration tab of AAA Server



### Step 2 - Configure AAA account for R1 in AAA Server:

Client name: R1

Client IP: 10.1.1.1

Secret: secretaaa

A screenshot of a computer

Description automatically generated

Click on add and compare screenshots.

A screenshot of a computer

Description automatically generated

### Step 3 – Add AAA user to AAA server.

Create User Account on AAA Server:

Username: **admin**

Password: **adminaaa**

A screenshot of a computer

Description automatically generated

Click on Add.

Screenshot of correct configuration:

A screenshot of a computer

Description automatically generated

## Task 4 – Configure Local AAA Authentication for Console Access on R1

### Step 1 - Configure a local username on R1

Configure a username of **admin** with a secret password of **adminlocal** .

***R1(config)#username admin privilege 15 password adminlocal***

### Step 2 - Configure local AAA authentication for console access on R1.

Enable AAA on R1 and configure AAA authentication for the console login to use the local database.

***R1(config)# aaa new-model***

***R1(config)# aaa authentication login default local***

### Step 3 - Configure the line console to use the defined AAA authentication method.

Enable AAA on R1 and configure AAA authentication for the console login to use the default method list.

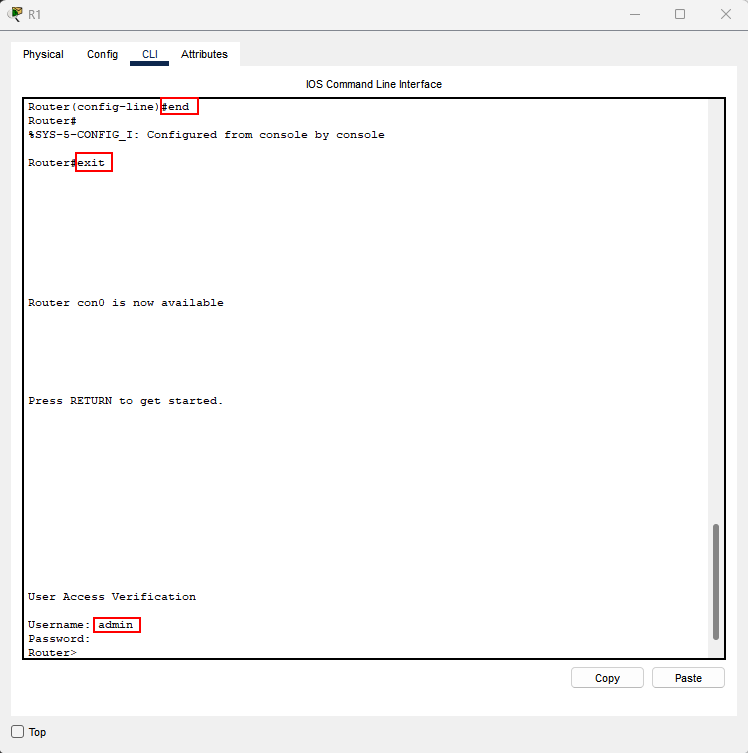
***R1(config)# line console 0***

***R1(config-line)# login authentication default***

### Step 4 - Verify the AAA authentication method.

Verify the user EXEC login using the local database:

Exit to Login Screen as shown on picture below.



Log in using created credentials.

## Task 5 – Configure Local AAA Authentication for vty Lines on R1

### Step 1 - Configure domain name and crypto key for use with SSH.

1. Use cybertech.local as the domain name on R1.

***R1(config)# ip domain-name cybertech.local***

1. Create an RSA crypto key using 2048 bits.

***R1(config)# crypto key generate rsa general-keys modulus 2048***

### Step 2: Configure the vty lines to use the defined AAA authentication method.

Configure the vty lines to use the named AAA method and only allow SSH for remote access.

***R1(config)# line vty 0 4***

***R1(config-line)# login authentication default***

***R1(config-line)# transport input ssh***

***R1(config-line)# end***

### Step 3: Verify the AAA authentication method.

Verify the SSH configuration SSH to R1 from the command prompt of PC1..

***PC1> ssh –l admin 10.1.1.1***

Password: adminlocal

A black background with a black square

Description automatically generated with medium confidence

## Task 6 - Configure Server-Based AAA Authentication Using RADIUS on R1

### Step 1: Configure the RADIUS server specifics on R1.

Configure the AAA RADIUS server IP address and secret key on R1.

Note: The commands radius-server host and radius-server key are deprecated. Currently Packet Tracer does not support the new command radius server.

***R1(config)# radius server AAASRV***

***R1(config-radius-server)#address ipv4 10.1.1.3***

***R1(config-radius-server)#key secretaaa***

A screenshot of a computer error

Description automatically generated

### Step 2: Configure AAA login authentication for console access on R1.

Enable AAA on R1 and configure all logins to authenticate using the AAA RADIUS server. If it is not available, then use the local database.

***R1(config)# aaa authentication login default group radius local***

### Step 3 - Verify the AAA authentication method for Console lines.

Verify the user EXEC login using the AAA RADIUS server.

***R3(config-line)# end***

*%SYS-5-CONFIG\_I: Configured from console by console R3# exit R3 con0 is now available Press RETURN to get started. \*\*\*\*\*\*\*\*\*\*\*\* AUTHORIZED ACCESS ONLY \*\*\*\*\*\*\*\*\*\*\*\*\* UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.*

*User Access Verification Username: admin Password:* ***adminaaa***

***R1>***

### Step 4 - Verify the AAA authentication method for vty lines.

Verify the user remote login using the AAA RADIUS server.

On PC1 connect to R1 using SSH AAA credentials **admin** **adminaaa**