# Lab 04

# Configure AAA Authentication on Cisco Routers

|  |  |
| --- | --- |
| **Name: Syed Asghar Abbas Zaidi** | **Student ID: 07201** |

## 2.1 Objective

The Objectives of this lab are:

* Configure a local user account on R1 and configure authenticate on the console and vty lines using local AAA.
* Verify local AAA authentication from the R1 console and the PC-A client. Packet Tracer - Configure AAA Authentication on Cisco Routers
* Configure server-based AAA authentication using TACACS+.
* Verify server-based AAA authentication from the PC-B client.
* Configure server-based AAA authentication using RADIUS.
* Verify server-based AAA authentication from the PC-C client.

## 2.2 Introduction

The network topology shows routers R1, R2 and R3. Currently, all administrative security is based on knowledge of the enable secret password. Your task is to configure and test local and server-based AAA solutions.

You will create a local user account and configure local AAA on router R1 to test the console and vty logins.

* User account: **Admin1** and password **admin1pa55**

You will then configure router R2 to support server-based authentication using the TACACS+ protocol. The TACACS+ server has been pre-configured with the following:

* Client: **R2** using the keyword **tacacspa55**
* User account: **Admin2** and password **admin2pa55**

Finally, you will configure router R3 to support server-based authentication using the RADIUS protocol. The RADIUS server has been pre-configured with the following:

* Client: **R3** using the keyword **radiuspa55**
* User account: **Admin3** and password **admin3pa55**

The routers have also been pre-configured with the following:

* Enable secret password: **ciscoenpa55**
* OSPF routing protocol with MD5 authentication using password: **MD5pa55**

**Note**: The console and vty lines have not been pre-configured.

**Note**: IOS version 15.3 uses SCRYPT as a secure encryption hashing algorithm; however, the IOS version that is currently supported in Packet Tracer uses MD5. Always use the most secure option available on your equipment.

**Topology**

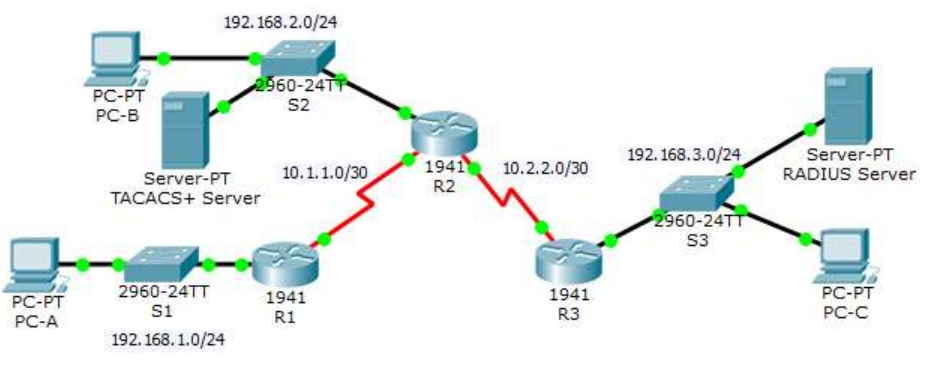


Figure 1: Topology

**Addressing Table**

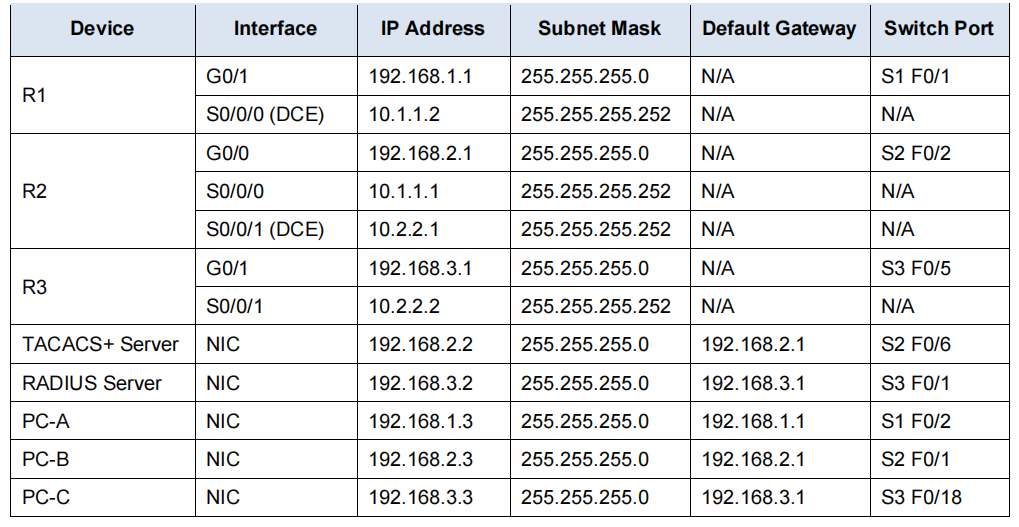
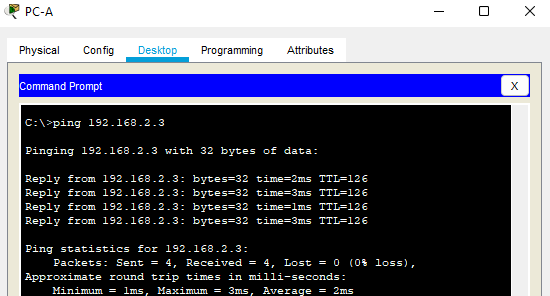


Table 1: Addressing Table

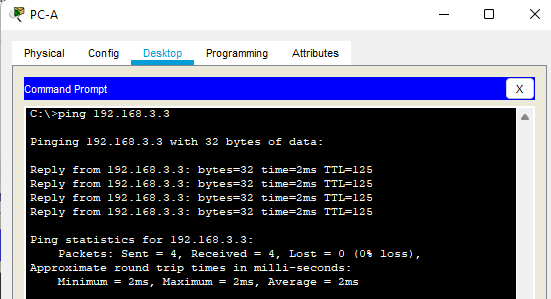
### Task 1: Configure Local AAA Authentication for Console Access on R1

1. Test connectivity.

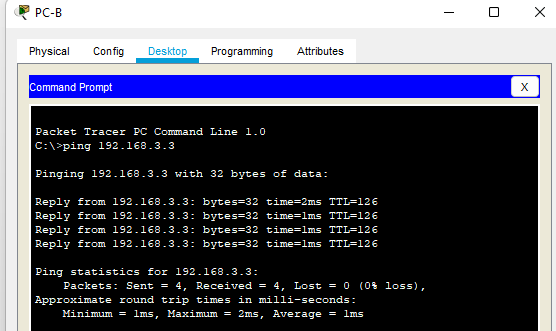
* Ping from PC-A to PC-B.



* Ping from PC-A to PC-C.



* Ping from PC-B to PC-C.



1. Configure a local username on R1.

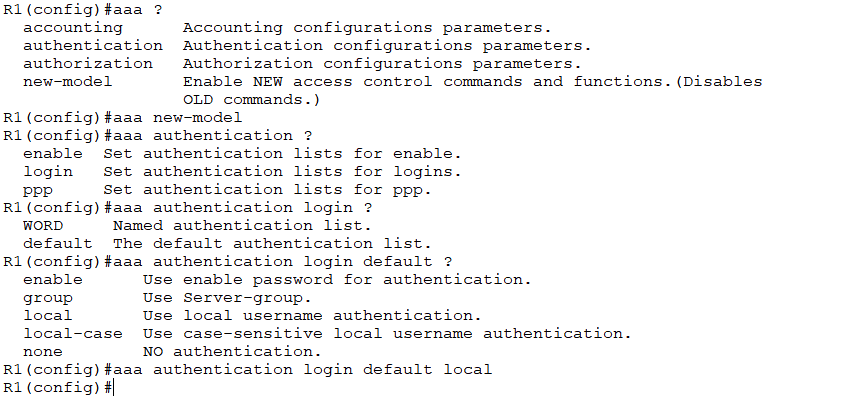
Configure a username of **Admin1** with a secret password of **admin1pa55**.

Attach screenshot of commands below.

|  |
| --- |
| PC-A (192.168.1.3), PC-B (192.168.2.3), PC-C (192.168.3.3) |

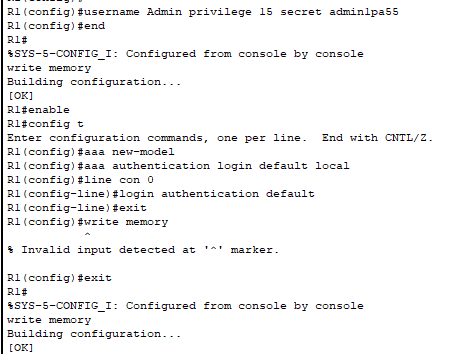
1. Configure local AAA authentication for console access on R1.

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



Note: You can enter a question mark after a command to see the available list of options for it as shown above.

Attach screenshot of commands below.



1. Configure the **line console** to use the defined AAA authentication method.

Configure AAA authentication for the console **login** to use the default method list.

Use the **line** command on a Cisco router to enter line configuration mode, you can configure settings for specific lines, such as the console, auxiliary, or virtual terminal (VTY) lines. Here, **line console 0** will configure settings for the console line.

Attach screenshot below.

1. Verify the AAA authentication method.

Verify the user EXEC login using the local database.

Attach screenshot below.

### Task 2: Configure Local AAA Authentication for vty Lines on R1

**Note:** You have already seen how to configure some of these settings in the previous lab. You may refer to that lab for the necessary commands.

1. Configure domain name and crypto key for use with SSH.
2. Use ccnasecurity.com as the domain name on R1.
3. Create an RSA crypto key using 1024 bits.

Attach screenshot of your commands below.

1. Configure a named list AAA authentication method for the **vty lines** on R1.

Configure a named list called SSH-LOGIN to authenticate logins using local AAA.

Attach screenshot of your commands below.

1. 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. Hint: use the **transport** command to define protocols for lines.

Attach screenshot of commands below.

1. Verify the AAA authentication method.

Verify the SSH configuration SSH to **R1** from the command prompt of **PC-A**.

Attach screenshot below.

### Task 3: Configure Server-Based AAA Authentication Using TACACS+ on R2

1. Configure a backup local database entry called Admin.

For backup purposes, configure a local username of **Admin2** and a secret password of **admin2pa55.**

1. Verify the TACACS+ Server configuration.

Click the TACACS+ Server. On the Services tab, click AAA. Notice that there is a Network configuration entry for R2 and a User Setup entry for Admin2.

1. Configure the TACACS+ server specifics on R2.

Configure the AAA TACACS server IP address and secret key on R2.

R2(config)# **tacacs-server host 192.168.2.2**

R2(config)# **tacacs-server key tacacspa55**

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

1. Configure AAA login authentication for console access on R2.
2. Enable AAA on R2
3. Configure all logins to authenticate using the AAA TACACS+ server. If it is not available, then use the local database.

R2(config) # aaa authentication login default group tacacs+ local

Attach screenshots of the commands below.

1. Configure the line console to use the defined AAA authentication method.

Configure AAA authentication for console login to use the default AAA authentication method.

1. Verify the AAA authentication method.

Verify the user EXEC login using the AAA TACACS+ server.

Attach screenshot below.

### Task 4: Configure Server-Based AAA Authentication Using RADIUS on R3

1. Configure a backup local database entry called Admin.

For backup purposes, configure a local username of **Admin3** and a secret password of **admin3pa55**.

1. Verify the RADIUS Server configuration.

Click the RADIUS Server. On the Services tab, click **AAA.** Notice that there is a Network configuration entry for **R3** and a User Setup entry for **Admin3**.

1. Configure the RADIUS server specifics on R3.

Configure the AAA RADIUS server IP address and secret key on R3.

R3(config)# **radius-server host 192.168.3.2**

R3(config)# **radius-server key radiuspa55**

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

1. Configure AAA login authentication for console access on R3.

Enable AAA on **R3** and configure all logins to authenticate using the AAA RADIUS server. If it is not available, then use the local database.

Attach screenshot of your commands below.

1. Configure the line console to use the defined AAA authentication method.

Configure AAA authentication for console log

1. Verify the AAA authentication method.

Verify the user EXEC login using the AAA RADIUS server.

Attach screenshot below

1. Check results.

Your completion percentage should be 100%. Click Check Results to see feedback and verification of which required components have been completed.

## Assessment Rubric

**Lab 04**

**Configure AAA Authentication on Cisco Routers**

|  |  |
| --- | --- |
| **Name:** | **Student ID:** |

**Points Distribution**

|  |  |  |
| --- | --- | --- |
| **Task No.** | **LR 2**  **Simulation** | **LR9**  **Report** |
| Task 1 | 30 |  |
| Task 2 | 10 |  |
| Task 3 | 20 |  |
| Task 4 | 20 |  |
| Total | /80 | /10 |
| **CLO Mapped** | CLO 1 | CLO1 |
|  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Affective Domain Rubric** | | **Points** | **CLO Mapped** |
| AR 7 | Report Submission | /10 | CLO 1 |

|  |  |  |
| --- | --- | --- |
| **CLO** | **Total Points** | **Points Obtained** |
| 1 | 90 |  |
| 1 | 10 |  |
| **Total** | **100** |  |

*For description of different levels of the mapped rubrics, please refer the provided Lab Evaluation Assessment Rubrics and Affective Domain Assessment Rubrics.*

**Lab Evaluation Assessment Rubric**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **#** | **Assessment Elements** | **Level 1: Unsatisfactory**  **Points 0-1** | **Level 2: Developing**  **Points 2** | **Level 3:Good**  **Points 3** | **Level 4:Exemplary**  **Points 4** |
| **LR2** | **Program/Code/ Simulation Model/ Network Model** | Program/code/simulation model/network model does not implement the required functionality and has several errors. The student is not able to utilize even the basic tools of the software. | Program/code/simulation model/network model has some errors and does not produce completely accurate results. Student has limited command on the basic tools of the software. | Program/code/simulation model/network model gives correct output but not efficiently implemented or implemented by computationally complex routine. | Program/code/simulation /network model is efficiently implemented and gives correct output. Student has full command on the basic tools of the software. |
| **LR9** | **Report** | All the in-lab tasks are not included in report and / or the report is submitted too late. | Most of the tasks are included in report but are not well explained. All the necessary figures / plots are not included. Report is submitted after due date. | Good summary of most the in-lab tasks is included in report. The work is supported by figures and plots with explanations. The report is submitted timely. | Detailed summary of the in-lab tasks is provided. All tasks are included and explained well. Data is presented clearly including all the necessary figures, plots and tables. |