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

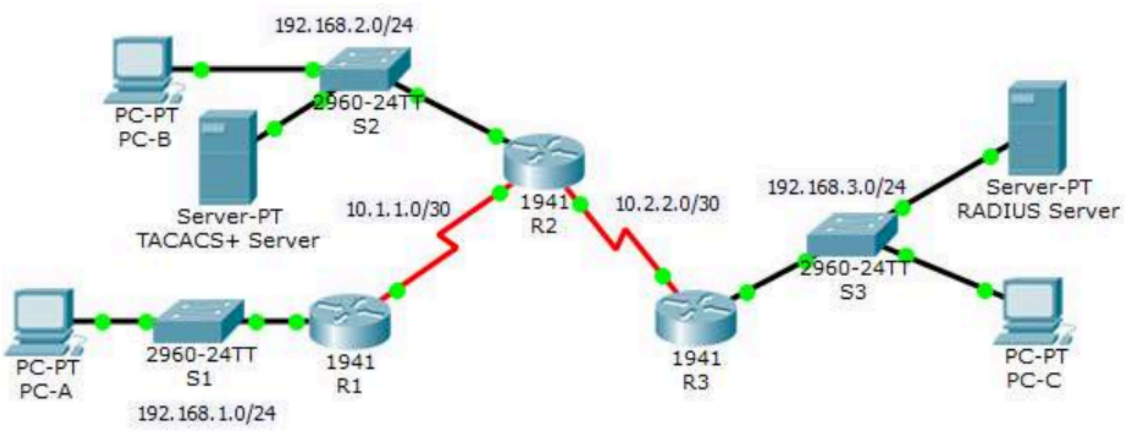


Figure 1: Topology

Addressing Table

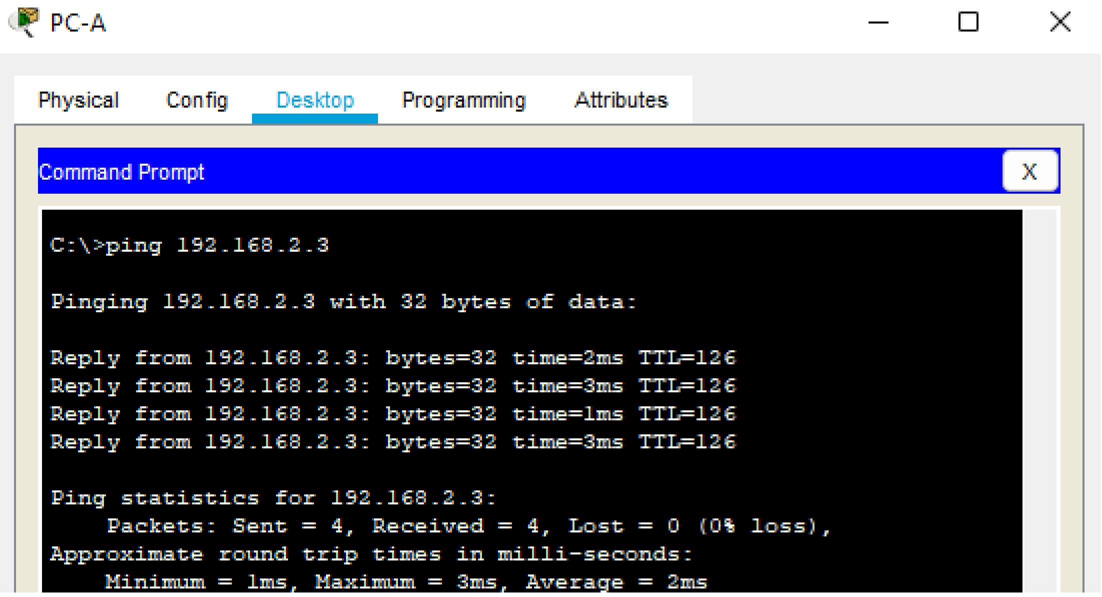
Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/1	192.168.1.1	255.255.255.0	N/A	S1 F0/1
	S0/0/0 (DCE)	10.1.1.2	255.255.255.252	N/A	N/A
R2	G0/0	192.168.2.1	255.255.255.0	N/A	S2 F0/2
	S0/0/0	10.1.1.1	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.1	255.255.255.252	N/A	N/A
R3	G0/1	192.168.3.1	255.255.255.0	N/A	S3 F0/5
	S0/0/1	10.2.2.2	255.255.255.252	N/A	N/A
TACACS+ Server	NIC	192.168.2.2	255.255.255.0	192.168.2.1	S2 F0/6
RADIUS Server	NIC	192.168.3.2	255.255.255.0	192.168.3.1	S3 F0/1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/2
PC-B	NIC	192.168.2.3	255.255.255.0	192.168.2.1	S2 F0/1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

Table 1: Addressing Table

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

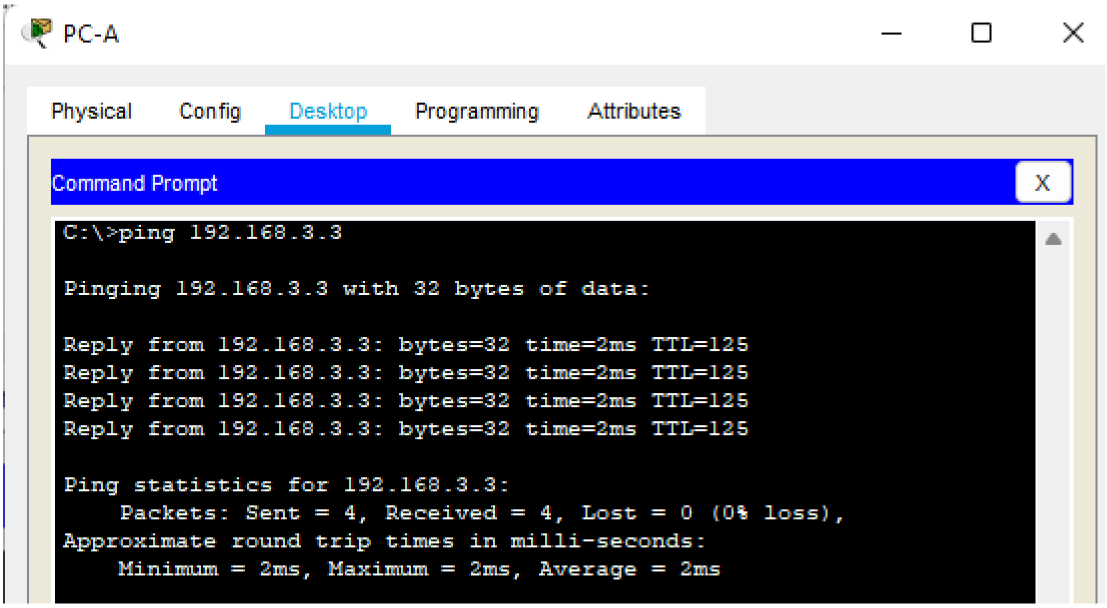
1. Test connectivity.

- Ping from PC-A to PC-B.



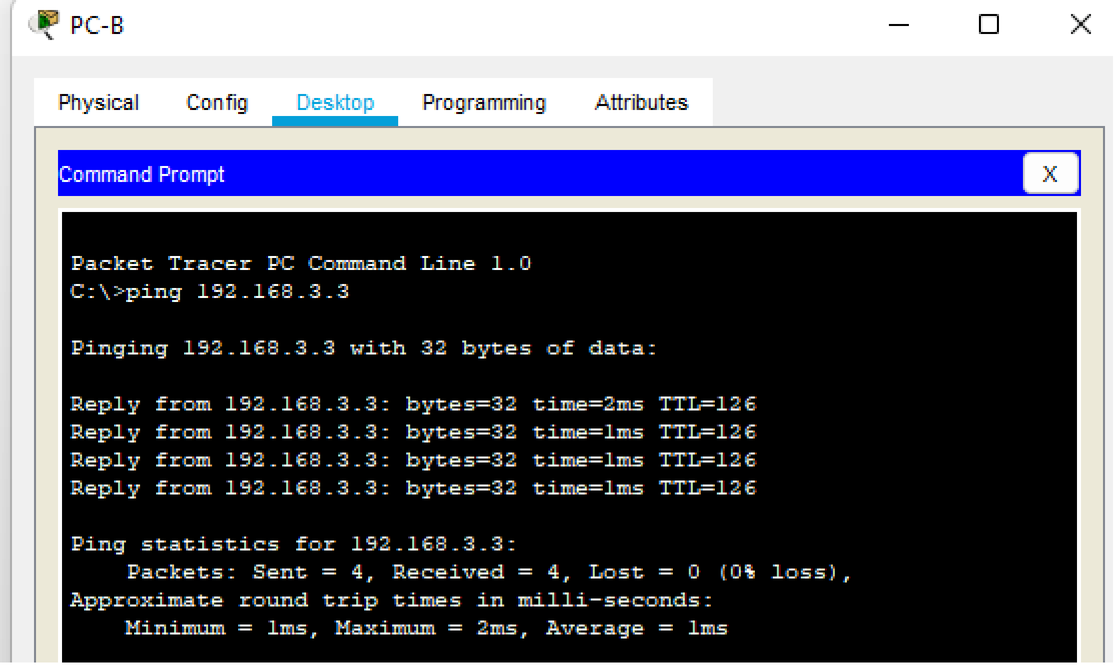
```
C:\>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.2.3: bytes=32 time=2ms TTL=126
Reply from 192.168.2.3: bytes=32 time=3ms TTL=126
Reply from 192.168.2.3: bytes=32 time=1ms TTL=126
Reply from 192.168.2.3: bytes=32 time=3ms TTL=126

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 3ms, Average = 2ms
```

- Ping from PC-A to PC-C.



```
C:\>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Reply from 192.168.3.3: bytes=32 time=2ms TTL=125
Reply from 192.168.3.3: bytes=32 time=2ms TTL=125
Reply from 192.168.3.3: bytes=32 time=2ms TTL=125
Reply from 192.168.3.3: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 2ms, Average = 2ms
```

- Ping from PC-B to PC-C.



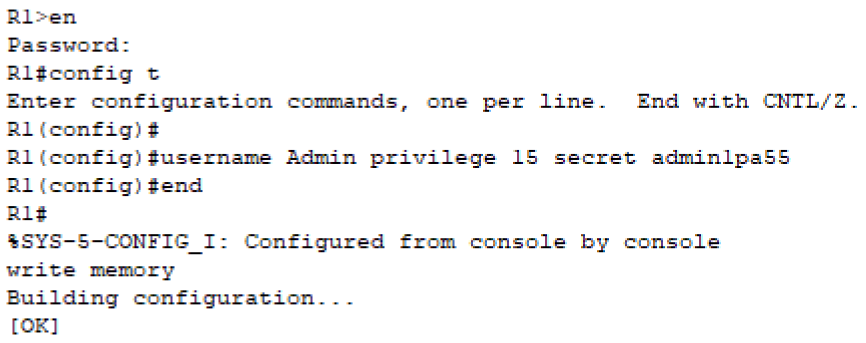
```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.3.3

Pinging 192.168.3.3 with 32 bytes of data:

Reply from 192.168.3.3: bytes=32 time=2ms TTL=126
Reply from 192.168.3.3: bytes=32 time=1ms TTL=126
Reply from 192.168.3.3: bytes=32 time=1ms TTL=126
Reply from 192.168.3.3: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

2. Configure a local username on R1.

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

   Attach screenshot of commands below.

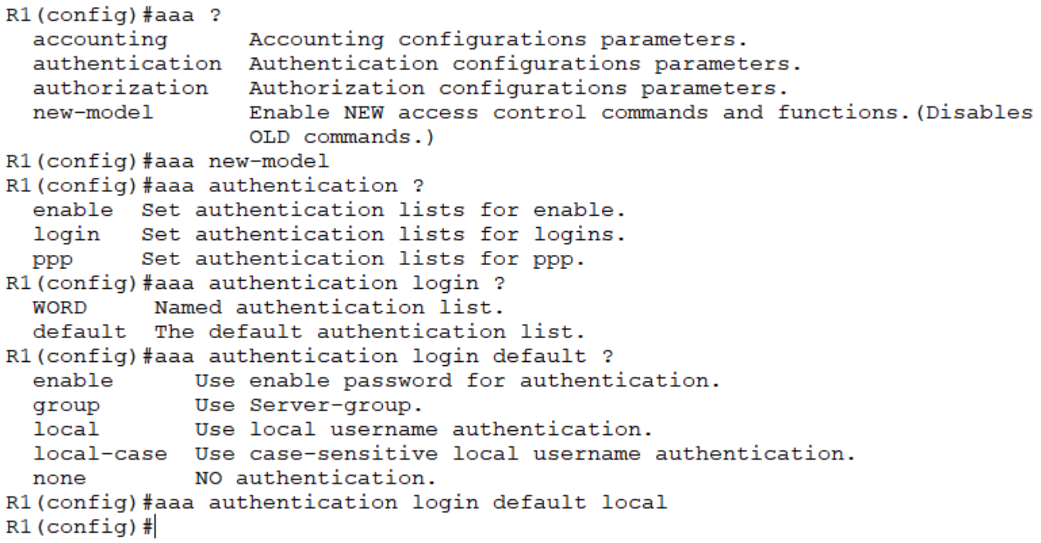
PC-A (192.168.1.3), PC-B (192.168.2.3), PC-C (192.168.3.3)



```
R1>en
Password:
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#
R1(config)#username Admin privilege 15 secret admin1pa55
R1(config)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
write memory
Building configuration...
[OK]
```

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

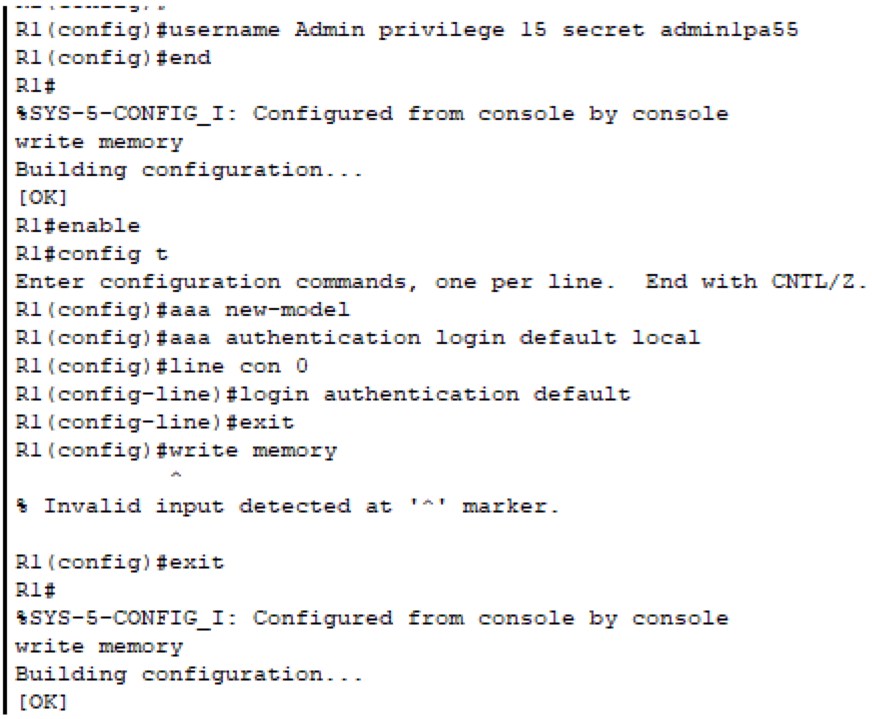
   Enable AAA on R1 and configure AAA authentication for the console login to use the local database



```
R1(config)#aaa ?
  accounting      Accounting configurations parameters.
  authentication  Authentication configurations parameters.
  authorization   Authorization configurations parameters.
  new-model       Enable NEW access control commands and functions.(Disables
                  OLD commands.)
R1(config)#aaa new-model
R1(config)#aaa authentication ?
  enable  Set authentication lists for enable.
  login   Set authentication lists for logins.
  ppp     Set authentication lists for ppp.
R1(config)#aaa authentication login ?
  WORD     Named authentication list.
  default  The default authentication list.
R1(config)#aaa authentication login default ?
  enable      Use enable password for authentication.
  group       Use Server-group.
  local       Use local username authentication.
  local-case  Use case-sensitive local username authentication.
  none        NO authentication.
R1(config)#aaa authentication login default local
R1(config)#
```

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.



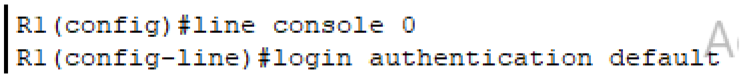
```
R1(config)#username Admin privilege 15 secret admin1pa55
R1(config)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
write memory
Building configuration...
[OK]
R1#enable
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#aaa new-model
R1(config)#aaa authentication login default local
R1(config)#line con 0
R1(config-line)#login authentication default
R1(config-line)#exit
R1(config)#write memory
              ^
% Invalid input detected at '^' marker.

R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
write memory
Building configuration...
[OK]
```

4. 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.

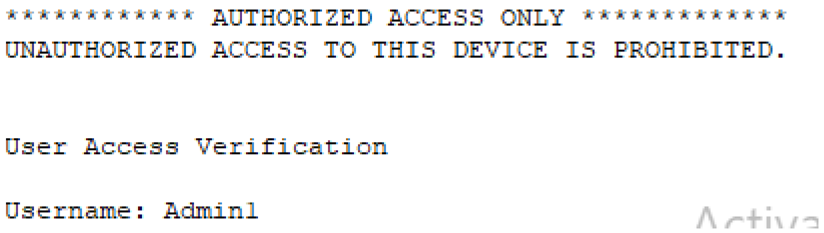


```
R1(config)#line console 0
R1(config-line)#login authentication default
```

5. Verify the AAA authentication method.

   Verify the user EXEC login using the local database.

   Attach screenshot below.



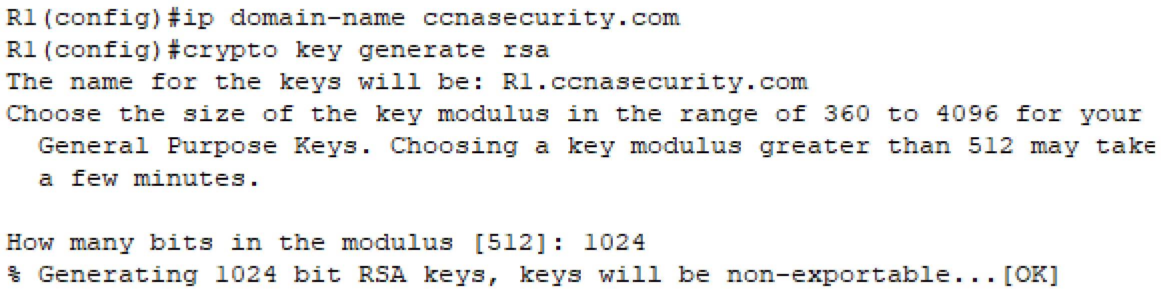
```
************ AUTHORIZED ACCESS ONLY *************
UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.


User Access Verification

Username: Admin1
```

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.
   a. Use ccnasecurity.com as the domain name on R1.
   b. Create an RSA crypto key using 1024 bits.

   Attach screenshot of your commands below.

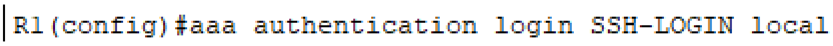


```
R1(config)#ip domain-name ccnasecurity.com
R1(config)#crypto key generate rsa
The name for the keys will be: R1.ccnasecurity.com
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

2. 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.

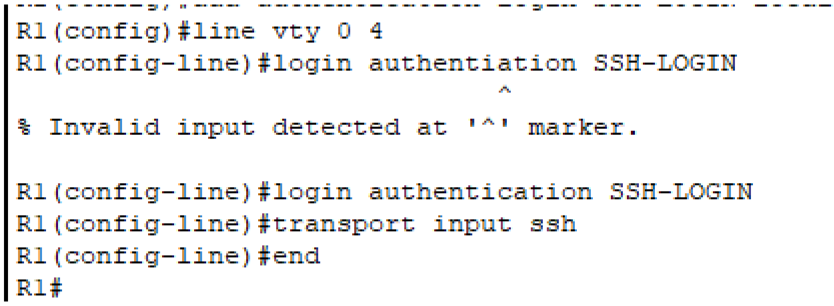


```
R1(config)#aaa authentication login SSH-LOGIN local
```

3. 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.

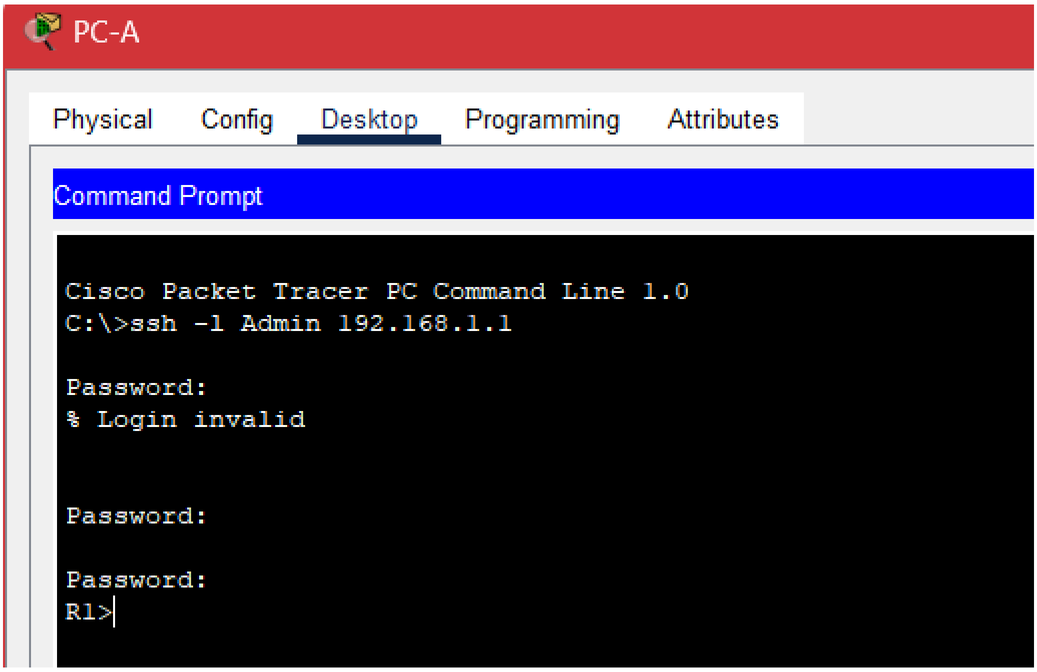


```
R1(config)#line vty 0 4
R1(config-line)#login authentiation SSH-LOGIN
                               ^
% Invalid input detected at '^' marker.

R1(config-line)#login authentication SSH-LOGIN
R1(config-line)#transport input ssh
R1(config-line)#end
R1#
```

4. Verify the AAA authentication method.

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

   Attach screenshot below.

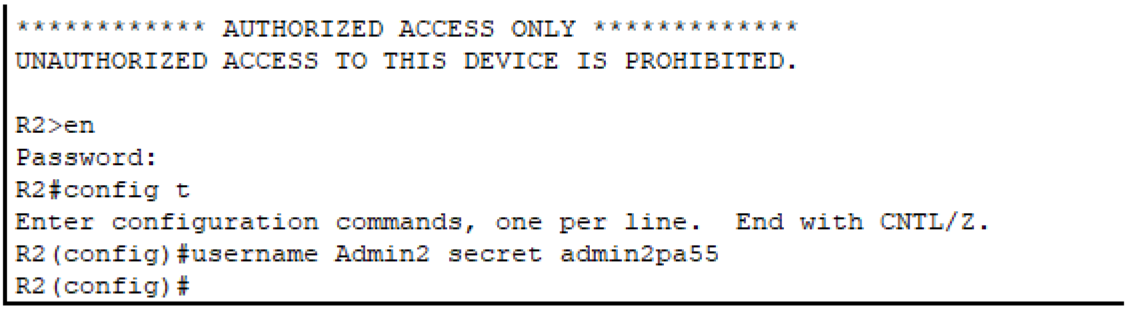


```
Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l Admin 192.168.1.1

Password:
% Login invalid


Password:

Password:
R1>
```

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

1. Configure a backup local database entry called Admin.

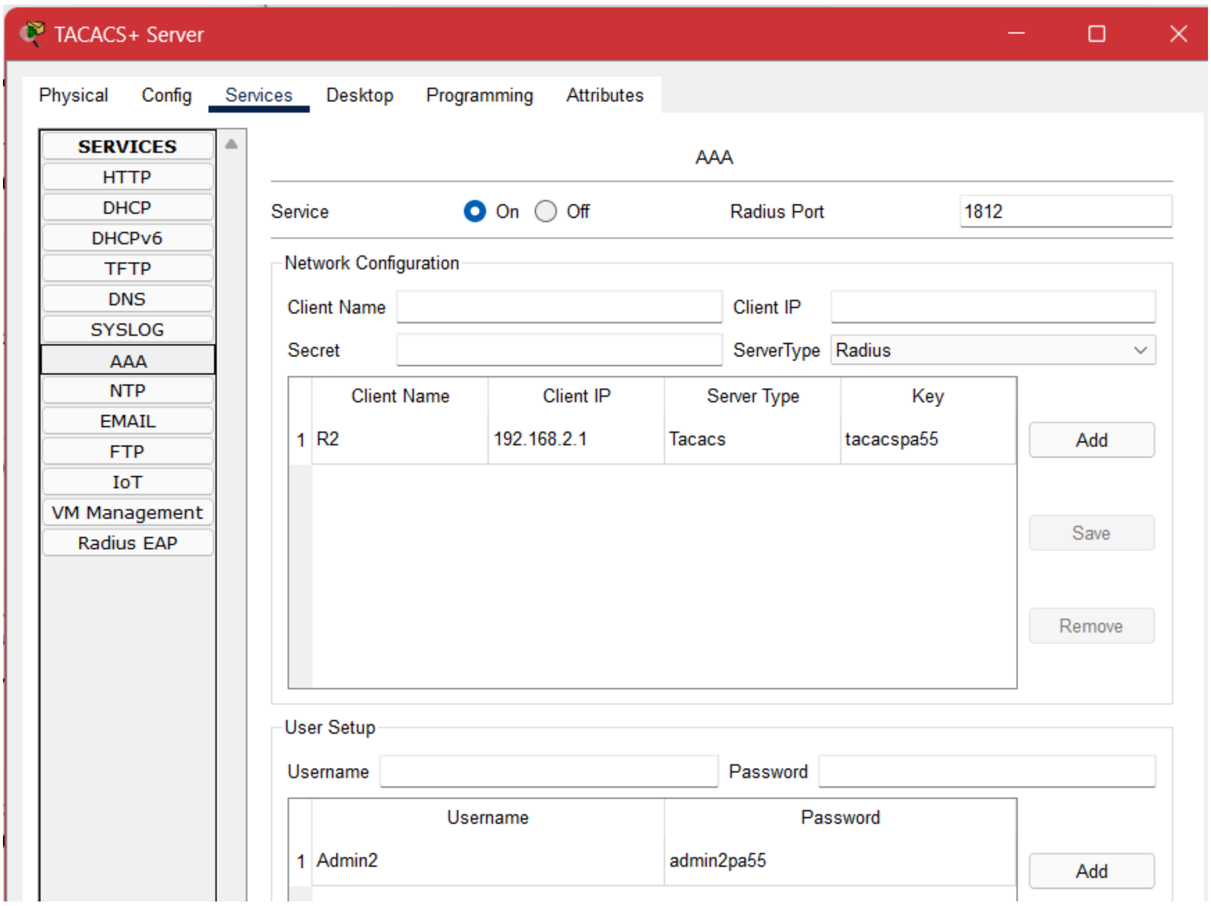
   For backup purposes, configure a local username of **Admin2** and a secret password of **admin2pa55.**



```
************ AUTHORIZED ACCESS ONLY *************
UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.

R2>en
Password:
R2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#username Admin2 secret admin2pa55
R2(config)#
```

2. 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.



AAA

Service ● On ○ Off Radius Port 1812

Network Configuration

Client Name Client IP

Secret ServerType Radius

	Client Name	Client IP	Server Type	Key
1	R2	192.168.2.1	Tacacs	tacacspa55

User Setup

Username Password

	Username	Password
1	Admin2	admin2pa55

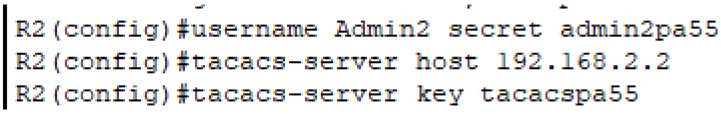
3. Configure the TACACS+ server specifics on R2.

   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**.

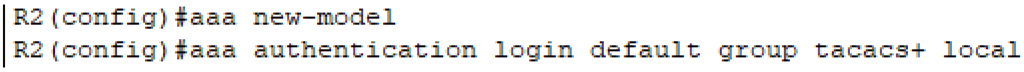


```
R2(config)#username Admin2 secret admin2pa55
R2(config)#tacacs-server host 192.168.2.2
R2(config)#tacacs-server key tacacspa55
```

4. Configure AAA login authentication for console access on R2.
   a. Enable AAA on R2
   b. 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

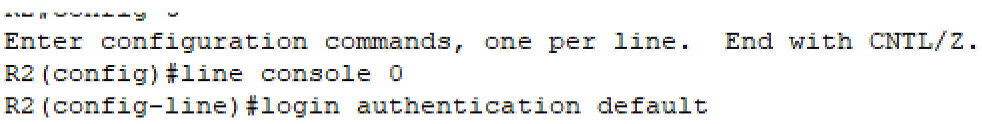
   Attach screenshots of the commands below.



```
R2(config)#aaa new-model
R2(config)#aaa authentication login default group tacacs+ local
```

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

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

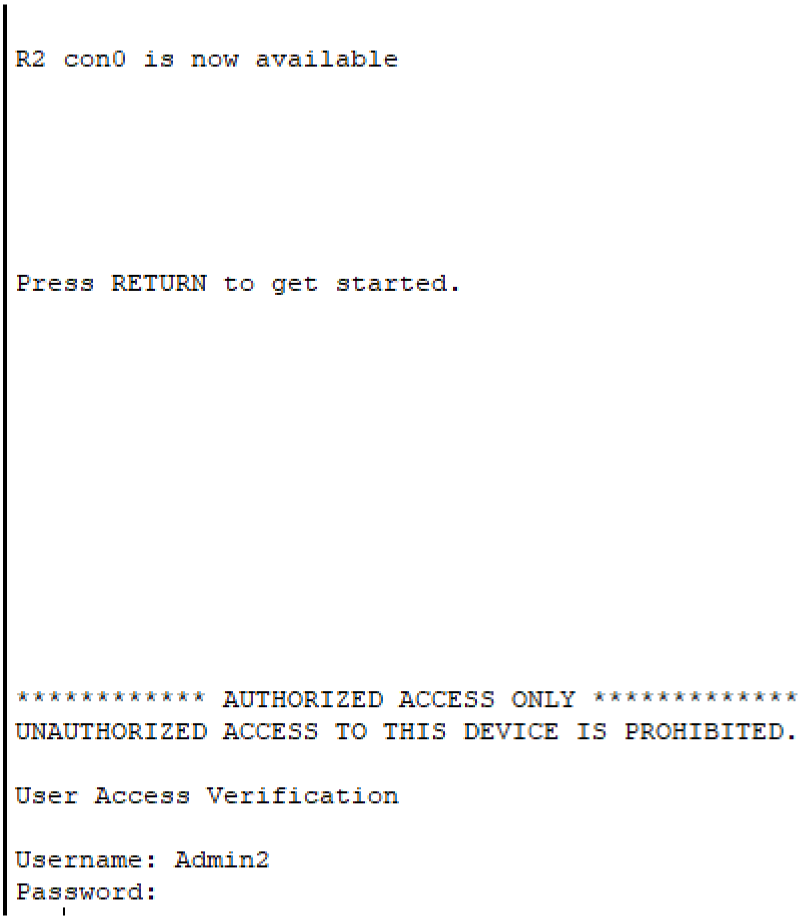


```
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#line console 0
R2(config-line)#login authentication default
```

6. Verify the AAA authentication method.

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

   Attach screenshot below.

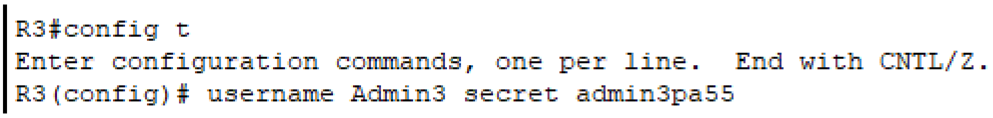


```
R2 con0 is now available




Press RETURN to get started.









************ AUTHORIZED ACCESS ONLY *************
UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.

User Access Verification

Username: Admin2
Password:
```

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

1. Configure a backup local database entry called Admin.

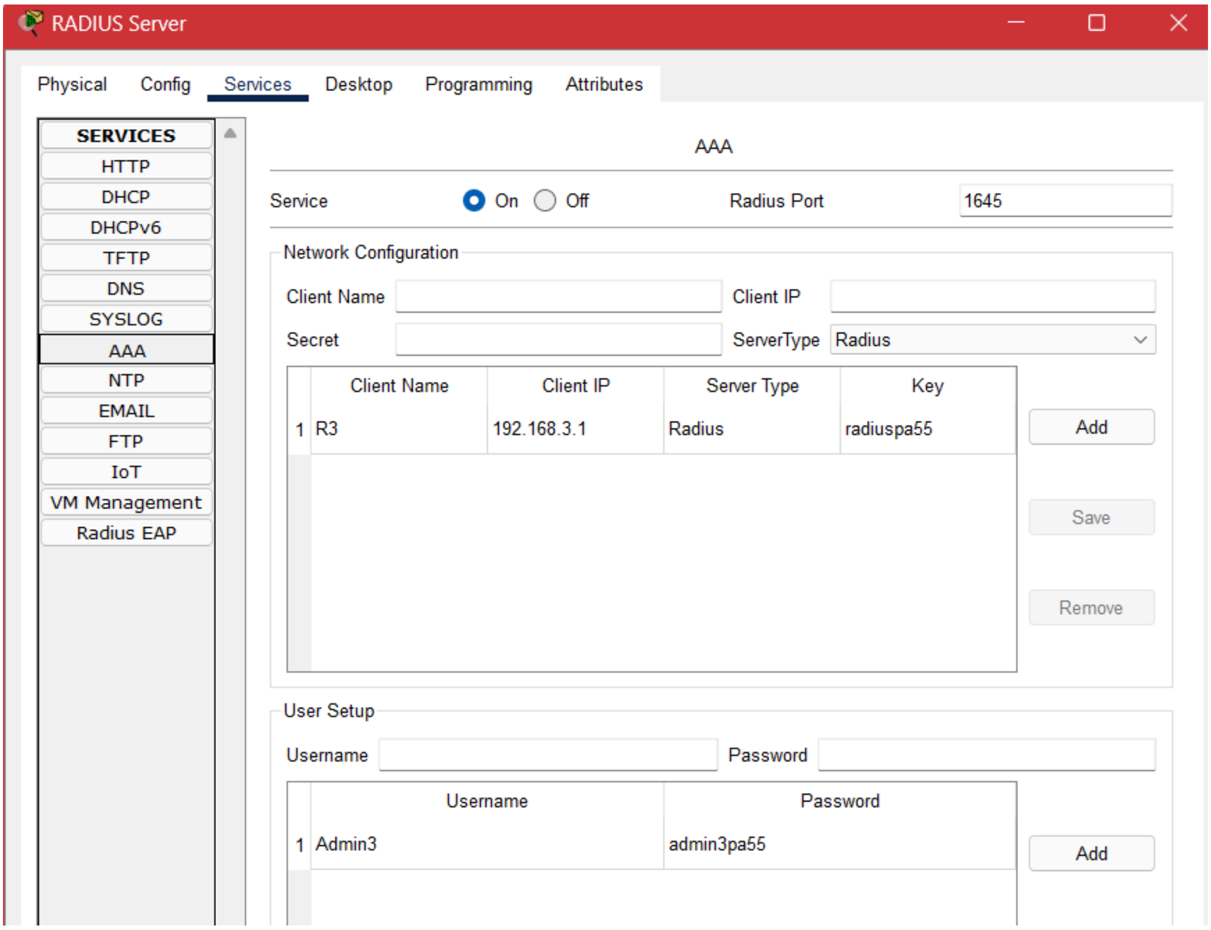
   For backup purposes, configure a local username of **Admin3** and a secret password of **admin3pa55**.



```
R3#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)# username Admin3 secret admin3pa55
```

2. 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**.



AAA

Service ● On ○ Off Radius Port 1645

Network Configuration

Client Name Client IP

Secret ServerType Radius

	Client Name	Client IP	Server Type	Key
1	R3	192.168.3.1	Radius	radiuspa55

User Setup

Username Password

	Username	Password
1	Admin3	admin3pa55

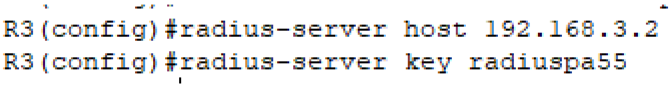
3. Configure the RADIUS server specifics on R3.

   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.

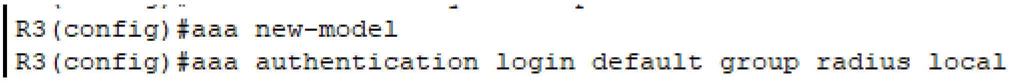


```
R3(config)#radius-server host 192.168.3.2
R3(config)#radius-server key radiuspa55
```

4. 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.

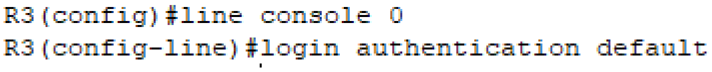
   Attach screenshot of your commands below.



```
R3(config)#aaa new-model
R3(config)#aaa authentication login default group radius local
```

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

   Configure AAA authentication for console log

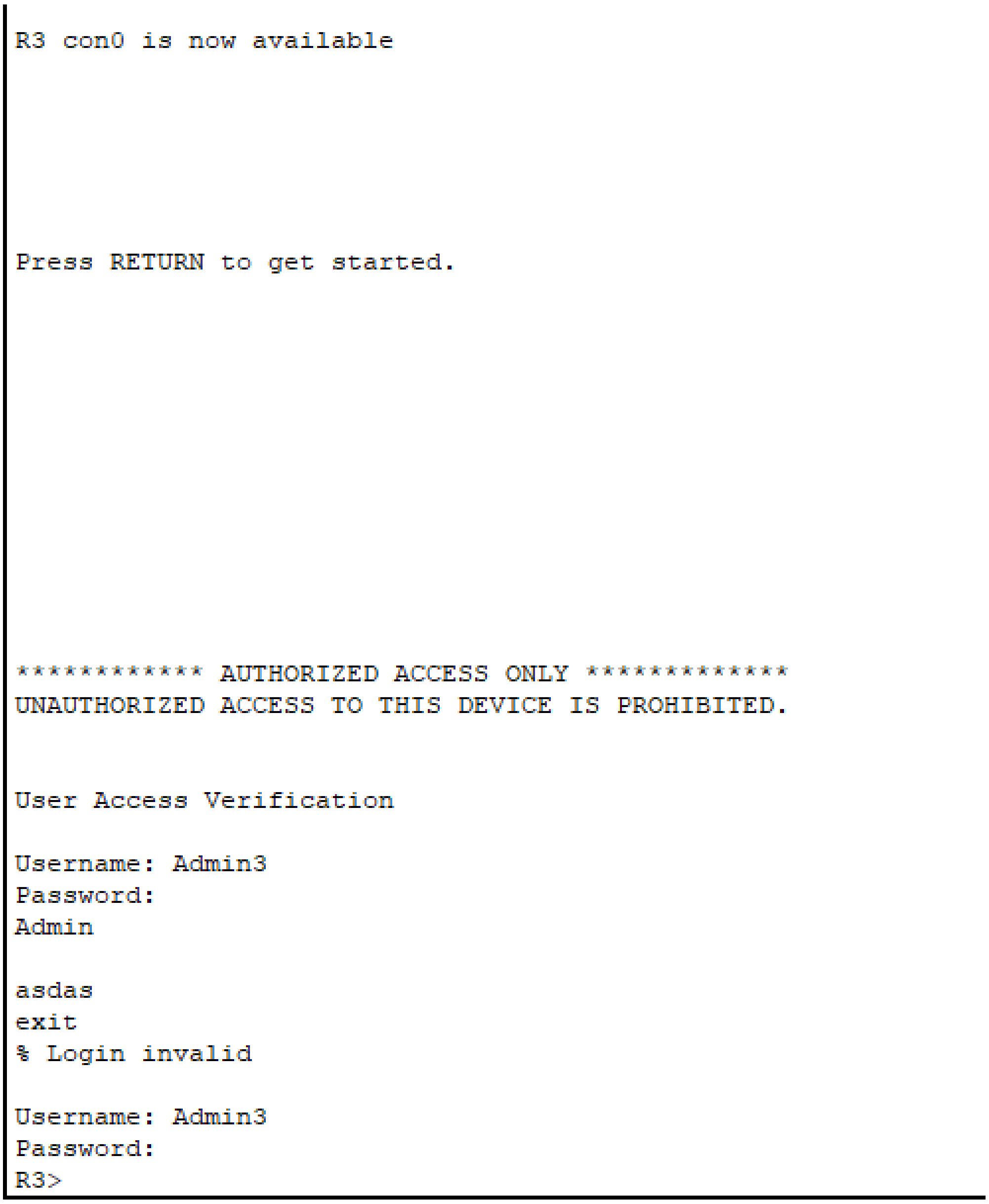


```
R3(config)#line console 0
R3(config-line)#login authentication default
```

6. Verify the AAA authentication method.

   Verify the user EXEC login using the AAA RADIUS server.

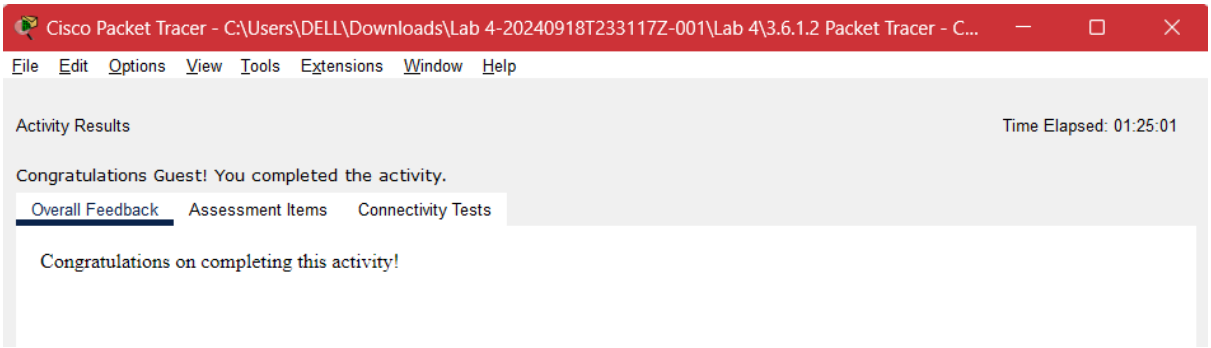
   Attach screenshot below



```
R3 con0 is now available





Press RETURN to get started.












************ AUTHORIZED ACCESS ONLY *************
UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.


User Access Verification

Username: Admin3
Password:
Admin

asdas
exit
% Login invalid

Username: Admin3
Password:
R3>
```

7. Check results.

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

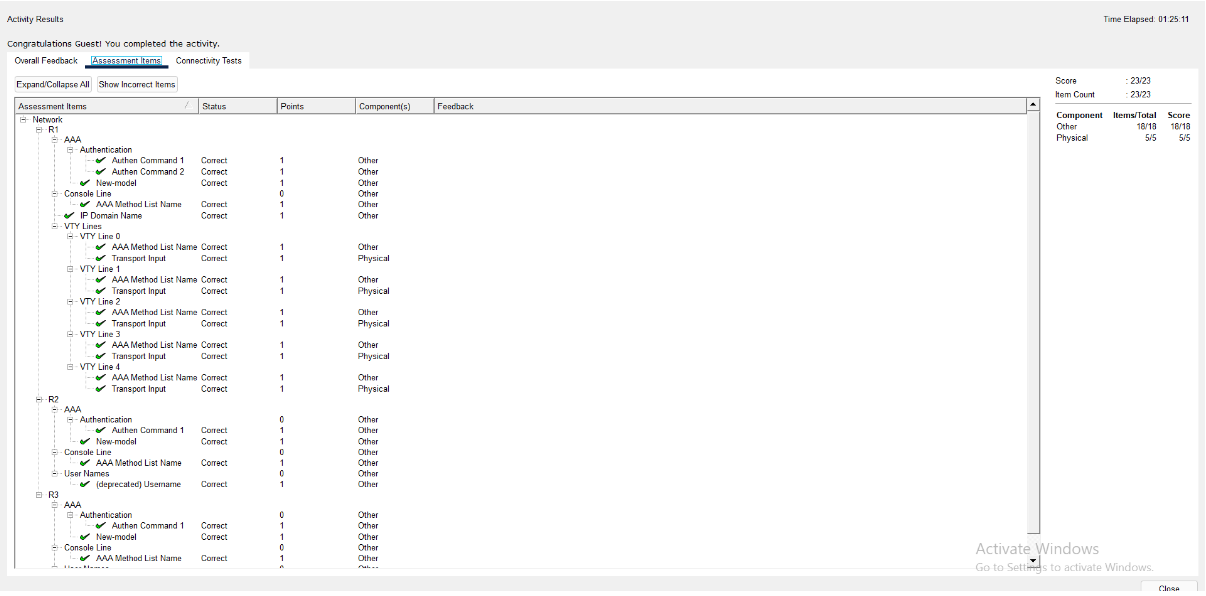

Cisco Packet Tracer - C:\Users\DELL\Downloads\Lab 4-20240918T233117Z-001\Lab 4\3.6.1.2 Packet Tracer - C...
File Edit Options View Tools Extensions Window Help
Overall Feedback
Assessment Items
Connectivity Tests

Activity Results

Time Elapsed: 01:25:01

Congratulations Guest! You completed the activity.

Congratulations on completing this activity!



Activity Results

Time Elapsed: 01:25:11

Congratulations Guest! You completed the activity.

Assessment Items	Status	Points	Component(s)	Feedback
Network				
R1				
AAA				
Authentication				
✓ Authen Command 1	Correct	1	Other	
✓ Authen Command 2	Correct	1	Other	
✓ New-model	Correct	1	Other	
Console Line		0	Other	
✓ AAA Method List Name	Correct	1	Other	
✓ IP Domain Name	Correct	1	Other	
VTY Lines				
VTY Line 0				
✓ AAA Method List Name	Correct	1	Other	
✓ Transport Input	Correct	1	Physical	
VTY Line 1				
✓ AAA Method List Name	Correct	1	Other	
✓ Transport Input	Correct	1	Physical	
VTY Line 2				
✓ AAA Method List Name	Correct	1	Other	
✓ Transport Input	Correct	1	Physical	
VTY Line 3				
✓ AAA Method List Name	Correct	1	Other	
✓ Transport Input	Correct	1	Physical	
VTY Line 4				
✓ AAA Method List Name	Correct	1	Other	
✓ Transport Input	Correct	1	Physical	
R2				
AAA				
Authentication		0	Other	
✓ Authen Command 1	Correct	1	Other	
✓ New-model	Correct	1	Other	
Console Line		0	Other	
✓ AAA Method List Name	Correct	1	Other	
User Names		0	Other	
✓ (deprecated) Username	Correct	1	Other	
R3				
AAA				
Authentication		0	Other	
✓ Authen Command 1	Correct	1	Other	
✓ New-model	Correct	1	Other	
Console Line		0	Other	
✓ AAA Method List Name	Correct	1	Other	

Score : 23/23

Item Count : 23/23

Component	Items/Total	Score
Other	18/18	18/18
Physical	5/5	5/5

User Names		0	Other
✓ (deprecated) Username	Correct	1	Other

Assessment Rubric

Lab 04

Configure AAA Authentication on Cisco Routers

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

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.