VSIT

Security in Computing
Practical #2

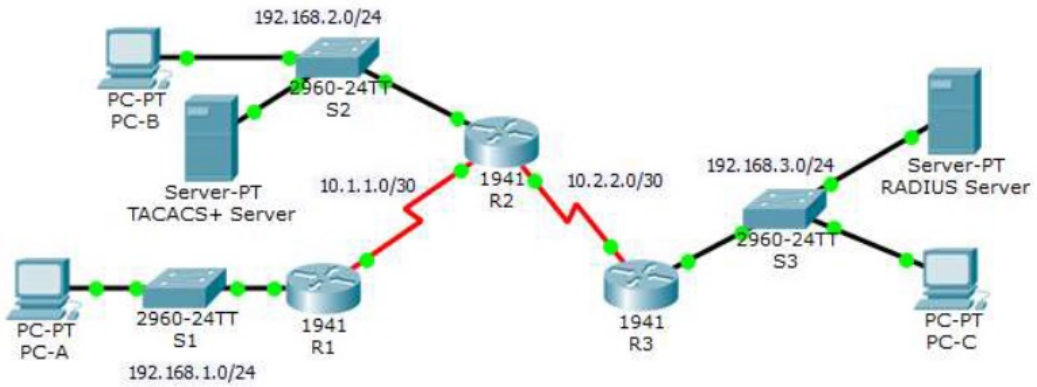
Name	Sanjeev Gupta	**Roll Number**	21302B0023
Class	TYBSc.IT	**Division**	C
Subject/Course	Security in Computing		
Topic	Configuring AAA on Cisco Routers		

Configure AAA Authentication

a. Configure a local user account on Router and configure authenticate on the console and vty lines using local AAA

b. Verify local AAA authentication from the Router console and the PC-A client

Topology



Addressing Table

Device	Interface	IP Address
R1	G0/1	192.168.1.1
	S0/0/0 (DCE)	10.1.1.2
R2	G0/0	192.168.2.1
	S0/0/0	10.1.1.1
	S0/0/1 (DCE)	10.2.2.1
R3	G0/1	192.168.3.1
	S0/0/1	10.2.2.2
TACACS+ Server	NIC	192.168.2.2
RADIUS Server	NIC	192.168.3.2
PC-A	NIC	192.168.1.3
PC-B	NIC	192.168.2.3
PC-C	NIC	192.168.3.3

Background / Scenario

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

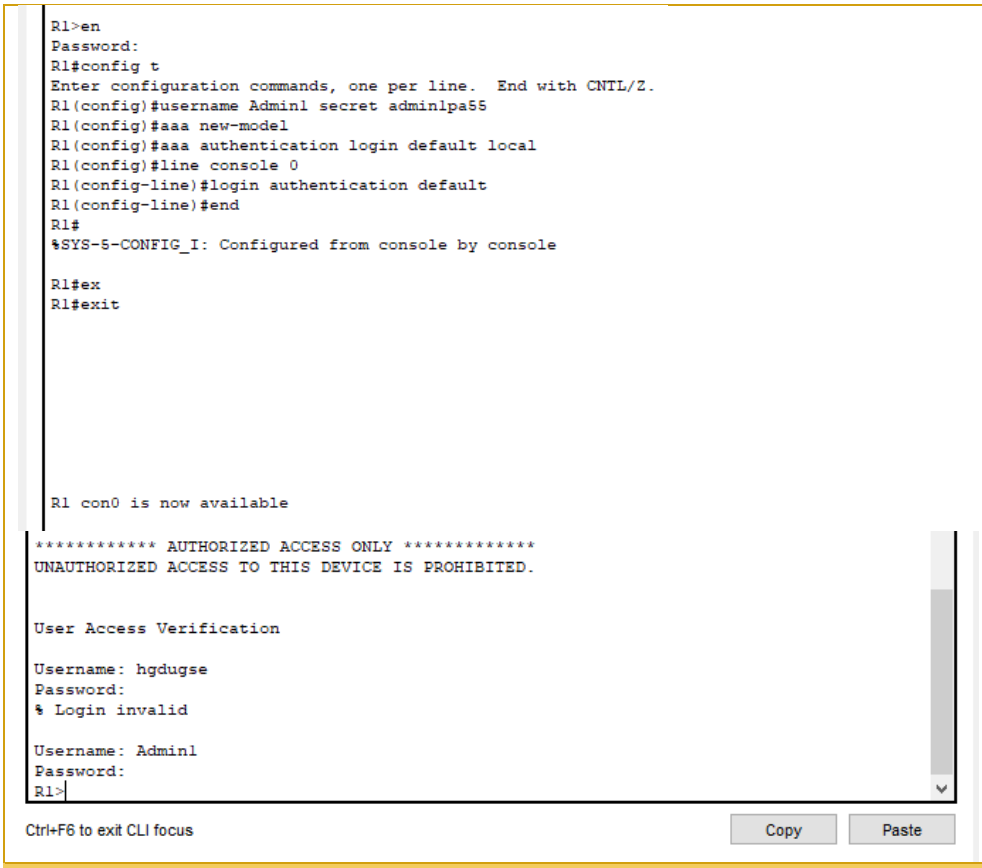
1. Create a local user account and configure local AAA on router R1 to test the console and vty logins.
- User account: Admin1 and password admin1pa55
2. Configure router R2 to support server-based authentication using the TACACS+ protocol
- Client: R2 using the keyword tacacspa55
- User account: Admin2 and password admin2pa55
3. Configure router R3 to support server-based authentication using the RADIUS protocol
- Client: R3 using the keyword radiuspa55
- User account: Admin3 and password admin3pa55
4. Configure the routers with the following:
- Enable secret password: ciscoenpa55
- OSPF routing protocol with MD5 authentication using password: MD5pa55

Configure AAA Authentication – on the console

Part 1: Configure Local AAA Authentication for Console Access on R1
Step 1: Test connectivity.
- Ping from PC-A to PC-B.
- Ping from PC-A to PC-C.
- Ping from PC-B to PC-C.

Step 2: Configure a local username on R1.
Configure a username of Admin1 with a secret password of admin1pa55.
R1(config)# username Admin1 secret admin1pa55
Step 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 new-model
R1(config)# aaa authentication login default local
Step 4: 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 5: Verify the AAA authentication method.
Verify the user EXEC login using the local database.
R1(config-line)# end
%SYS-5-CONFIG_I: Configured from console by console
R1# exit
R1 con0 is now available
Press RETURN to get started.
********** AUTHORIZED ACCESS ONLY **********
UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.
User Access Verification
Username: Admin1
Password: admin1pa55
R1>

Insert screenshots here

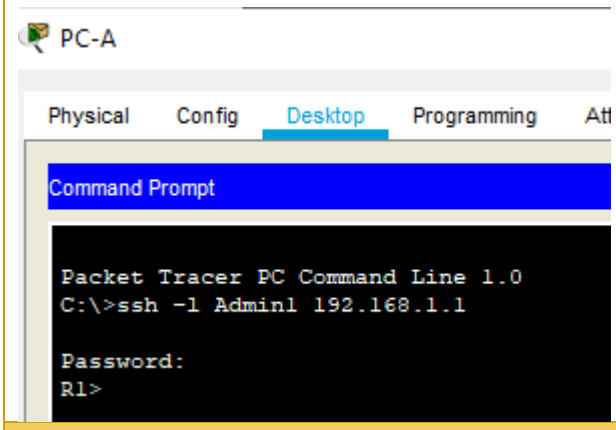


Configure AAA Authentication – for vty lines on R1

Part 2: Configure Local AAA Authentication for vty Lines on R1
Step 1: Configure domain name and crypto key for use with SSH.
a. Use ccnasecurity.com as the domain name on R1.
R1(config)# ip domain-name ccnasecurity.com
b. Create an RSA crypto key using 1024 bits.
R1(config)# crypto key generate rsa
Choose the size of the key modulus in the range of 360 to 2048 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]
Step 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.
R1(config)# aaa authentication login SSH-LOGIN local
Step 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.
R1(config)# line vty 0 4
R1(config-line)# login authentication SSH-LOGIN
R1(config-line)# transport input ssh
R1(config-line)# end
Step 4: Verify the AAA authentication method.
Verify the SSH configuration SSH to R1 from the command prompt of PC-A..
PC> ssh –l Admin1 192.168.1.1
Open
Password: admin1pa55

Insert screenshots here

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


User Access Verification

Username: exit
Password:
% Login invalid

Username: Admin1
Password:
R1>en
Password:
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
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 2048 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]

R1(config)# aaa authentication login SSH-LOGIN local
*Mar 1 0:15:45.579: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)#line vty 0 4
R1(config-line)#login authentication SSH-LOGIN
R1(config-line)#transport input ssh
R1(config-line)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
```



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

Step 1: Configure a backup local database entry called Admin.

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

R2(config)# username Admin2 secret admin2pa55

Step 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.

Step 3: Configure the TACACS+ server specifics on R2.

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

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)# tacacs-server host 192.168.2.2

R2(config)# tacacs-server key tacacspa55

Step 4: Configure AAA login authentication for console access on R2.

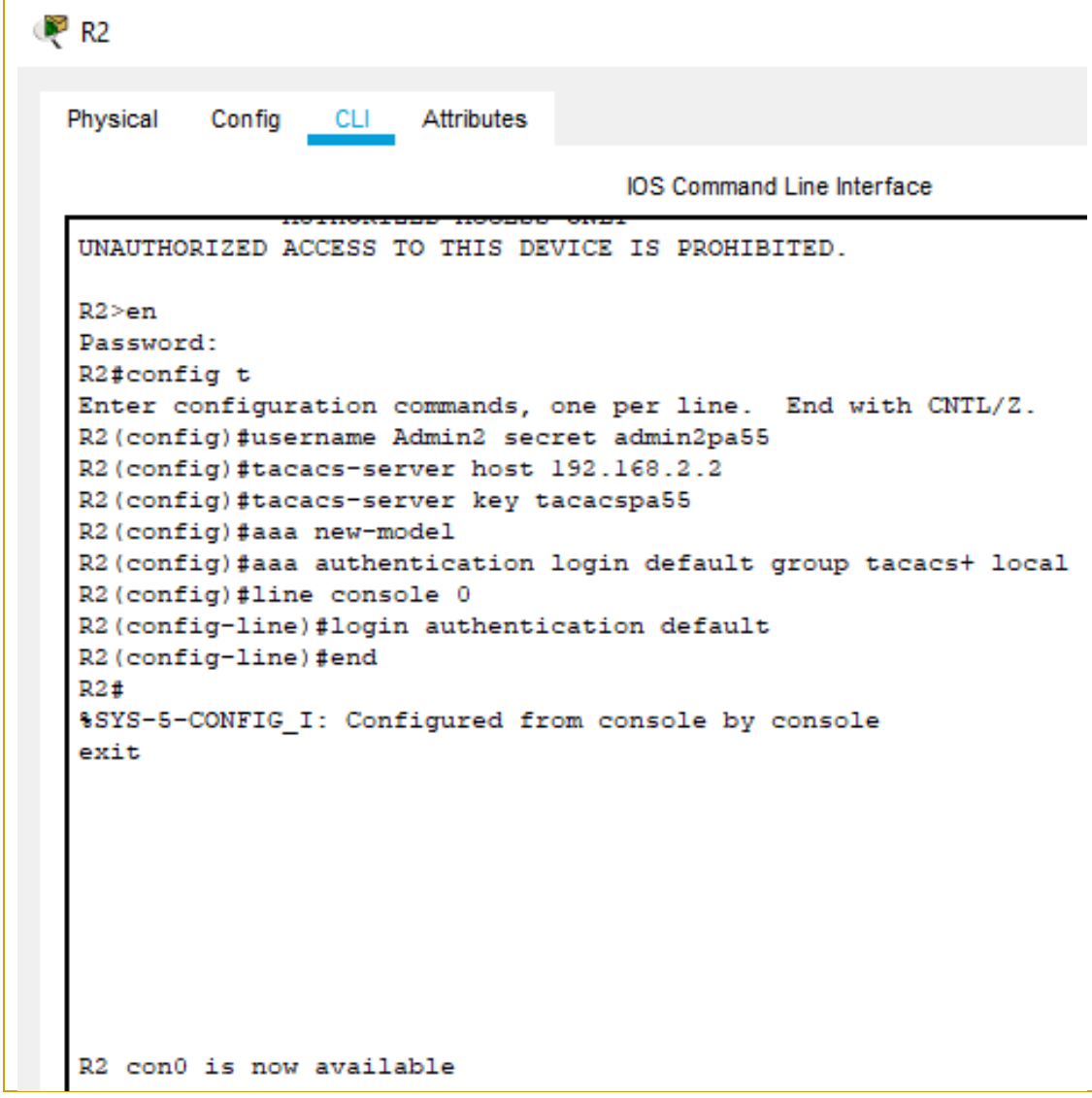
Enable AAA on R2 and configure all logins to authenticate using the AAA TACACS+ server. If it is not available, then use the local database.

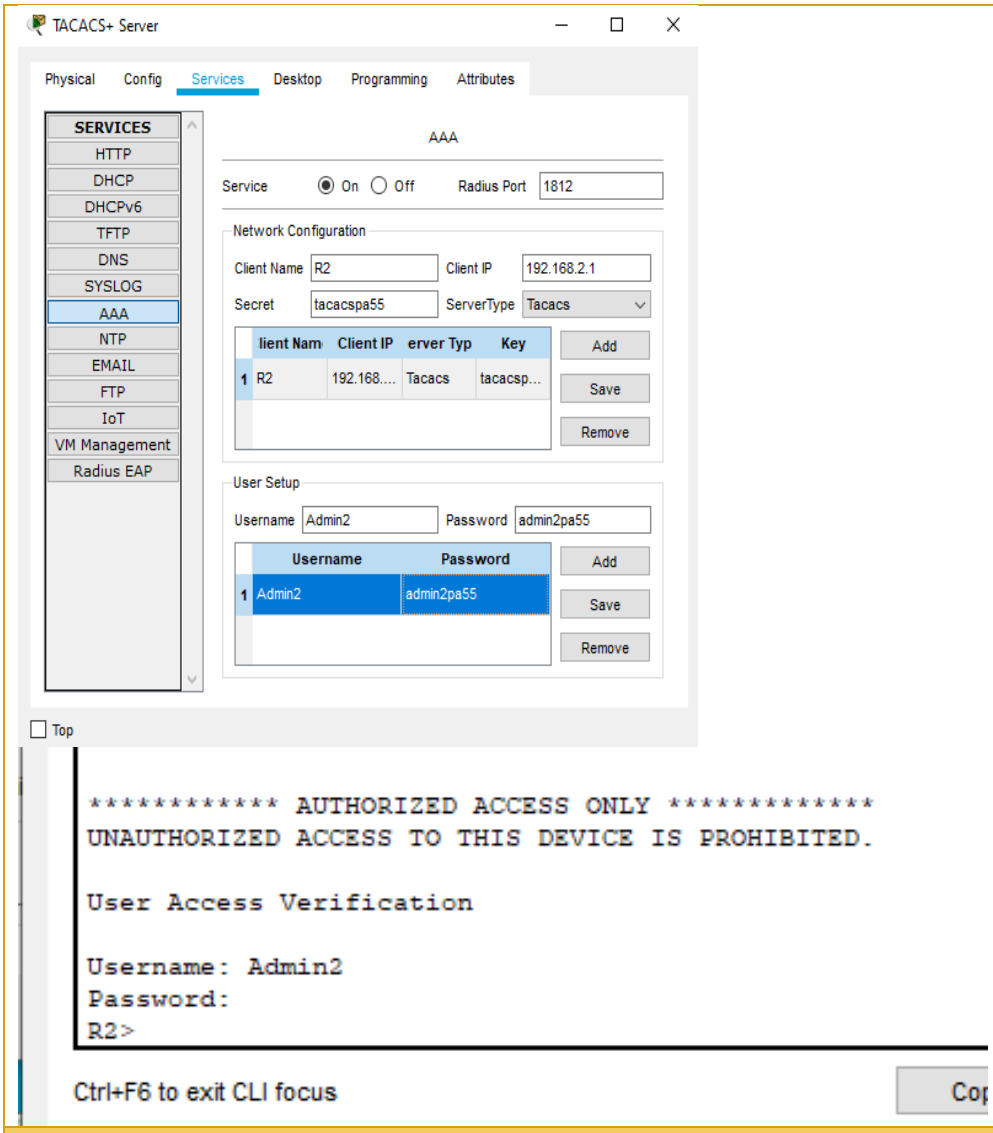
R2(config)# aaa new-model

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

Step 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.
R2(config)# line console 0
R2(config-line)# login authentication default
Step 6: Verify the AAA authentication method.
Verify the user EXEC login using the AAA TACACS+ server.
R2(config-line)# end
%SYS-5-CONFIG_I: Configured from console by console
R2# exit
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: admin2pa55
R2>

Insert screenshots here





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

Step 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)# username Admin3 secret admin3pa55

Step 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.

Step 3: Configure the RADIUS server specifics on R3.

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

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

Step 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.

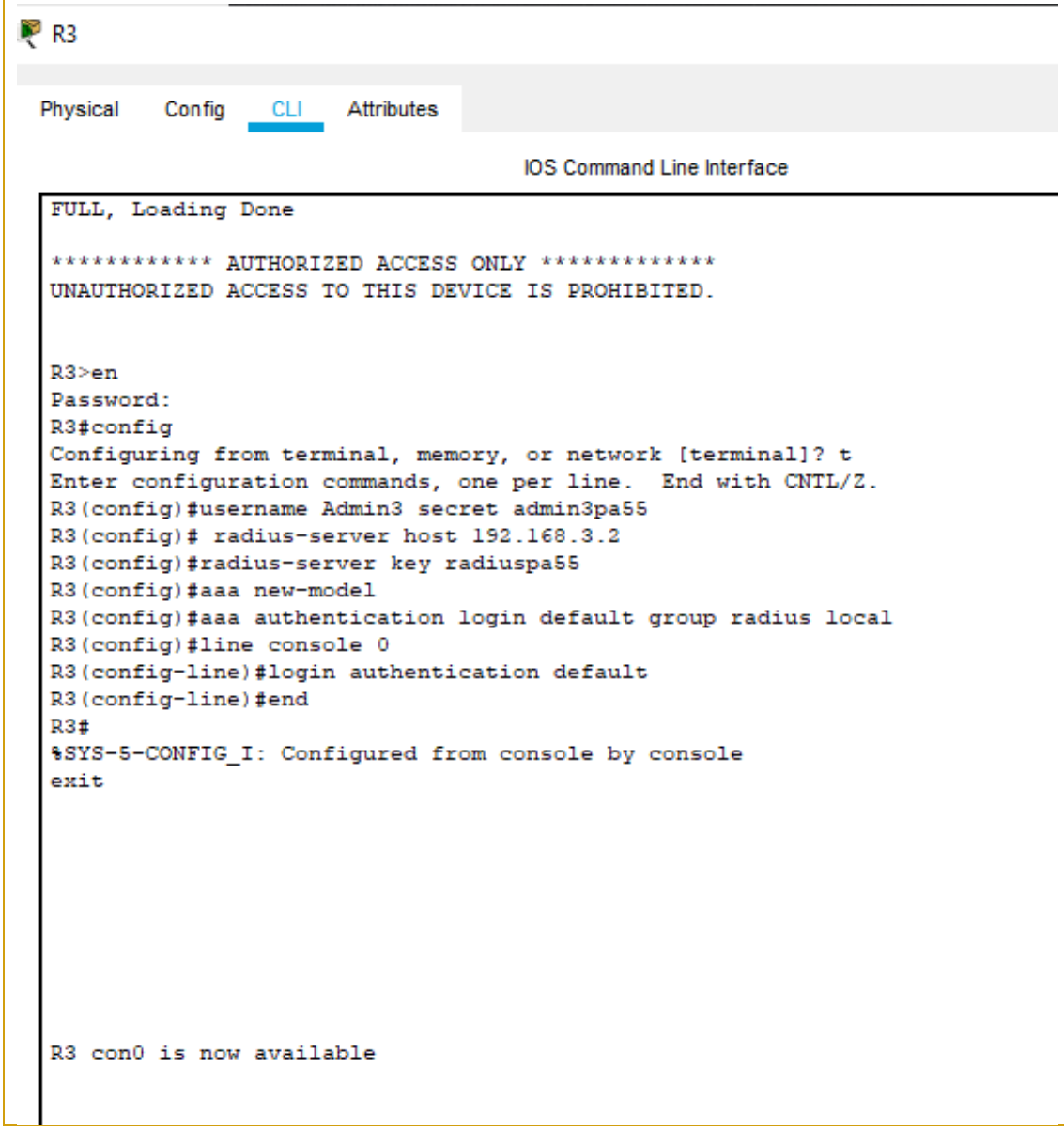
R3(config)# aaa new-model

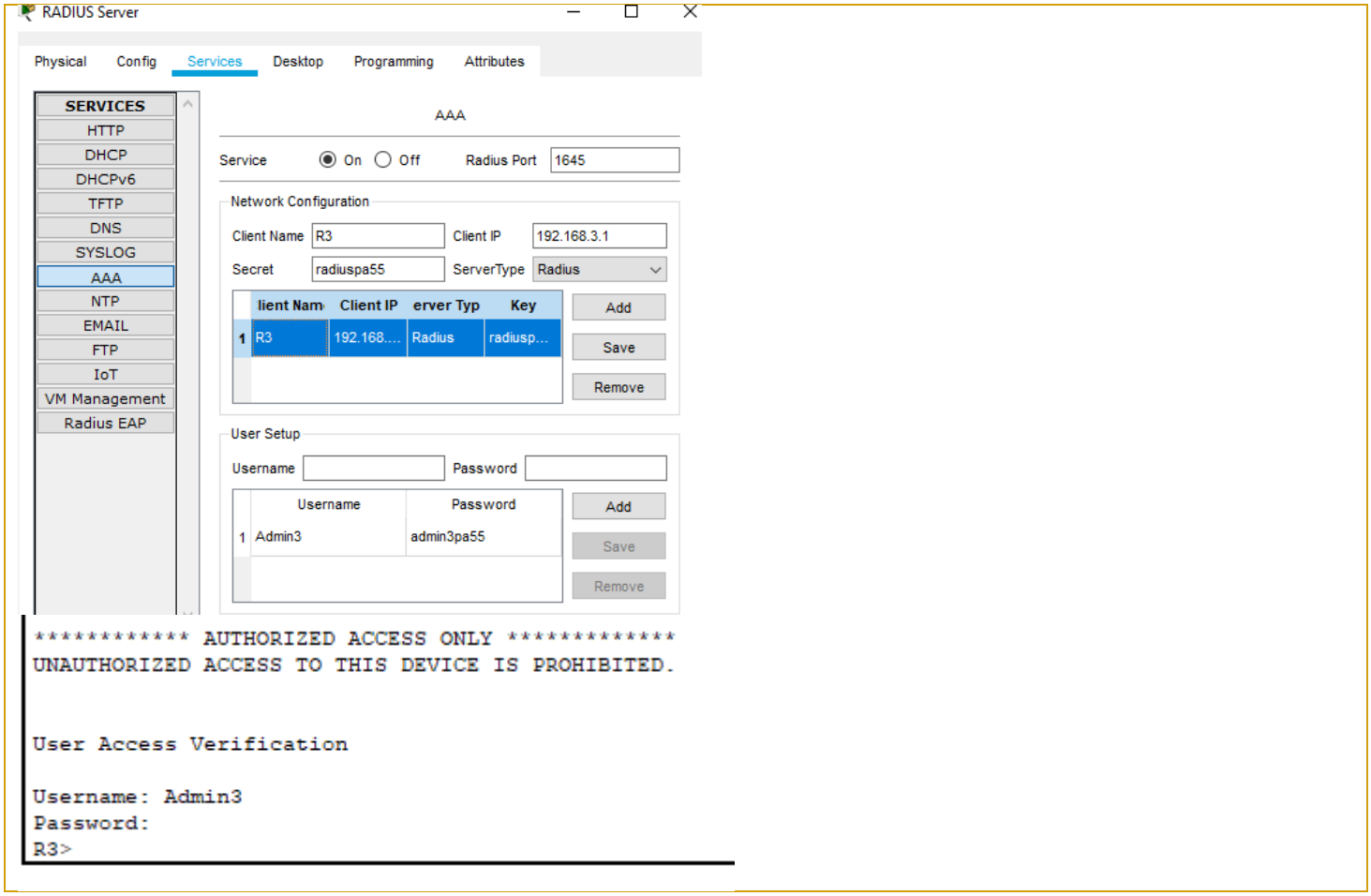
R3(config)# aaa authentication login default group radius local

Step 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.
R3(config)# line console 0
R3(config-line)# login authentication default
Step 6: Verify the AAA authentication method.
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: Admin3
Password: admin3pa55
R3>

Insert screenshots here




RADIUS Server
Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
AAA
Service
On
Off
Radius Port
1645
Network Configuration
Client Name
R3
Client IP
192.168.3.1
Secret
radiuspa55
ServerType
Radius
lient Nam
Client IP
erver Typ
Key
1
R3
192.168....
Radius
radiusp...
Add
Save
Remove
User Setup
Username
Password
Username
Password
1
Admin3
admin3pa55
Add
Save
Remove
********** AUTHORIZED ACCESS ONLY **********
UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.
User Access Verification
Username: Admin3
Password:
R3>