Cybersecurity Portfolio Project Report

Project Title: Configure AAA Authentication on Cisco Routers
Tool Used: Cisco Packet Tracer
Student Name: Thabiso K Dzveta

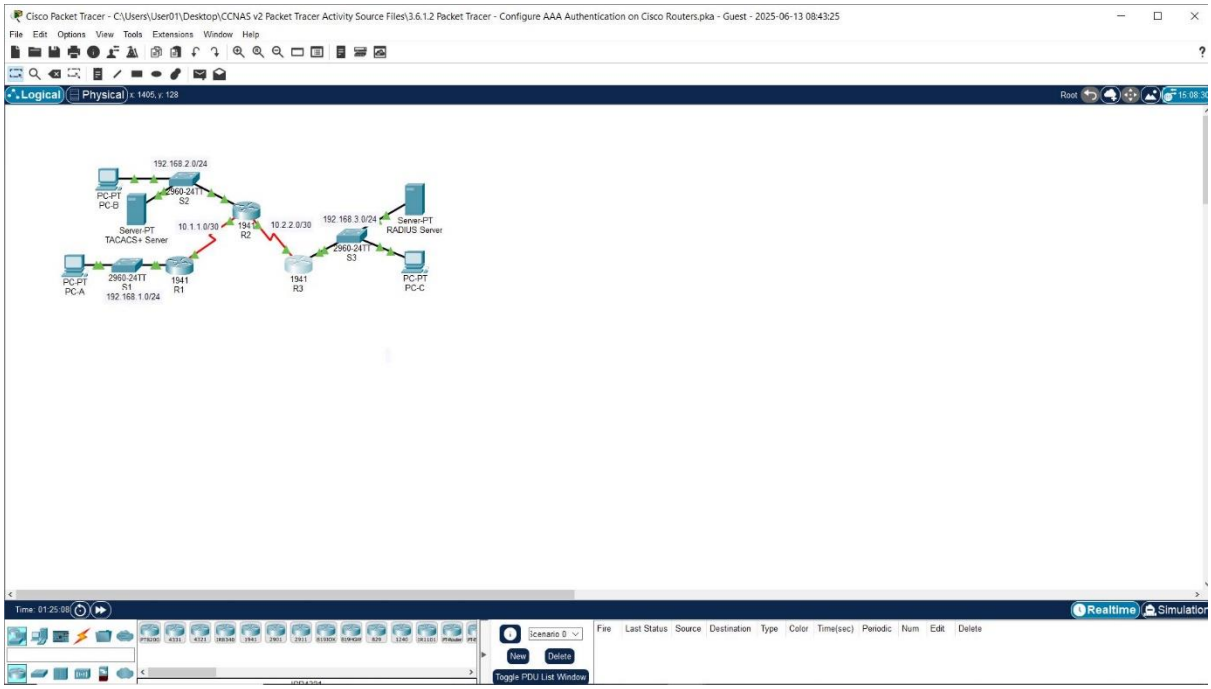
---

1. Project Overview

This project demonstrates the implementation of AAA (Authentication, Authorization, and Accounting) on Cisco routers using local, TACACS+, and RADIUS-based authentication. The objective is to improve administrative access security across routers in a network.

---

2. Network Topology



---

3. IP 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

---

4. AAA Configuration Summary

Part 1: Local AAA Authentication on R1 (Console and VTY)

Step-by-Step:

1. **Create Local User**

```
R1(config)# username Admin1 secret admin1pa55
```

2. **Enable AAA and Configure Console Login**

```
R1(config)# aaa new-model
R1(config)# aaa authentication login default local
```

3. **Apply to Console Line**

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

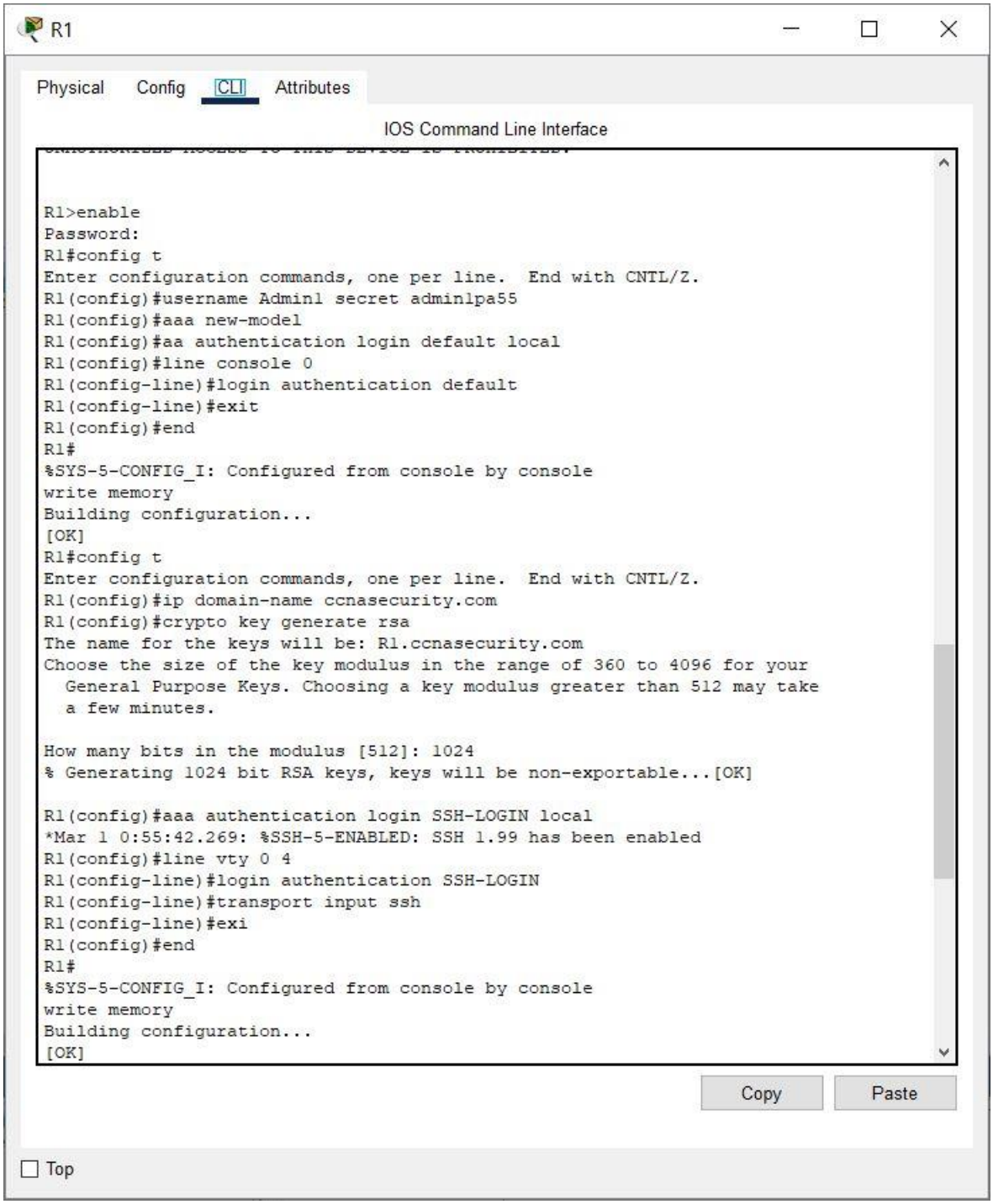
4. **Configure SSH for Remote Access**

```
R1(config)# ip domain-name ccnasecurity.com
```

R1(config)# crypto key generate rsa
! Select 1024 bits when prompted

5. Configure Named AAA Method List for VTY

R1(config)# aaa authentication login SSH-LOGIN local
R1(config)# line vty 0 4
R1(config-line)# login authentication SSH-LOGIN
R1(config-line)# transport input ssh



6. **Verify:**

- Connect via console to test local login.
- From PC-A, SSH into R1:

```
ssh -l Admin1 192.168.1.1
```

Part 2: TACACS+ AAA Authentication on R2

Step-by-Step:

1. **Create Backup Local User**

```
R2(config)# username Admin2 secret admin2pa55
```

2. **Configure TACACS+ Server Details**

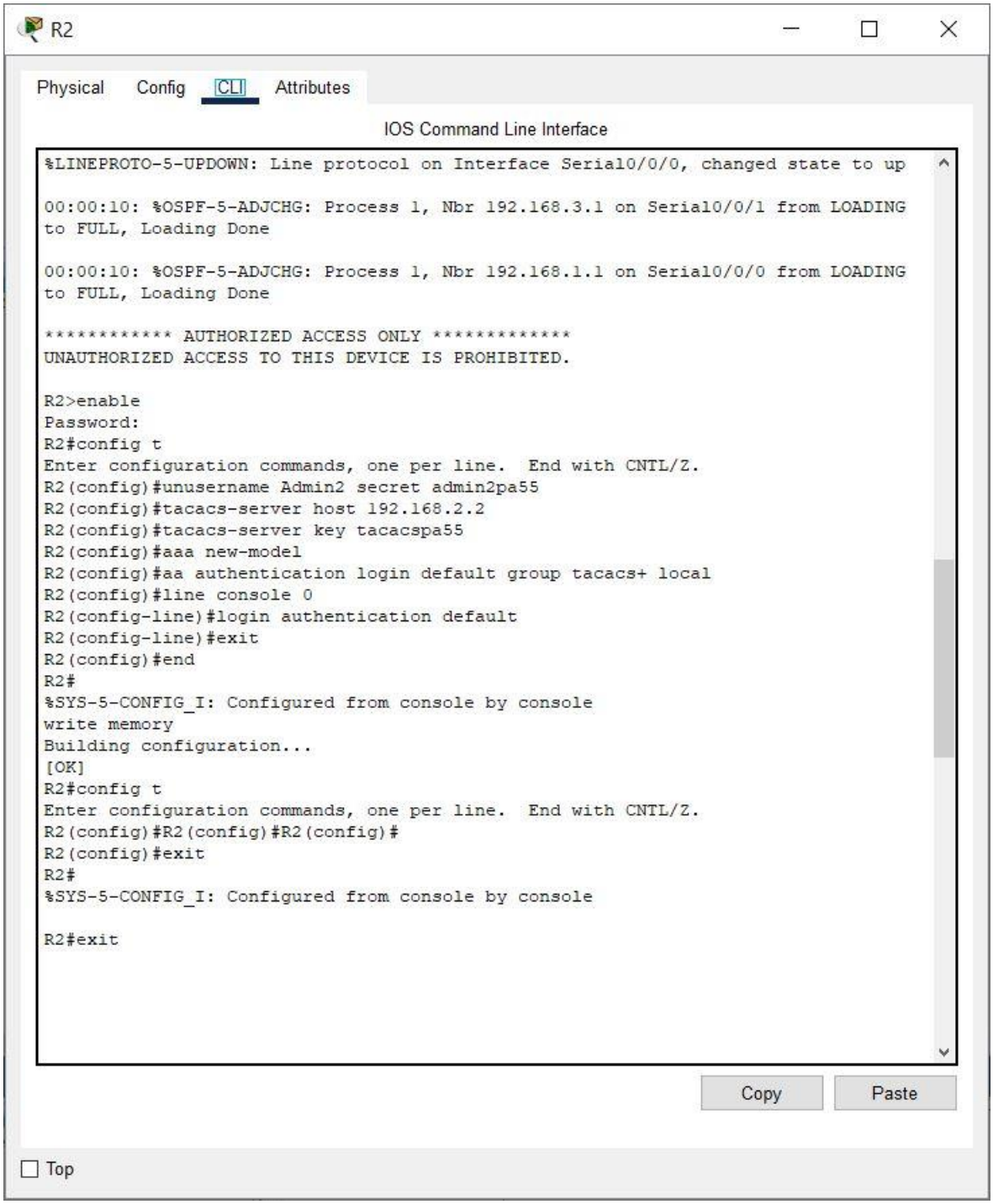
```
R2(config)# tacacs-server host 192.168.2.2
R2(config)# tacacs-server key tacacspa55
```

3. **Configure AAA Method with Local Backup**

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

4. **Apply to Console Line**

```
R2(config)# line console 0
R2(config-line)# login authentication default
```



5. **Verify:**

- Console into R2 or SSH from PC-B and test login using:

Username: Admin2
Password: admin2pa55

Part 3: RADIUS AAA Authentication on R3

Step-by-Step:

1. **Create Backup Local User**

```
R3(config)# username Admin3 secret admin3pa55
```

2. **Configure RADIUS Server Details**

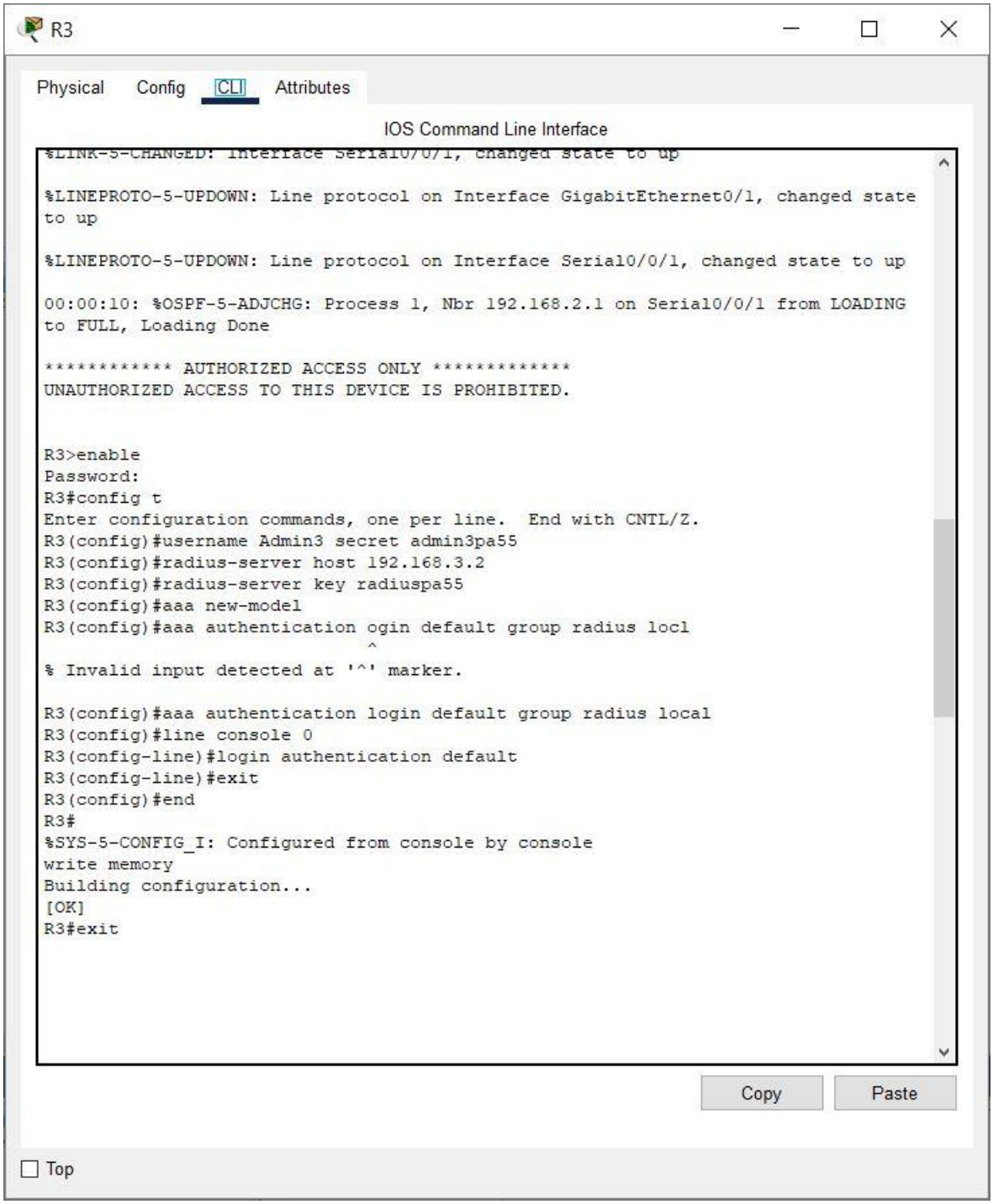
```
R3(config)# radius-server host 192.168.3.2
R3(config)# radius-server key radiuspa55
```

3. **Configure AAA Method with Local Backup**

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

4. **Apply to Console Line**

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



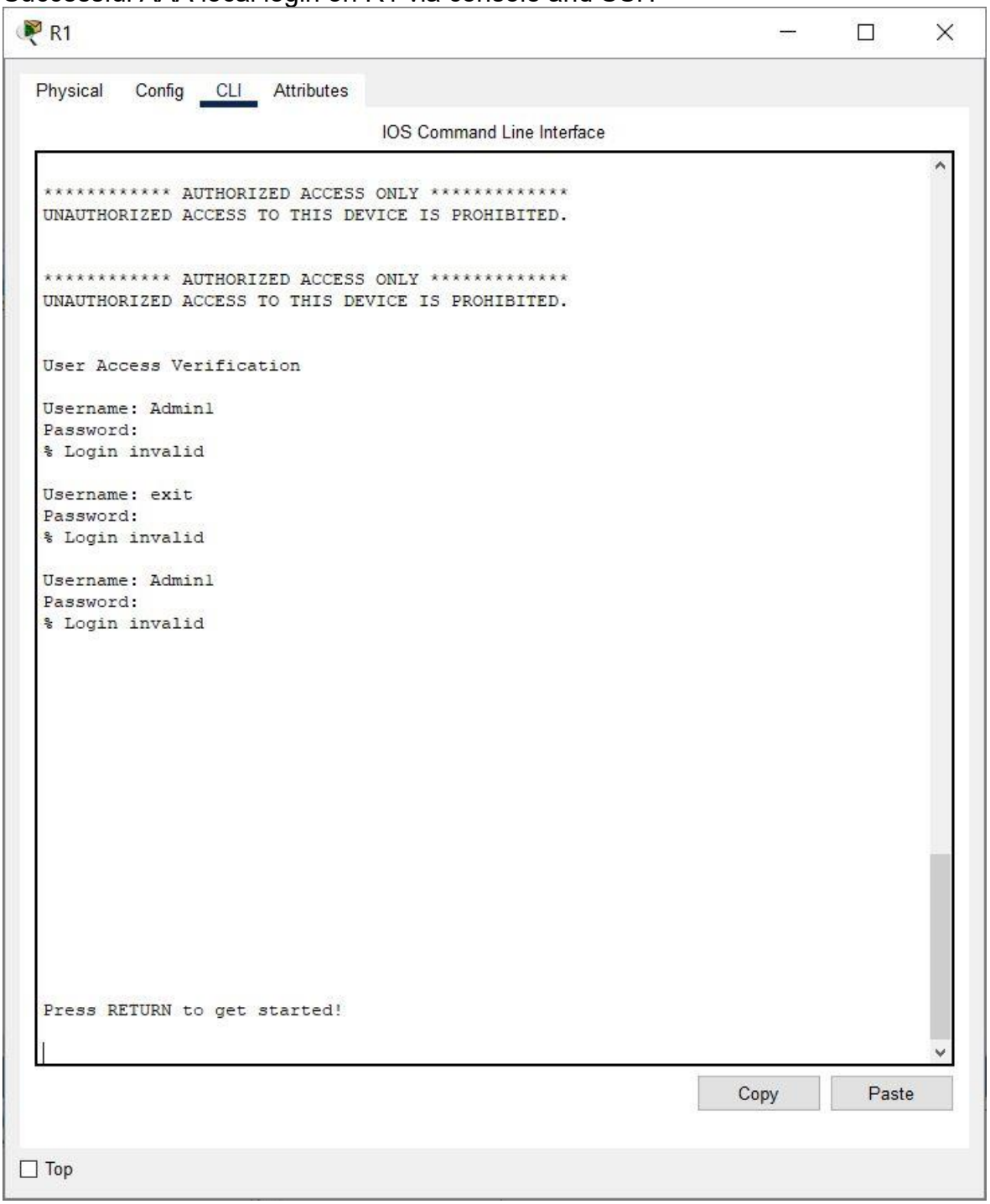
5. **Verify:**

- Console into R3 or SSH from PC-C and test login using:

Username: Admin3
Password: admin3pa55

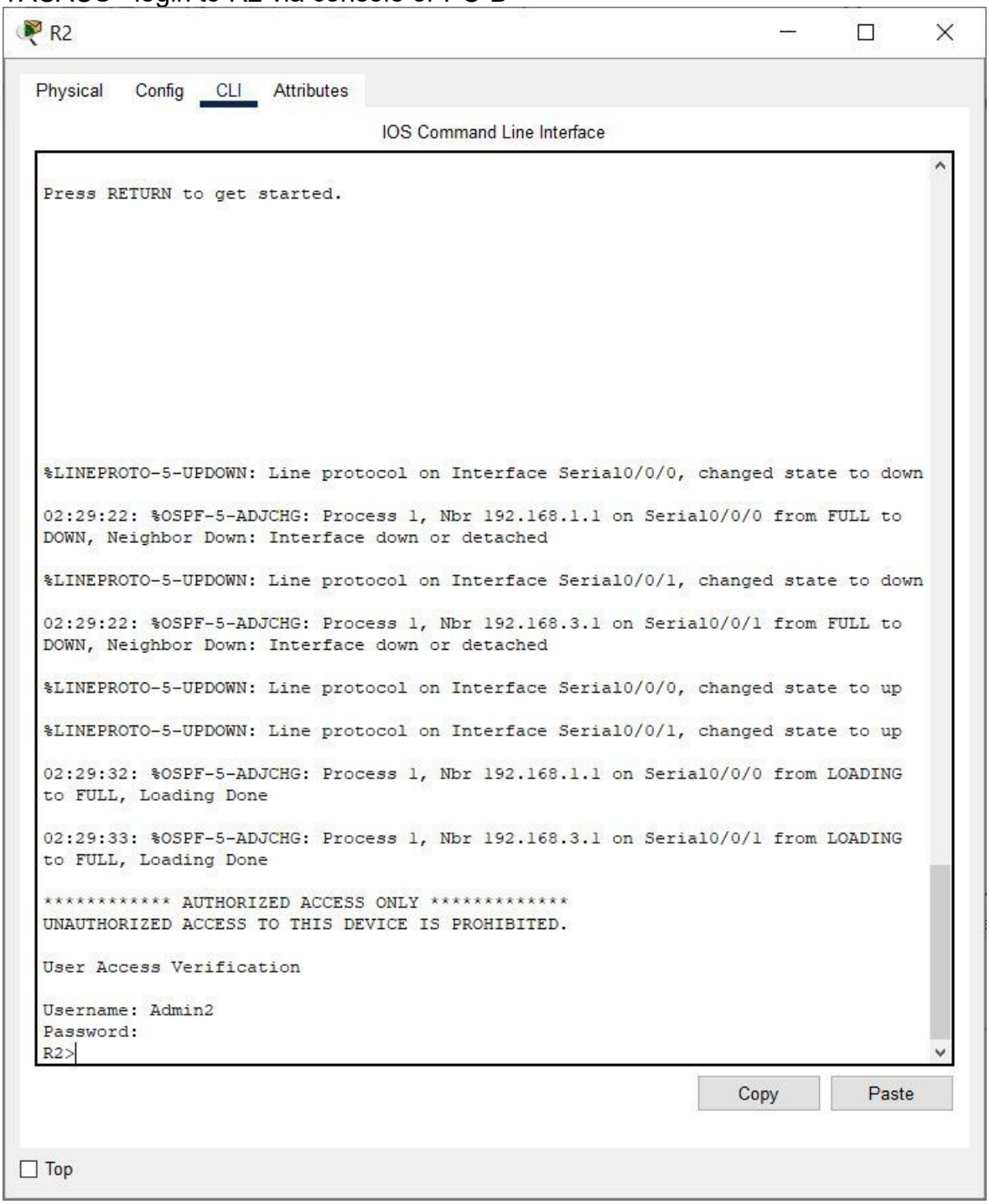
5. Verification Results

- Successful AAA local login on R1 via console and SSH



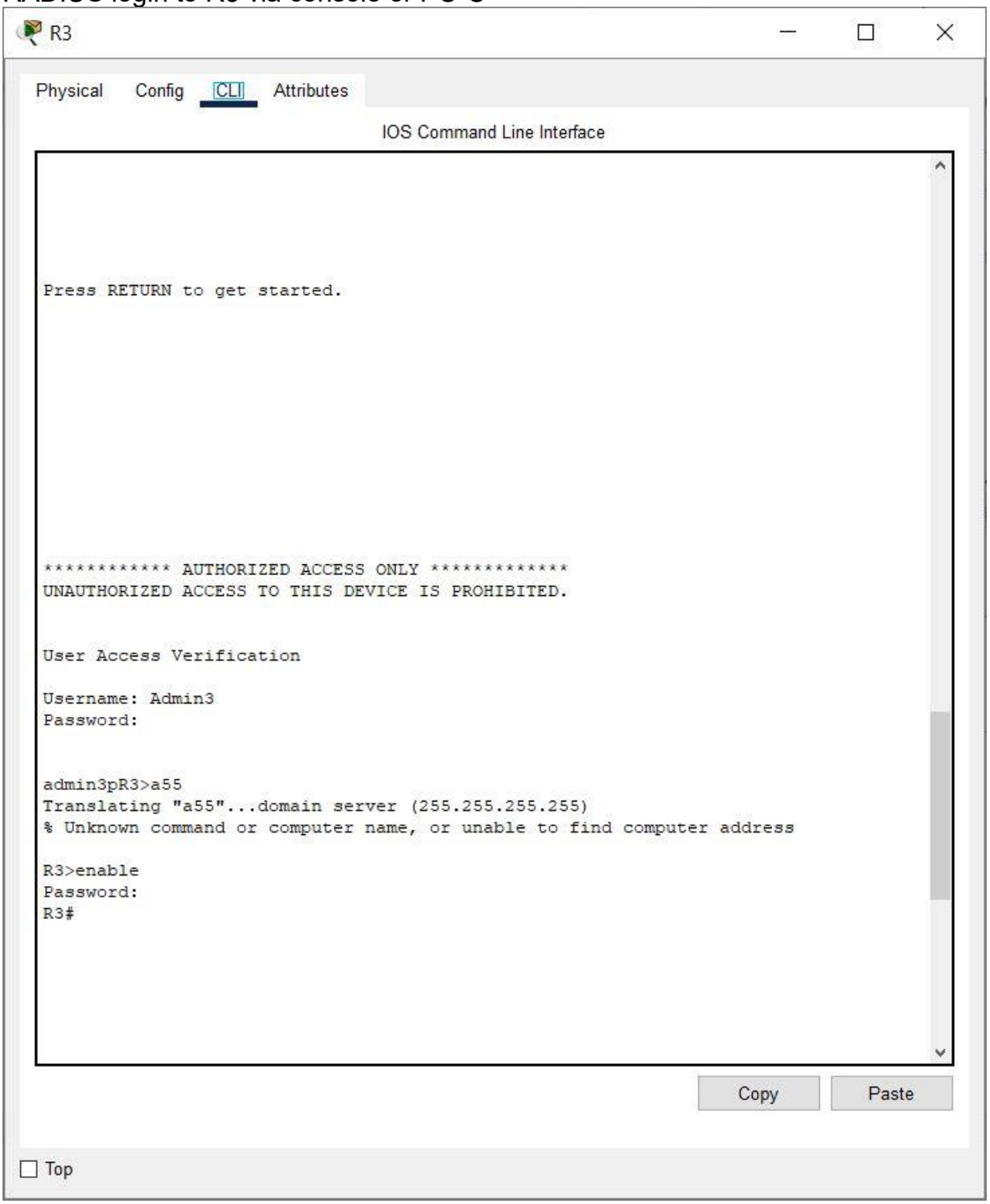
.

- TACACS+ login to R2 via console or PC-B



.

- RADIUS login to R3 via console or PC-C



.

6. Conclusion

This project highlights the process of securing administrative access to routers using multiple AAA methods. Each router was configured with fallback local accounts to ensure redundancy. The configurations demonstrate an enterprise-level access control solution leveraging local, TACACS+, and RADIUS authentication.

---

7. Reflection

This task deepened my understanding of:

- AAA architecture and protocols
- How to secure administrative access on Cisco IOS devices
- Integrating centralized authentication servers

[End of Report]