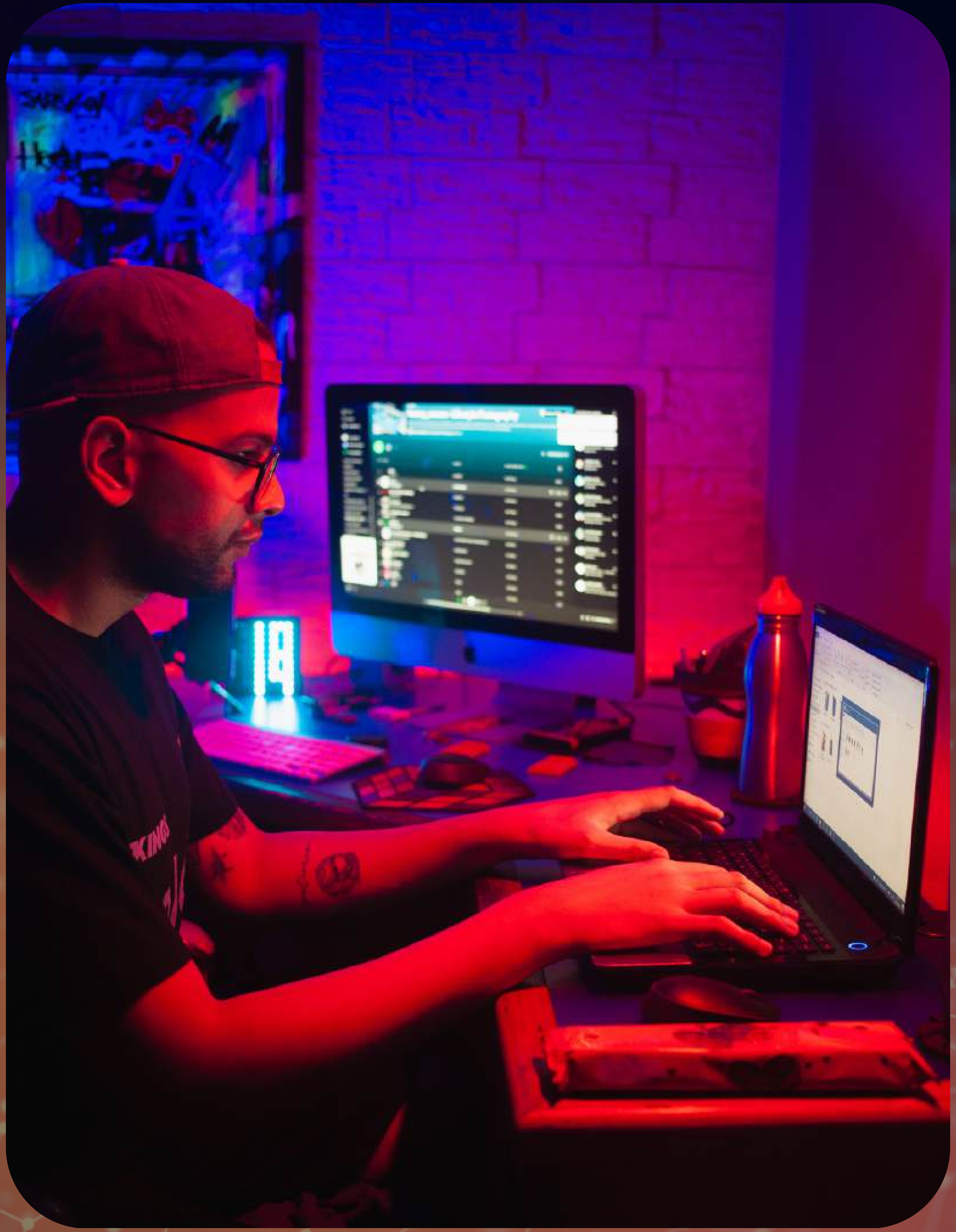
Enterprise Network Architecture Design Using VLAN Segmentation, Inter-VLAN Routing, and Dynamic IP Services

Michael Olayiwola



Origin of the creative idea

This project was created as part of my professional network engineering portfolio.

The idea was to design a lab that demonstrates skills beyond basic VLAN configuration; showcasing routing, service configuration, DHCP automation, DNS resolution, HTTP traffic, OSI-model analysis, and end-to-end enterprise connectivity.

The creative idea came from wanting a project that represents what a real network engineer builds in production.

Vision and mission

To design and implement a scalable, secure, and intelligently segmented enterprise network that demonstrates real-world Layer-3 and Layer-2 infrastructure capabilities, enabling automated IP management, seamless inter-department communication, centralized services, and efficient monitoring across all OSI model layers.

- To enable inter-VLAN routing through a multilayer switch
- To automate device configuration using DHCP
- To deliver centralized services including DNS and HTTP
- To simulate and analyze network behavior across the OSI model

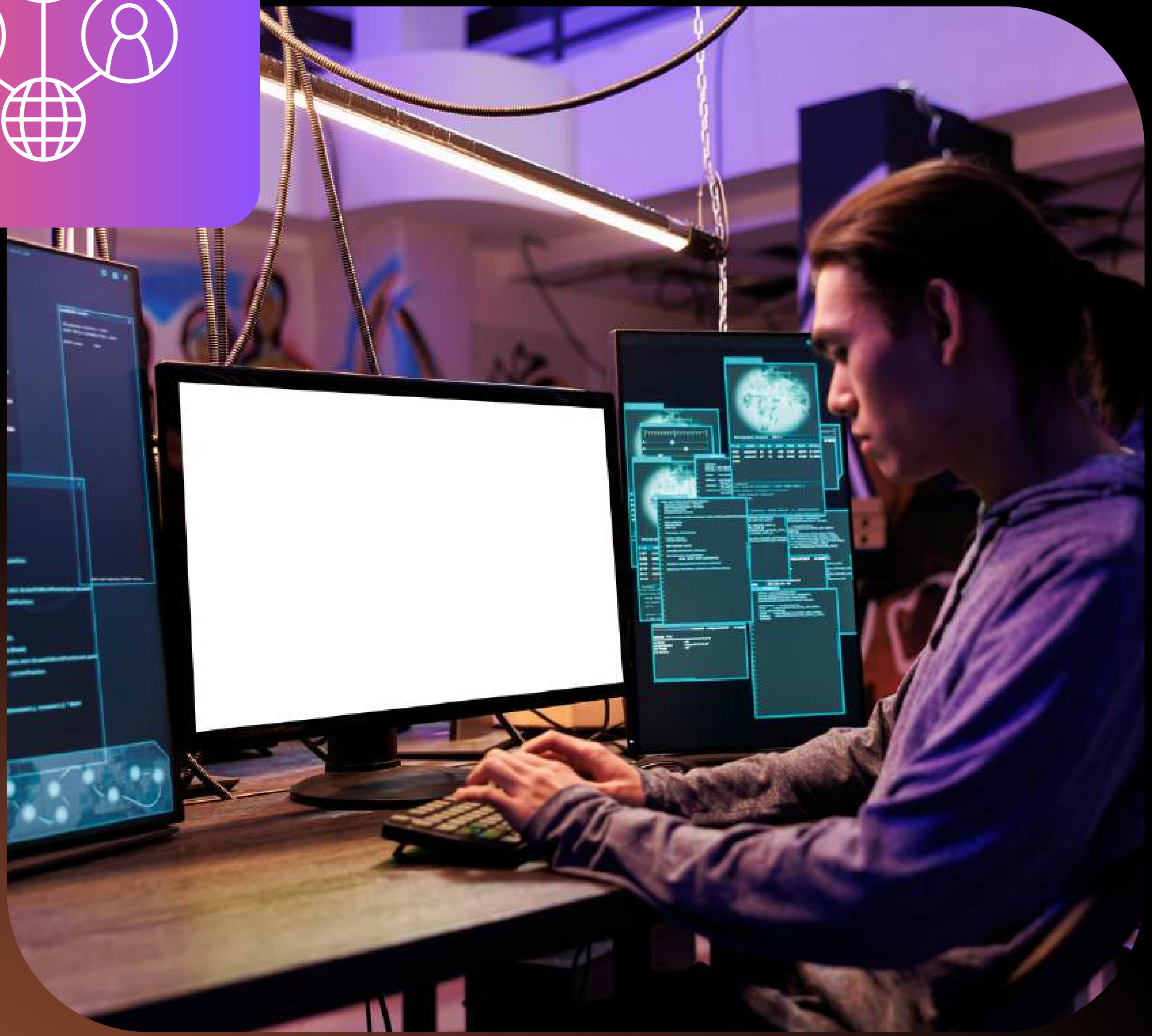
Ideation Process

The idea for this project emerged from my desire to move beyond basic networking tasks and build a realistic enterprise architecture that reflects modern industry practices.

While working with VLANs and trunking, I realized the need for automated IP management and centralized services, which inspired the integration of DHCP, DNS, and HTTP.

I also wanted to understand traffic behavior across the OSI model, leading me to incorporate simulation mode to observe packets, frames, and bits in real time.

Creation Process



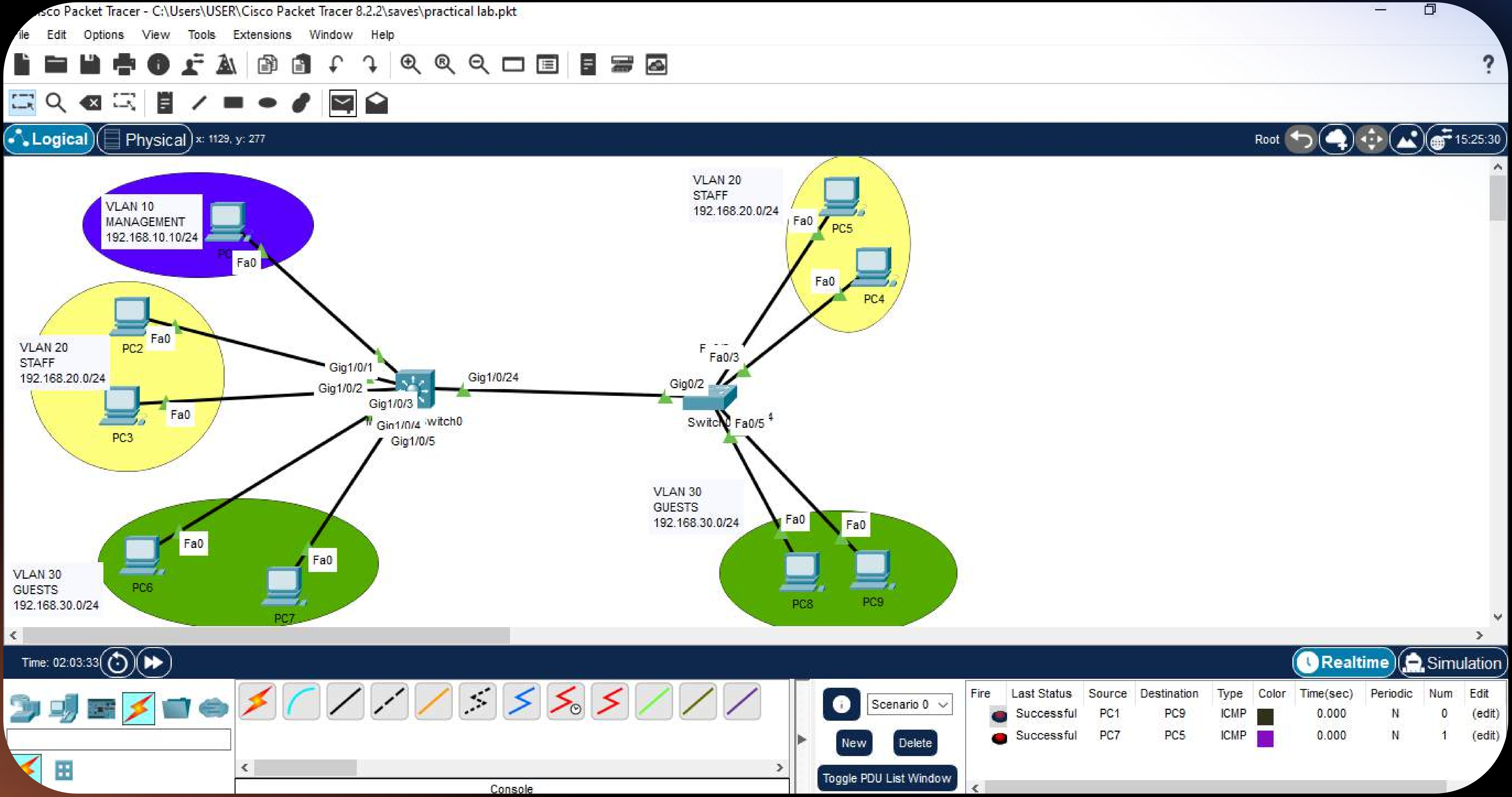
Designed the network topology by defining VLANs, IP subnets, trunk links, routing roles, and DHCP scopes to meet enterprise-level segmentation requirements.

Configured core services including DHCP, DNS, and HTTP on the server and ensured dynamic IP allocation for all connected hosts.

Implemented Layer-3 routing and Layer-2 switching using SVIs, inter-VLAN routing, trunking, and access-port assignments, followed by SSH-enabled secure device management.

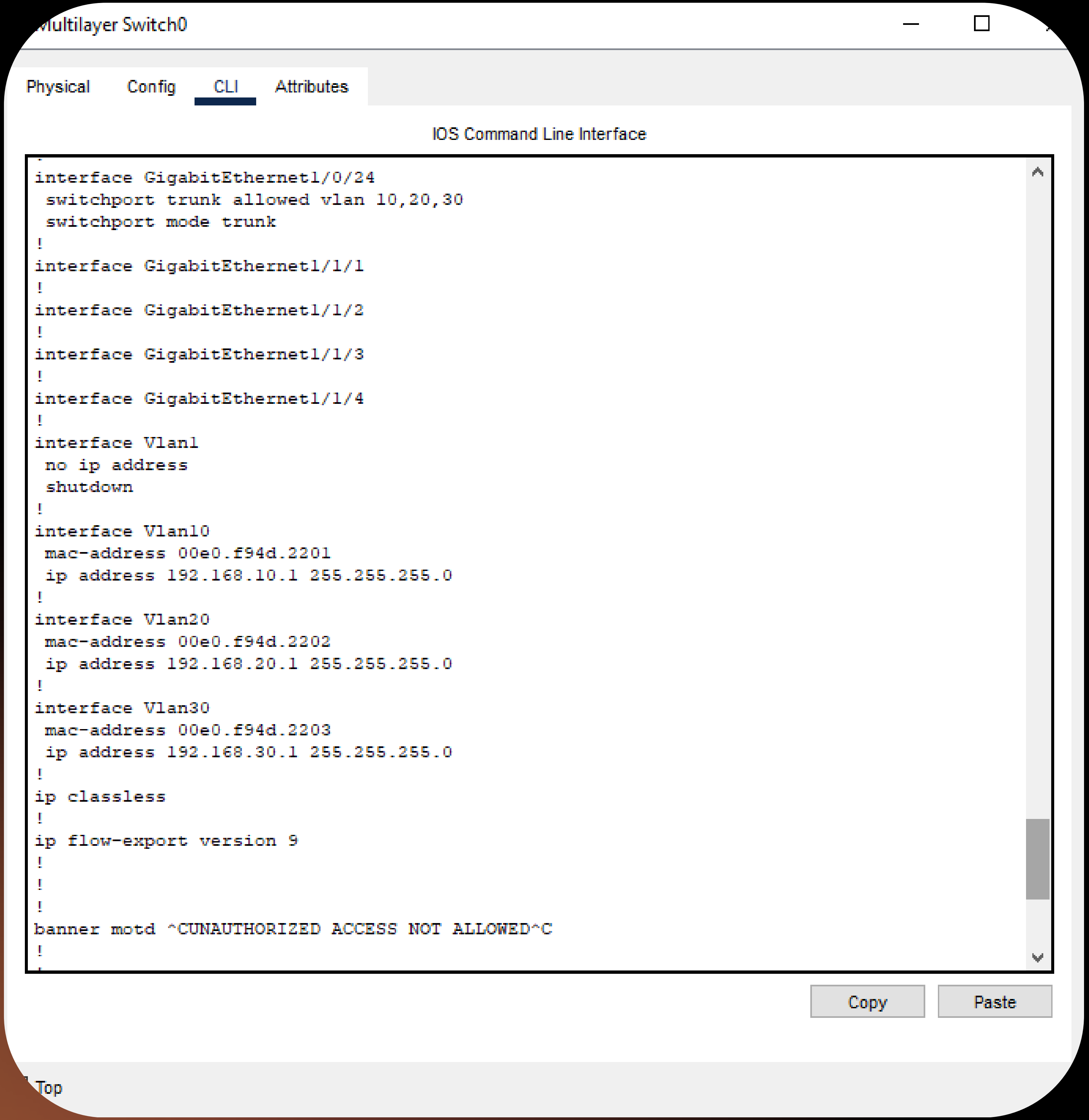
Validated the entire architecture through simulation mode by analyzing OSI-layer traffic and performing troubleshooting until all VLANs, services, and routes communicated successfully.

Network Topology

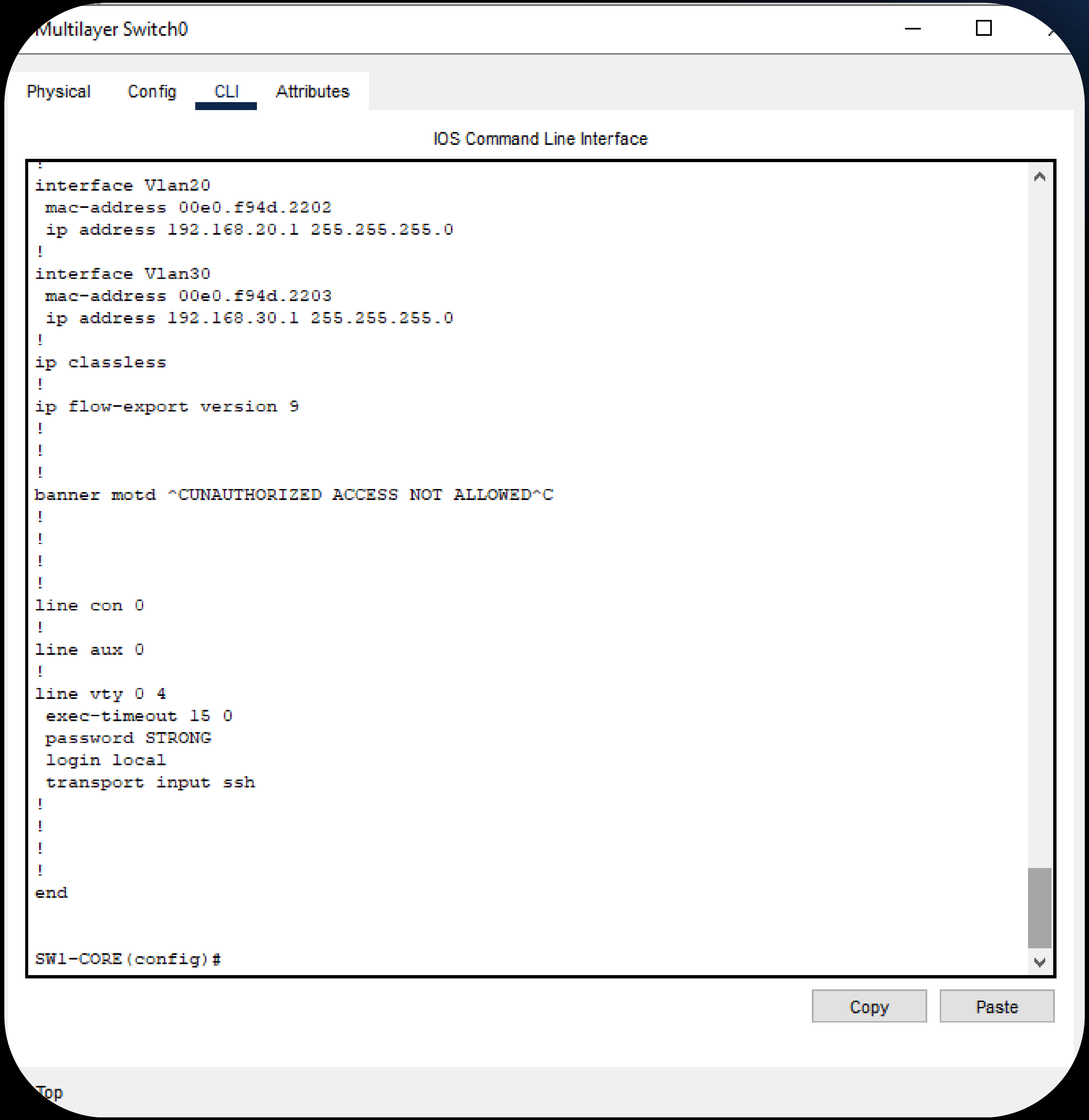


Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
●	Successful	PC1	PC9	ICMP	■	0.000	N	0	(edit)
●	Successful	PC7	PC5	ICMP	■	0.000	N	1	(edit)

CLI



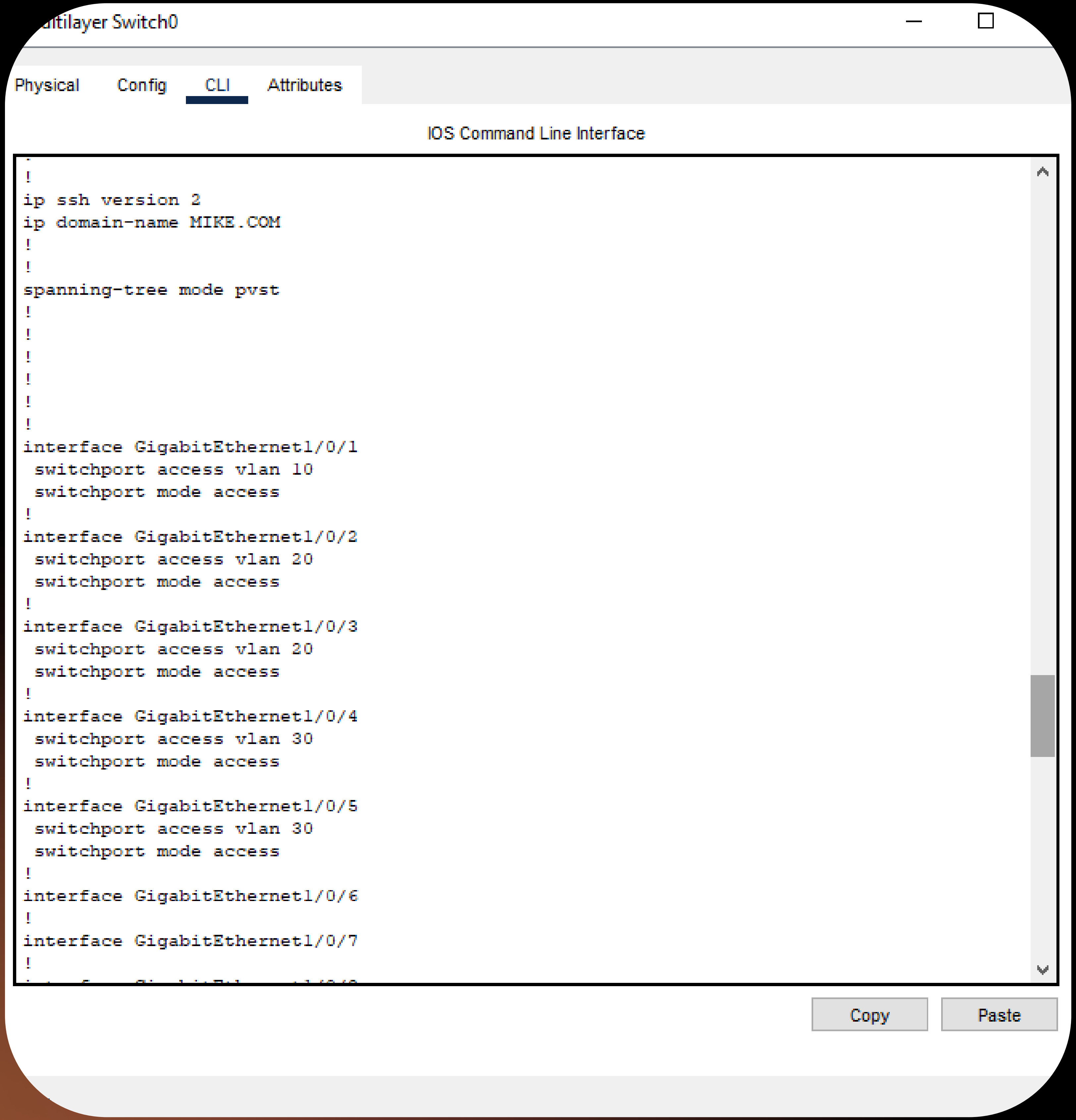
```
interface GigabitEthernet1/0/24
 switchport trunk allowed vlan 10,20,30
 switchport mode trunk
!
interface GigabitEthernet1/1/1
!
interface GigabitEthernet1/1/2
!
interface GigabitEthernet1/1/3
!
interface GigabitEthernet1/1/4
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 mac-address 00e0.f94d.2201
 ip address 192.168.10.1 255.255.255.0
!
interface Vlan20
 mac-address 00e0.f94d.2202
 ip address 192.168.20.1 255.255.255.0
!
interface Vlan30
 mac-address 00e0.f94d.2203
 ip address 192.168.30.1 255.255.255.0
!
ip classless
!
ip flow-export version 9
!
!
!
banner motd ^CUNAUTHORIZED ACCESS NOT ALLOWED^C
!
```



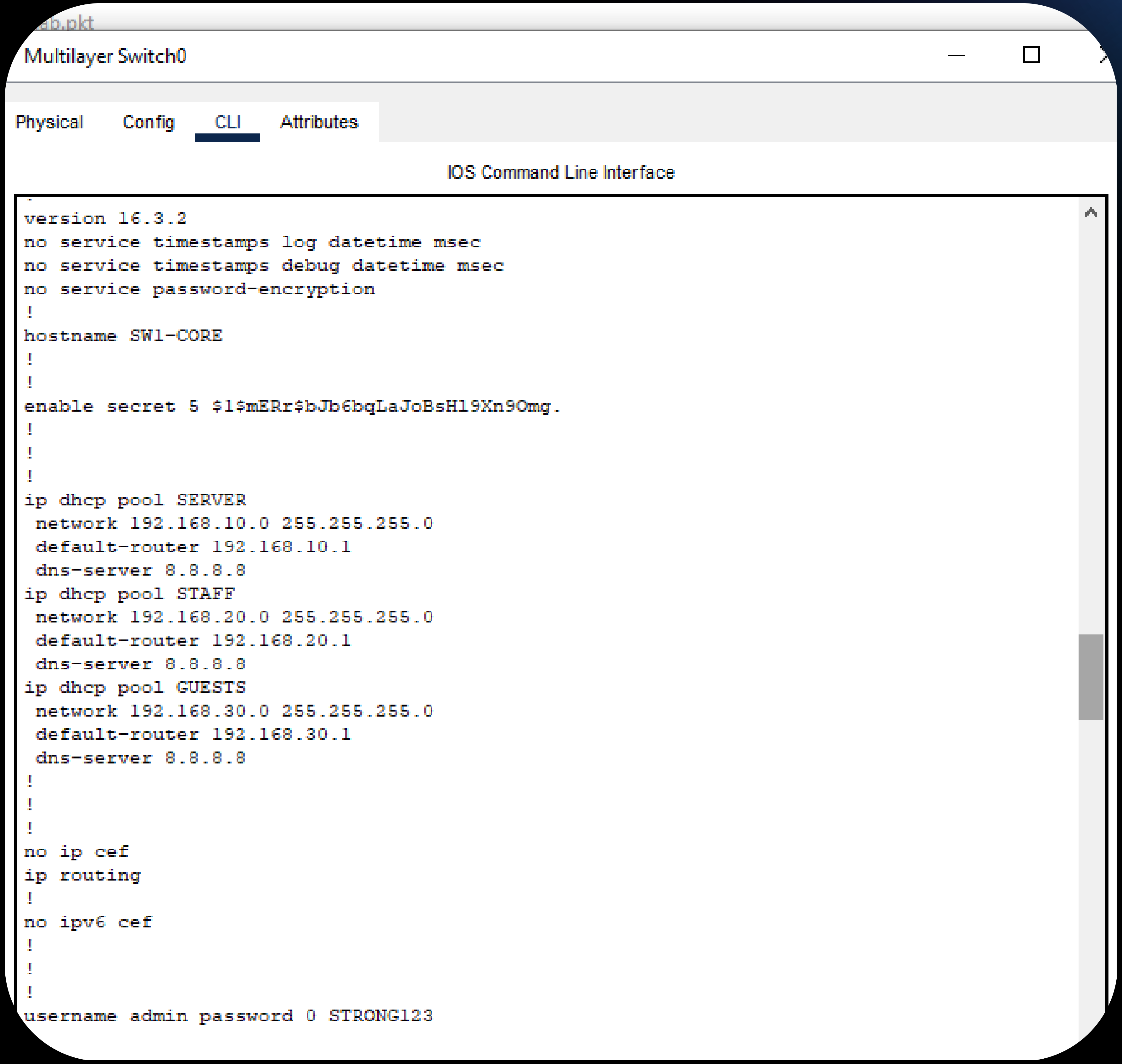
```
interface Vlan20
 mac-address 00e0.f94d.2202
 ip address 192.168.20.1 255.255.255.0
!
interface Vlan30
 mac-address 00e0.f94d.2203
 ip address 192.168.30.1 255.255.255.0
!
ip classless
!
ip flow-export version 9
!
!
!
banner motd ^CUNAUTHORIZED ACCESS NOT ALLOWED^C
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
 exec-timeout 15 0
 password STRONG
 login local
 transport input ssh
!
!
!
!
end


SW1-CORE(config)#
```

CLI



```
!
ip ssh version 2
ip domain-name MIKE.COM
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet1/0/1
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet1/0/2
 switchport access vlan 20
 switchport mode access
!
interface GigabitEthernet1/0/3
 switchport access vlan 20
 switchport mode access
!
interface GigabitEthernet1/0/4
 switchport access vlan 30
 switchport mode access
!
interface GigabitEthernet1/0/5
 switchport access vlan 30
 switchport mode access
!
interface GigabitEthernet1/0/6
!
interface GigabitEthernet1/0/7
!
```



```
version 16.3.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname SW1-CORE
!
!
enable secret 5 $1$mERr$bJb6bqLaJoBsHl9Xn9Omg.
!
!
!
ip dhcp pool SERVER
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.1
 dns-server 8.8.8.8
ip dhcp pool STAFF
 network 192.168.20.0 255.255.255.0
 default-router 192.168.20.1
 dns-server 8.8.8.8
ip dhcp pool GUESTS
 network 192.168.30.0 255.255.255.0
 default-router 192.168.30.1
 dns-server 8.8.8.8
!
!
!
no ip cef
ip routing
!
no ipv6 cef
!
!
!
username admin password 0 STRONG123
```

Weaknesses

- High learning curve: Advanced concepts like dynamic trunking, routing logic, and OSI traffic interpretation require more repetition to fully master.
- Limited scalability testing: The project focuses on a small enterprise topology and has not yet explored redundancy, STP, HSRP/VRRP, or failover mechanisms.

Strengths

- Real-world enterprise design: Integrates VLANs, DHCP, DNS, HTTP, trunking, and inter-VLAN routing, demonstrating practical, job-ready network engineering skills.
- Strong troubleshooting ability: Successfully resolved native VLAN mismatches, SVI issues, routing gaps, and DHCP conflicts using systematic verification commands and OSI-model analysis.

Threats

- Rapid industry evolution: Networking technologies like SDN, automation, and cloud networking may require continuous upskilling to stay relevant.
- Configuration errors in larger environments: Misconfigured VLANs, trunks, or DHCP scopes can create significant vulnerabilities or outages in real enterprise settings.

Opportunities

- Expand into security engineering: Project can evolve into ACLs, port security, firewall zoning, IPS/IDS labs, and segmentation hardening, which are key cybersecurity competencies.
- Opportunity for certification readiness: This project forms a solid foundation for professional exams like Cisco CCNA/CCNP, helping deepen theoretical understanding through hands-on, scenario-based practice.

Final reflections & future steps

This project strengthened my confidence in designing real-world enterprise networks, especially in understanding how VLANs, routing, DHCP, and core services work together to create a secure, efficient infrastructure.

It also reinforced the importance of careful configuration, verification, and OSI-layer analysis in solving complex networking issues.

Moving forward, I plan to expand this topology by adding redundancy protocols, implementing ACLs and security policies, and exploring automation with Python and Ansible. These next steps will help me build more resilient, scalable, and security-focused network architectures.