NETWORK SECURITY PROJECT REPORT

ABSTRACT

This project demonstrates the design and security configuration of a small office network using Cisco Packet Tracer, Nmap, and Wireshark. The objective is to understand how network components communicate, identify vulnerabilities, and apply security controls such as VLANs, firewalls, and access restrictions.

1. INTRODUCTION

The purpose of this project is to simulate a small office or personal network setup to understand network communication, segmentation, and security hardening.
In this project, we designed and secured a small office network using **Cisco Packet Tracer.** The main purpose of this work was to understand how a network can be vulnerable to attacks and how basic security measures can protect it. We focused on practical, hands-on learning by creating a network that includes routers, switches, a firewall, servers, and end-user devices, and then applying security controls to safeguard it. We planned and built the network step by step, assigning IP addresses, connecting devices with the correct cables, and configuring VLANs to separate trusted and untrusted areas. We also configured the firewall and router to secure traffic flow between the internal network and the Internet. By simulating a common threat, an unauthorized access attempt, we tested whether our security measures could effectively prevent an untrusted user from reaching sensitive internal resources. This project allowed us to apply and understand three essential security controls: firewall rules, strong password policies, and VLAN-based network segmentation. These controls reflect the same principles used in real-world networks to separate users, prevent unauthorized access, and protect sensitive data. Through this exercise, we gained practical experience in network design, device configuration, and threat prevention. It also provided insight into how simple but well-planned security measures can significantly improve the protection of even a small office network. This knowledge is directly applicable to real business environments, where network security is essential for safeguarding data, ensuring reliable operations, and maintaining user trust.

2. OBJECTIVES

1. Design a simple and secure network using VLANs and a firewall.
2. Implement and test communication between different network zones.
3. Apply firewall rules to control access between Office, Guest, and IoT networks.
4. Use Nmap for port scanning and vulnerability detection.
5. Use Wireshark to capture and analyze network packets.

3. TOOLS AND SOFTWARE USED

- Cisco Packet Tracer: To design, configure, and test the small network.
- Command Line Interface (CLI): To enter network configuration commands.
- Simulation Mode (in Packet Tracer): To observe how data moves and how security rules affect traffic.
- Parrot OS (Wireshark & Nmap)

4. Network Design and Topology

The network consists of three VLANs to represent different zones:
- VLAN 10: Office Network
- VLAN 20: Guest Network
- VLAN 30: IoT Network

The router connects all VLANs and provides inter-VLAN routing.
A firewall is used to enforce access control policies.
A server, workstation, and IoT device are connected as endpoints.

4.1 DEVICES USED

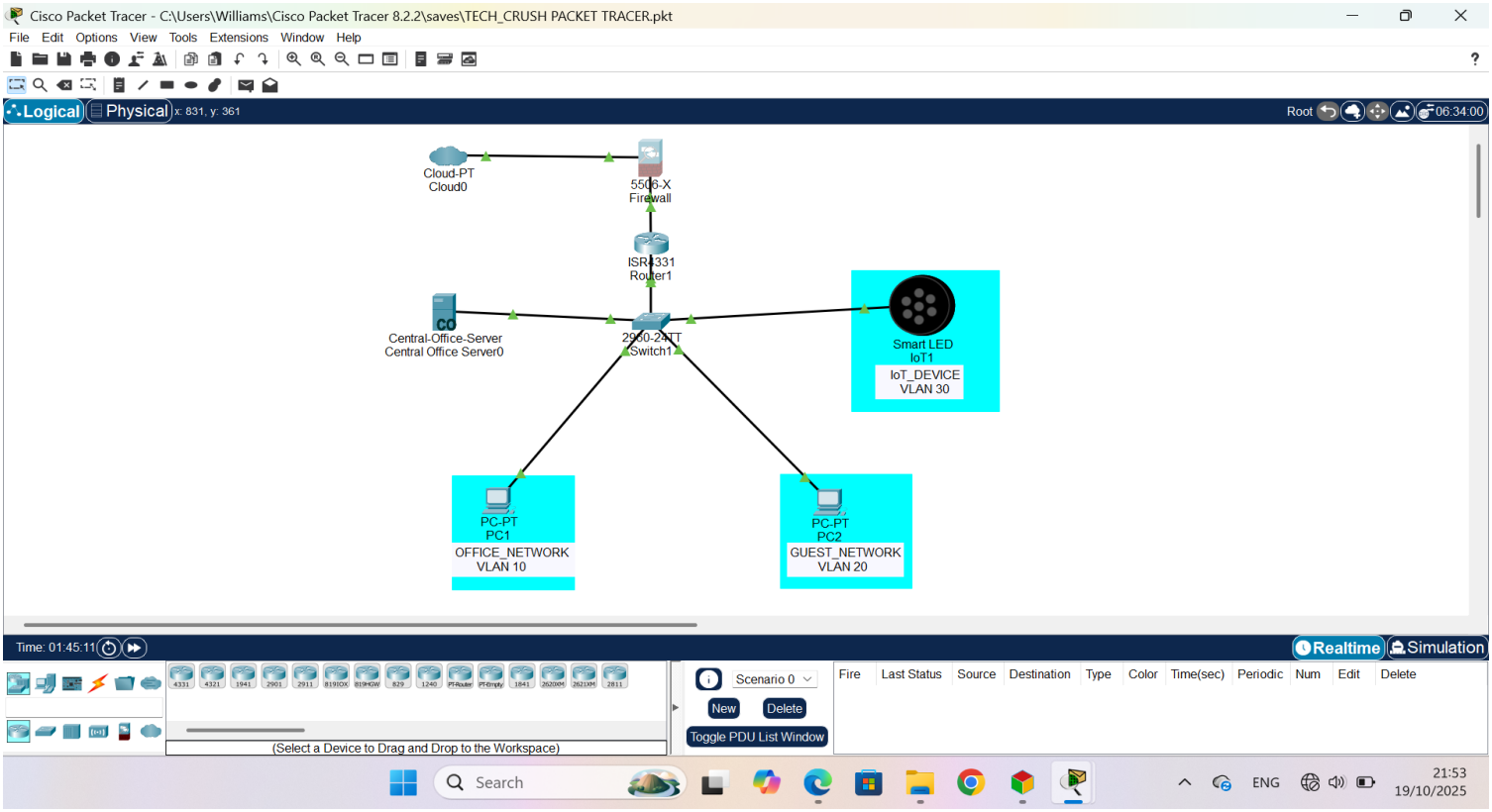
DEVICE TYPE	QUANTITY	MODEL EXAMPLE	PURPOSE
Firewall	1	Cisco ASA 5506-X	Protects the network by filtering traffic from the Internet
Router1	1	Cisco ISR 4331	Routes traffic between the firewall and the internal network
Switch1	1	Cisco 2960-24TT IOS15	Connects internal devices and manages VLANs
Server0	1	Central-Office-Server	Represents an internal company server
PC1	1	PC-PT	Represents an employee workstation
PC2	1	PC-PT	Represents a guest workstation

IoT1	1	Smart LED	IoT device
Cloud0	1	Cloud-PT	Simulates the Internet connection

4.2 NETWORK TOPOLOGY

The network is arranged as follows:

Cloud → Firewall → Router → Switch → Devices (Server, Office PC, Guest PC, IoT)



This means that all internal devices connect to the switch, the switch connects to the router, the router connects to the firewall, and the firewall connects to the Internet cloud.

4.3 Cable Types and Connections

CONNECTION	CABLE TYPE	INTERFACE DETAILS
Cloud to Firewall	Copper Straight-Through	Cloud Ethernet6 connected to Firewall GigabitEthernet1/2 outside interface.
Firewall to Router	Copper Straight-Through	Firewall Inside GigabitEthernet1/1 is

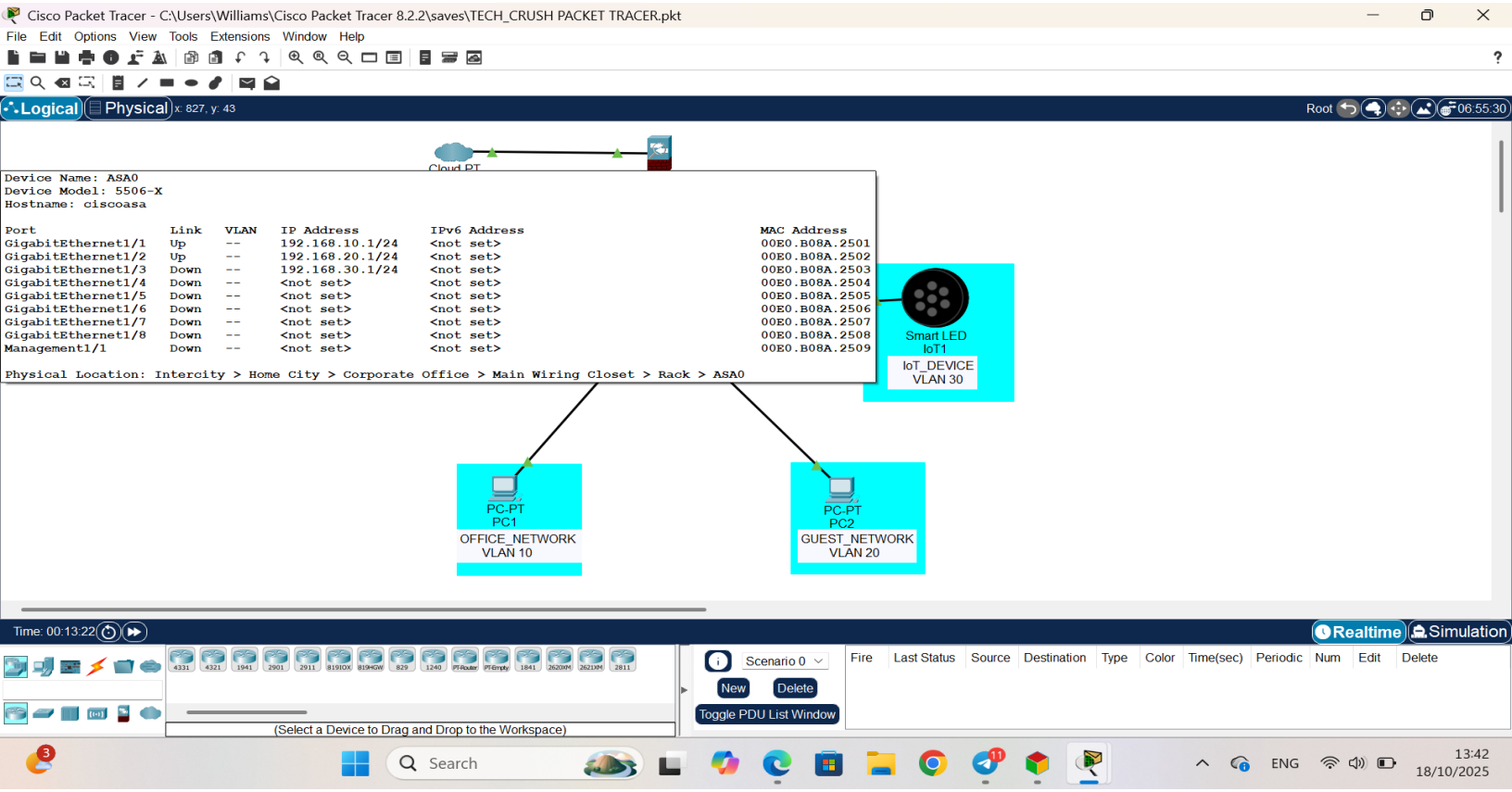
		connected to Router GigabitEthernet0/0 /1
Router to Switch	Copper Straight-Through	Router GigabitEthernet0/0/0 connected to Switch GigabitEthernet0/1
Switch to Server	Copper Straight-Through	Switch FastEthernet0/4 connected to Server FastEthernet0/0
Switch to Office PC	Copper Straight-Through	Switch FastEthernet0/1 connected to Office PC FastEthernet0
Switch to Guest PC	Copper Straight-Through	Switch FastEthernet0/2 connected to Guest PC FastEthernet0
Switch to IoT	Copper Straight-Through	Switch FastEthernet0/3 connected to IoT FastEthernet0

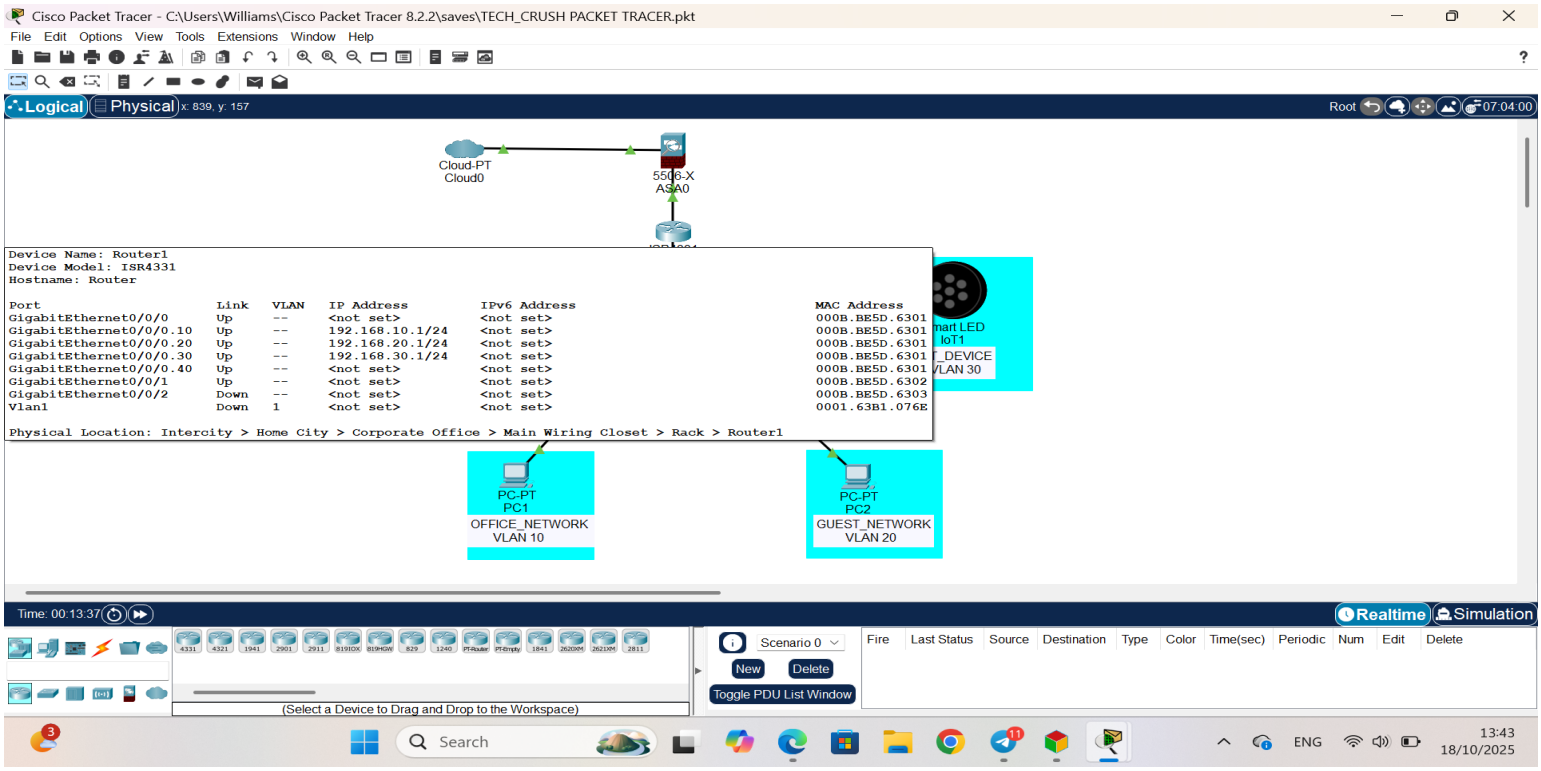
4.4 IP Addressing Plan

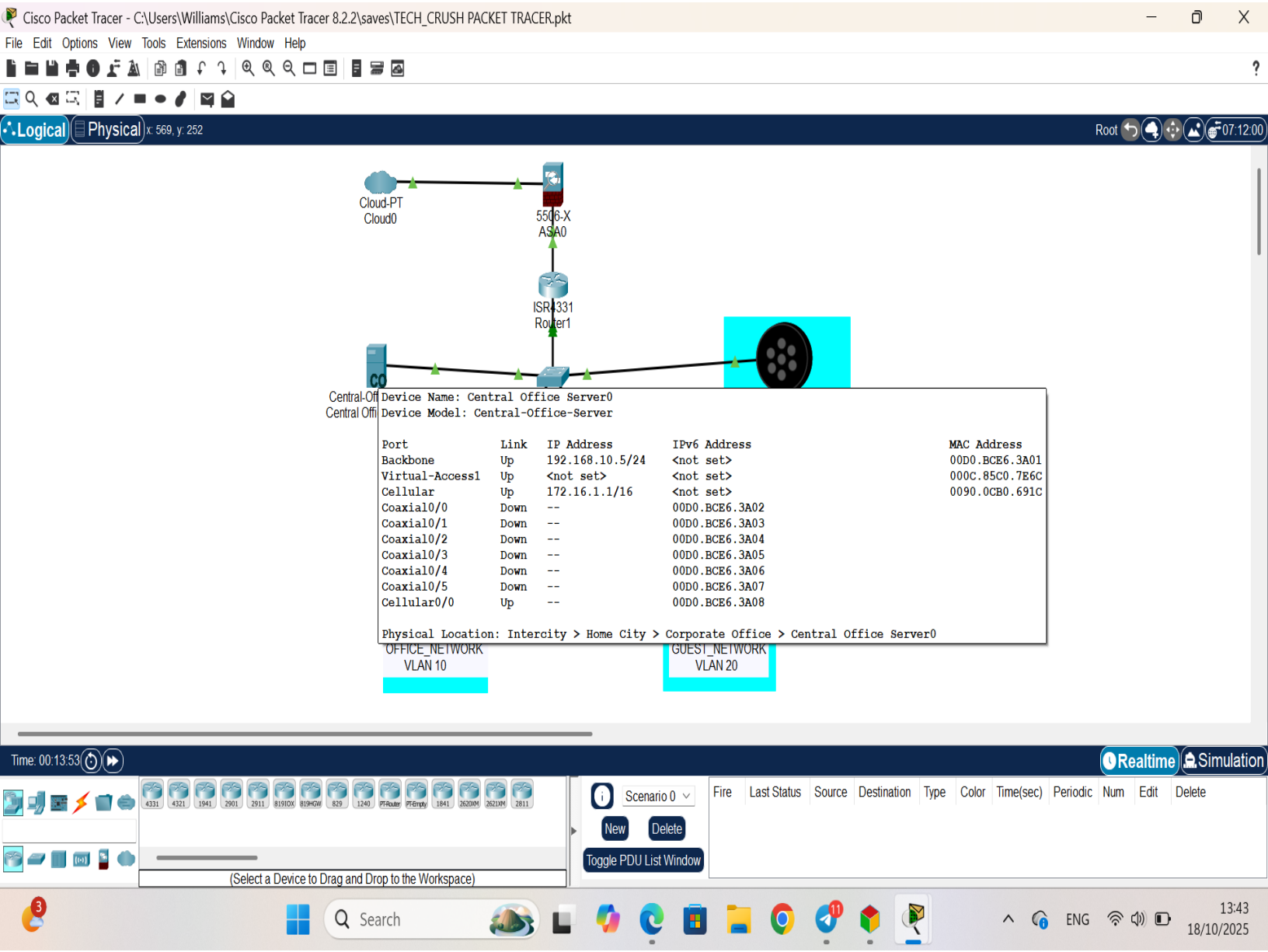
DEVICE	INTERFACE	IP ADDRESS	SUBNET MASK	PURPOSE
Firewall (Outside)	Connected to Cloud	203.0.113.1	255.255.255.0	Internet-facing interface
Firewall (Inside)	Connected to Router G0/0 /1	192.168.10.1 192.168.20.1 192.168.30.1	255.255.255.0	Internal interface for Router connection
Router (G0/0/1)	Connected to Firewall Inside	192.168.10.1 192.168.20.1 192.168.30.1	255.255.255.0	Connection to Firewall
Router (G0/0/0)	Connected to Switch	192.168.10.1 192.168.20.1 192.168.30.1	255.255.255.0	Gateway for internal devices

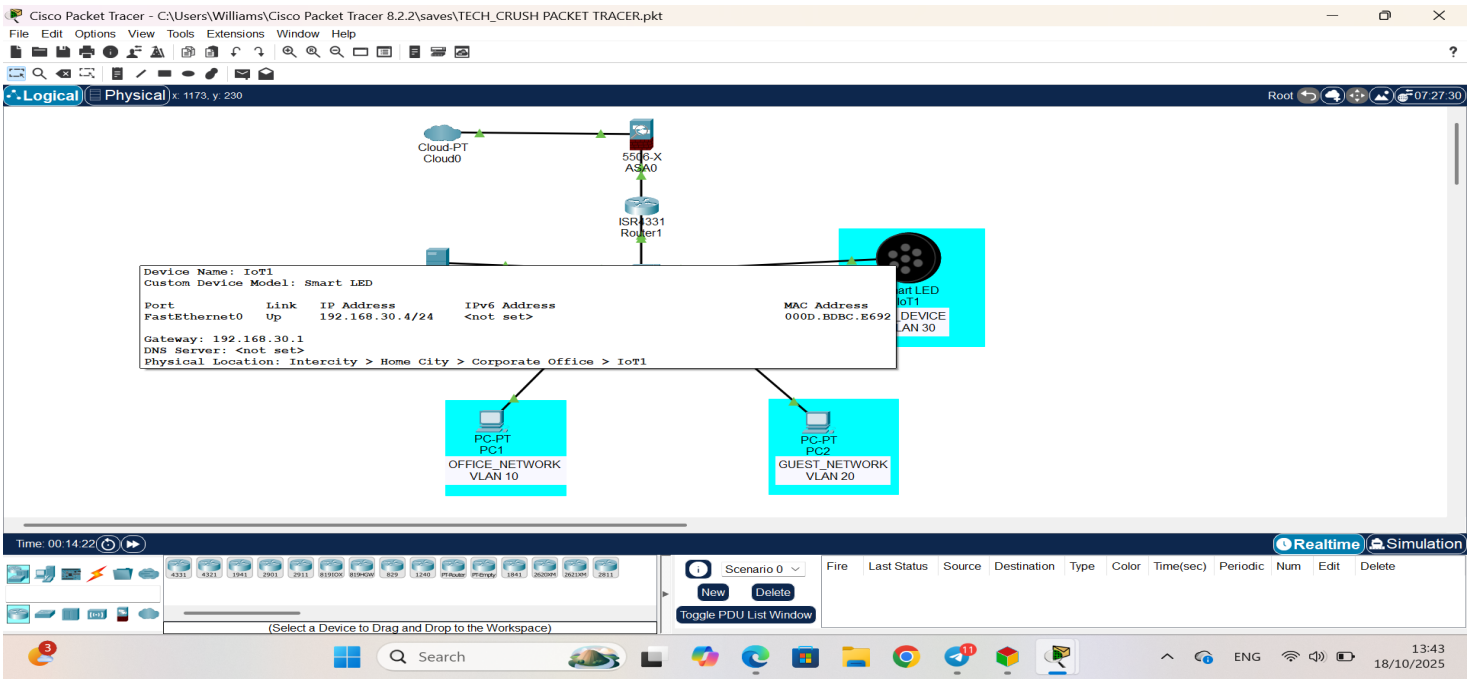
Server		192.168.10.1	255.255.255.0	Part of the Office VLAN
Office PC		192.168.10.1	255.255.255.0	Part of the Office VLAN
Guest PC		192.168.20.1	255.255.255.0	Part of the Guest VLAN
IoT		192.168.30.1	255.255.255.0	Part of the IoT VLAN

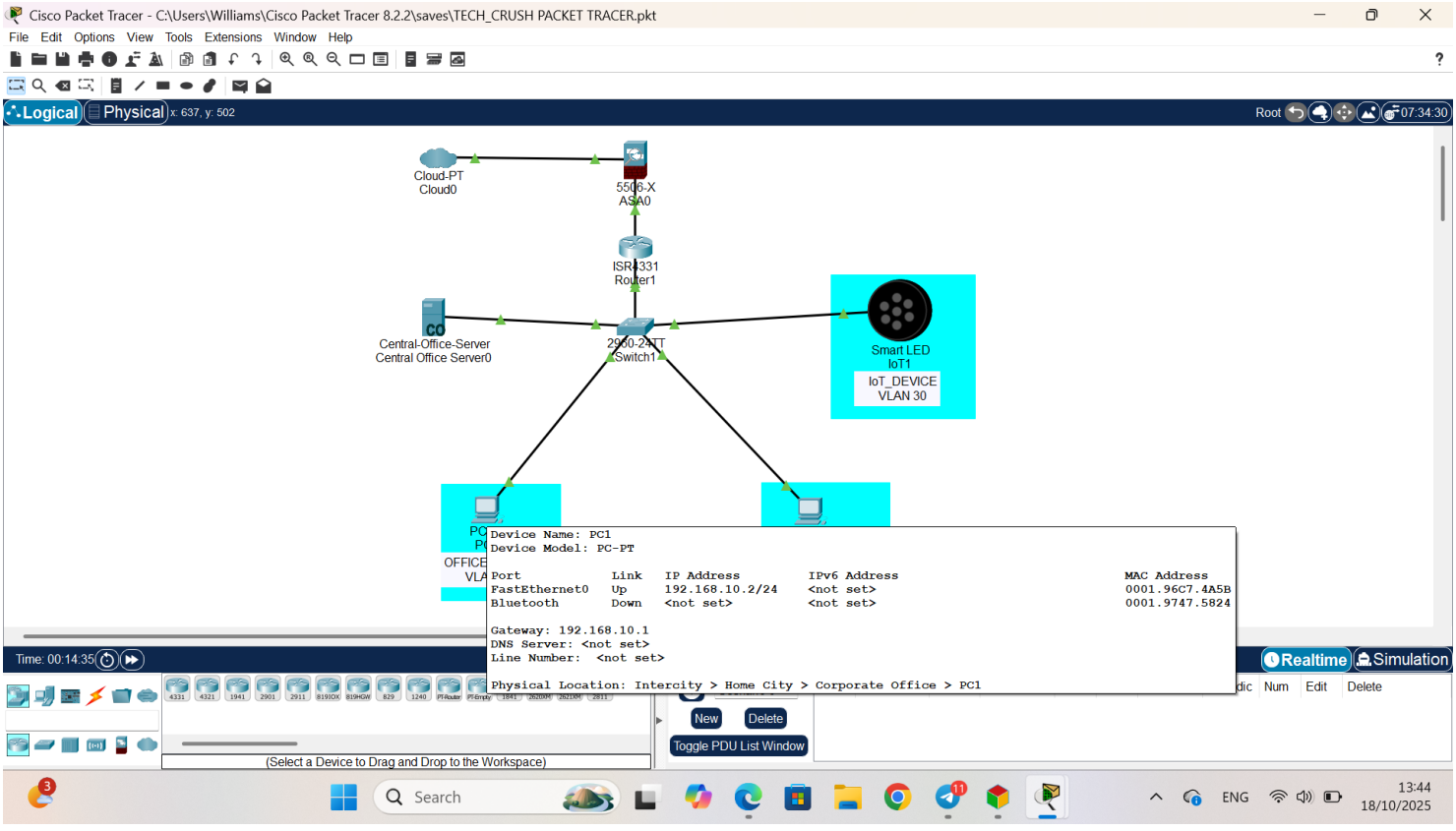
CHECK:

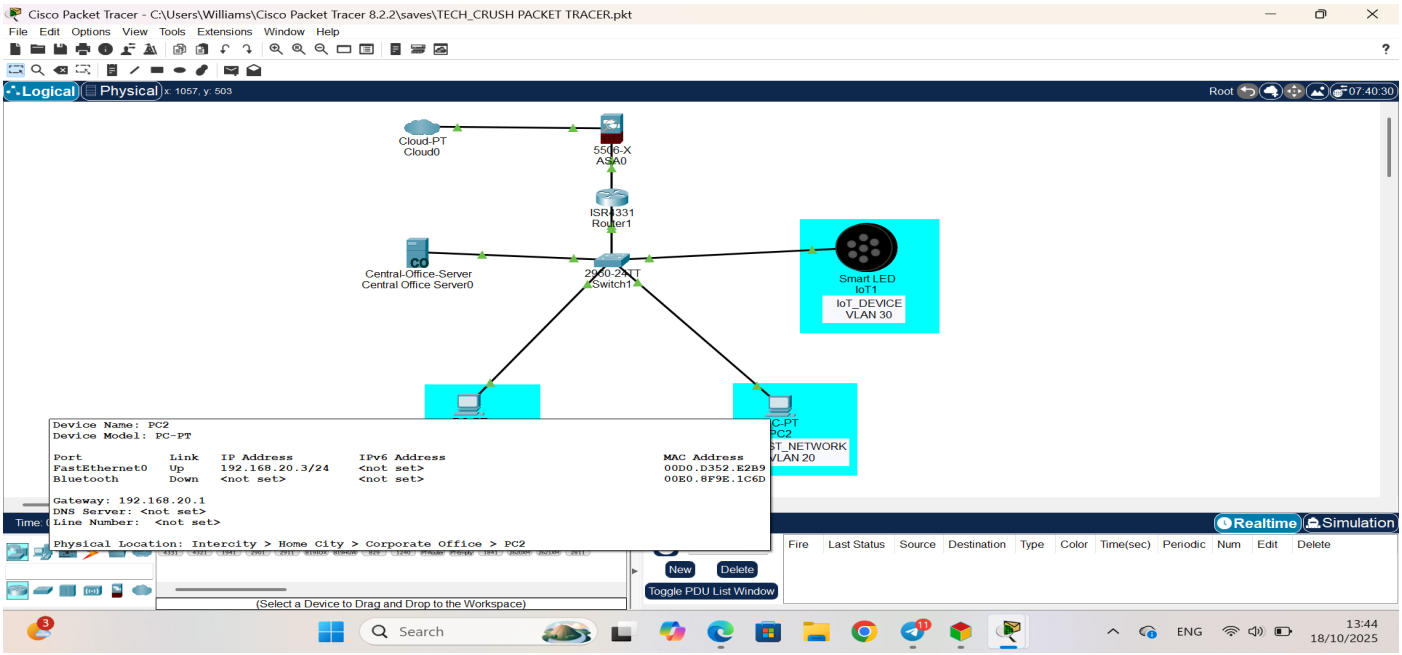



Cisco Packet Tracer - C:\Users\Williams\Cisco Packet Tracer 8.2.2\saves\TECH_CRUSH PACKET TRACER.pkt
File Edit Options View Tools Extensions Window Help
Logical Physical x: 839, y: 157
Root 07:04:00
Cloud-PT
Cloud0
5506-X
ASA0
Device Name: Router1
Device Model: ISR4331
Hostname: Router
Port Link VLAN IP Address IPv6 Address MAC Address
GigabitEthernet0/0/0 Up -- <not set> <not set> 000B.BE5D.6301
GigabitEthernet0/0/0.10 Up -- 192.168.10.1/24 <not set> 000B.BE5D.6301
GigabitEthernet0/0/0.20 Up -- 192.168.20.1/24 <not set> 000B.BE5D.6301
GigabitEthernet0/0/0.30 Up -- 192.168.30.1/24 <not set> 000B.BE5D.6301
GigabitEthernet0/0/0.40 Up -- <not set> <not set> 000B.BE5D.6301
GigabitEthernet0/0/1 Up -- <not set> <not set> 000B.BE5D.6302
GigabitEthernet0/0/2 Down -- <not set> <not set> 000B.BE5D.6303
Vlan1 Down 1 <not set> <not set> 0001.63B1.076E
Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Router1
PC-PT
PC1
OFFICE_NETWORK
VLAN 10
PC-PT
PC2
GUEST_NETWORK
VLAN 20
Time: 00:13:37
Realtime Simulation
(Select a Device to Drag and Drop to the Workspace)
Scenario 0
New
Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit Delete
Search
ENG
13:43
18/10/2025


Cisco Packet Tracer - C:\Users\Williams\Cisco Packet Tracer 8.2.2\saves\TECH_CRUSH PACKET TRACER.pkt
File Edit Options View Tools Extensions Window Help
Logical Physical x: 569, y: 252
Root 07:12:00
Cloud-PT
Cloud0
5506-X
ASA0
ISR4331
Router1
Central-Off
Central Offi
Device Name: Central Office Server0
Device Model: Central-Office-Server
Port Link IP Address IPv6 Address MAC Address
Backbone Up 192.168.10.5/24 <not set> 00D0.BCE6.3A01
Virtual-Access1 Up <not set> <not set> 000C.85C0.7E6C
Cellular Up 172.16.1.1/16 <not set> 0090.0CB0.691C
Coaxial0/0 Down -- 00D0.BCE6.3A02
Coaxial0/1 Down -- 00D0.BCE6.3A03
Coaxial0/2 Down -- 00D0.BCE6.3A04
Coaxial0/3 Down -- 00D0.BCE6.3A05
Coaxial0/4 Down -- 00D0.BCE6.3A06
Coaxial0/5 Down -- 00D0.BCE6.3A07
Cellular0/0 Up -- 00D0.BCE6.3A08
Physical Location: Intercity > Home City > Corporate Office > Central Office Server0
OFFICE_NETWORK
VLAN 10
GUEST_NETWORK
VLAN 20
Time: 00:13:53
Realtime Simulation
(Select a Device to Drag and Drop to the Workspace)
Scenario 0
New
Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit Delete
Search
ENG
13:43
18/10/2025


Cisco Packet Tracer - C:\Users\Williams\Cisco Packet Tracer 8.2.2\saves\TECH_CRUSH PACKET TRACER.pkt
File Edit Options View Tools Extensions Window Help
Logical Physical x: 1173, y: 230
Root 07:27:30
Cloud-PT Cloud0
5506-X ASA0
ISR4331 Router1
Device Name: IoT1
Custom Device Model: Smart LED
Port Link IP Address IPv6 Address MAC Address
FastEthernet0 Up 192.168.30.4/24 <not set> 000D.BDBC.E692
Gateway: 192.168.30.1
DNS Server: <not set>
Physical Location: Intercity > Home City > Corporate Office > IoT1
PC-PT PC1
OFFICE_NETWORK VLAN 10
PC-PT PC2
GUEST_NETWORK VLAN 20
Time: 00:14:22
Realtime Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit Delete
(Select a Device to Drag and Drop to the Workspace)
Search
ENG
13:43
18/10/2025


Cisco Packet Tracer - C:\Users\Williams\Cisco Packet Tracer 8.2.2\saves\TECH_CRUSH PACKET TRACER.pkt
File Edit Options View Tools Extensions Window Help
Logical Physical x: 637, y: 502
Root 07:34:30
Cloud-PT Cloud0
5506-X ASA0
ISR4331 Router1
Central-Office-Server Central Office Server0
2960-24TT Switch1
Smart LED IoT1
IoT_DEVICE VLAN 30
Device Name: PC1
Device Model: PC-PT
Port Link IP Address IPv6 Address MAC Address
FastEthernet0 Up 192.168.10.2/24 <not set> 0001.96C7.4A5B
Bluetooth Down <not set> <not set> 0001.9747.5824
Gateway: 192.168.10.1
DNS Server: <not set>
Line Number: <not set>
Physical Location: Intercity > Home City > Corporate Office > PC1
Time: 00:14:35
Realtime Simulation
New
Delete
Toggle PDU List Window
(Select a Device to Drag and Drop to the Workspace)
Search
ENG
13:44
18/10/2025

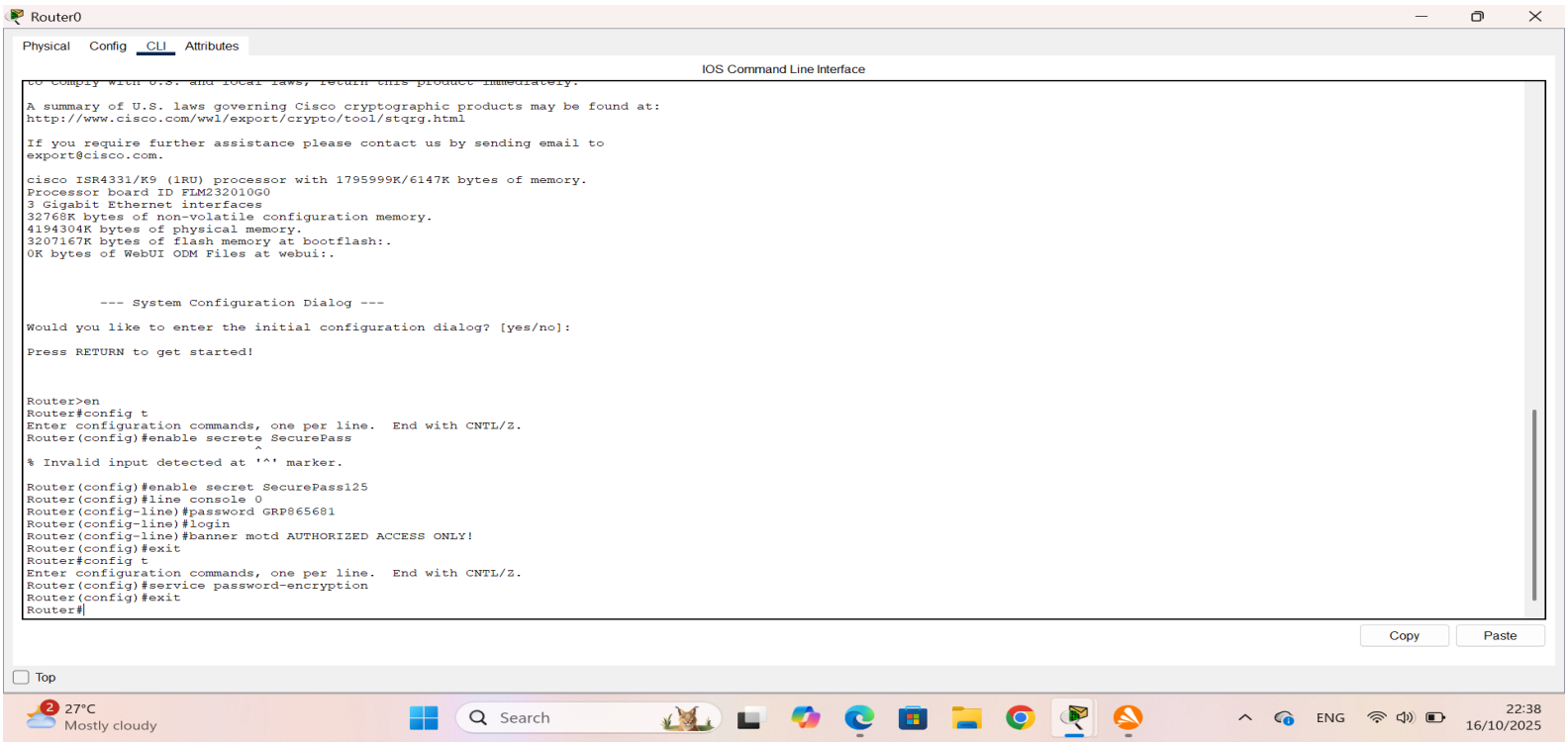


5. BASIC NETWORK SEGMENTATION USING VLANs

In this section, we configured the switch to perform two main roles within our network environment:

- to create separate VLANs for the Office and Guest networks, and
- to assign IP addresses to each VLAN interface for remote management purposes. This process allowed us to divide the network logically, increase security, and enable easier administration.

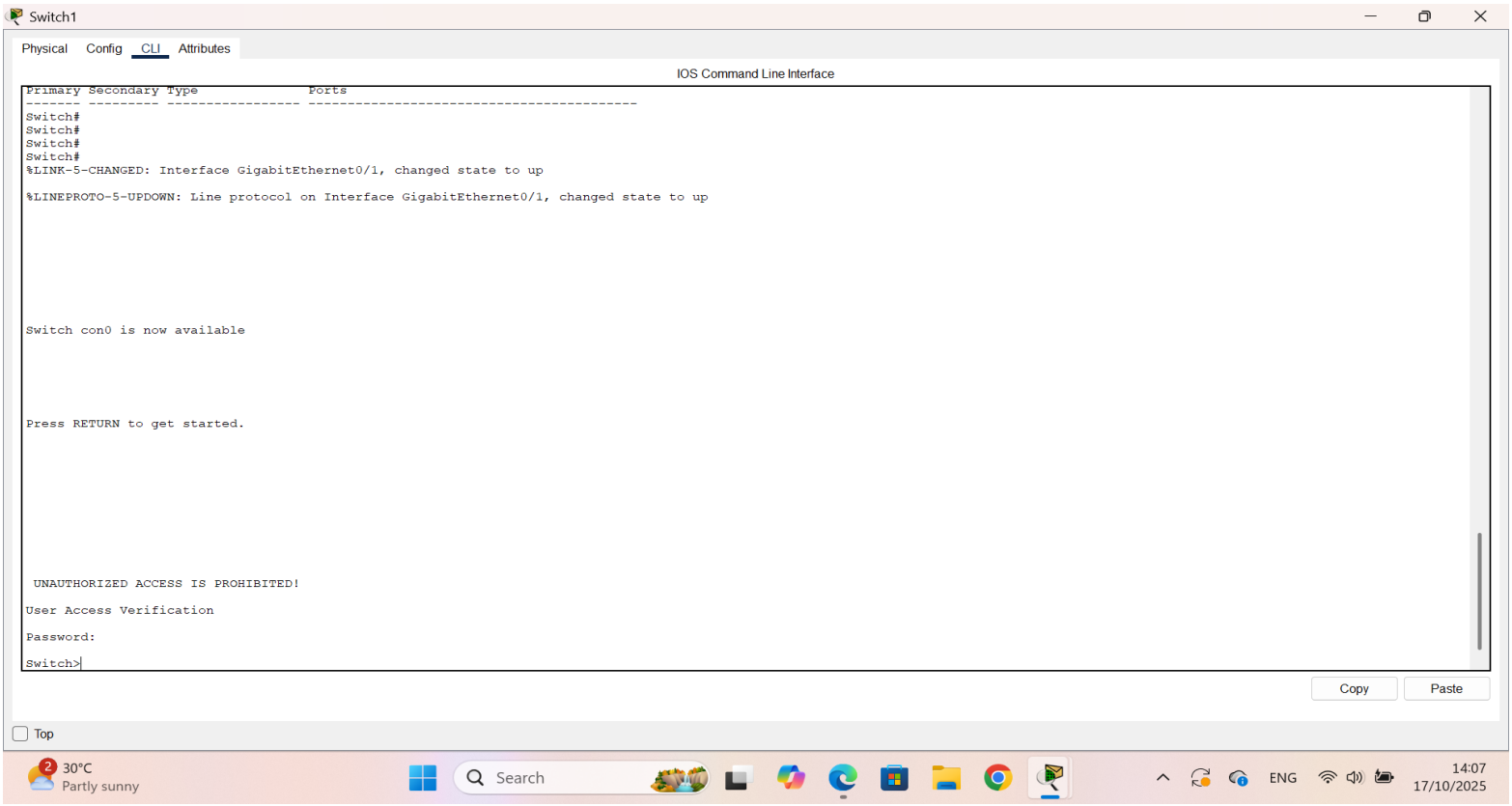
Firstly, we have to assign password to the Switch for confidentiality. Hence. Only authorized users can access the switch.



5.1 Explanation of Each Command

- **Enable secret SecurePass123:** We set a strong secret password for privileged EXEC mode, which protects high-level administrative commands. Unlike the regular "enable password," the "enable secret" is stored in an encrypted form, making it more secure.
- **Line console 0 / password RouterAccess1 / login:** We configured a password for the console line, which is the physical port used when directly connecting to the router with a console cable. This ensures that anyone trying to access the router locally must provide a valid password.
- **Line vty 0 4 / password RemoteLogin1 / login:** We configured remote (virtual terminal) access passwords for Telnet or SSH sessions. This allows administrators to manage the router remotely while ensuring that unauthorized users cannot connect.
- **Service password-encryption:** We enabled encryption for all stored passwords so they appear scrambled when viewed in the configuration file. This is an important security practice in real networks to prevent anyone from easily reading passwords.
- **Write memory:** We saved the running configuration to the startup configuration so that our settings are preserved after.

CHECK:



Why This Configuration Matters

In any real-world small or medium-sized business network, routers often store critical settings such as IP routes, firewall rules, and access control lists. If an attacker gains access to a router, they could reroute or intercept sensitive data. By setting strong passwords and encrypting them, we prevented unauthorized access and protected the device from insider misuse or external attacks. For example, in an office environment, if a staff member connects to the router console without permission, they will be unable to make any configuration changes without the proper credentials. This simple but essential layer of security significantly reduces the risk of accidental or malicious tampering. Real-World Application In practical business networks, these same steps are applied to every router and switch before deployment. Network administrators typically use unique, complex passwords for each device and store them securely. They also combine password protection with other controls such as SSH (Secure Shell) for encrypted remote management and AAA (Authentication, Authorization, and Accounting) servers for centralized user control. In this project, while we used simple passwords for demonstration, the structure and logic mirror exactly how network devices are protected in real-world corporate setups.

5.1 Creating VLAN Interfaces and Assigning IP Addresses

We began by accessing the firewall through the console interface and entered privileged mode and global configuration mode. We then created and configured two VLAN interfaces:

- **VLAN 10 (Inside Network):** representing the internal, trusted zone or network. And has full access to most resources including Server, IoT and other Workstations.
- **VLAN 20 (Outside Network):** representing the external, untrusted zone. Has restricted access, can only use the internet but cannot access the Office systems or Servers.
- **VLAN 30 (Outside Network) :** Represents Internet of Things (IoT) devices like Smart LED, cameras. This is separated to prevent IoT vulnerabilities from affecting other networks.

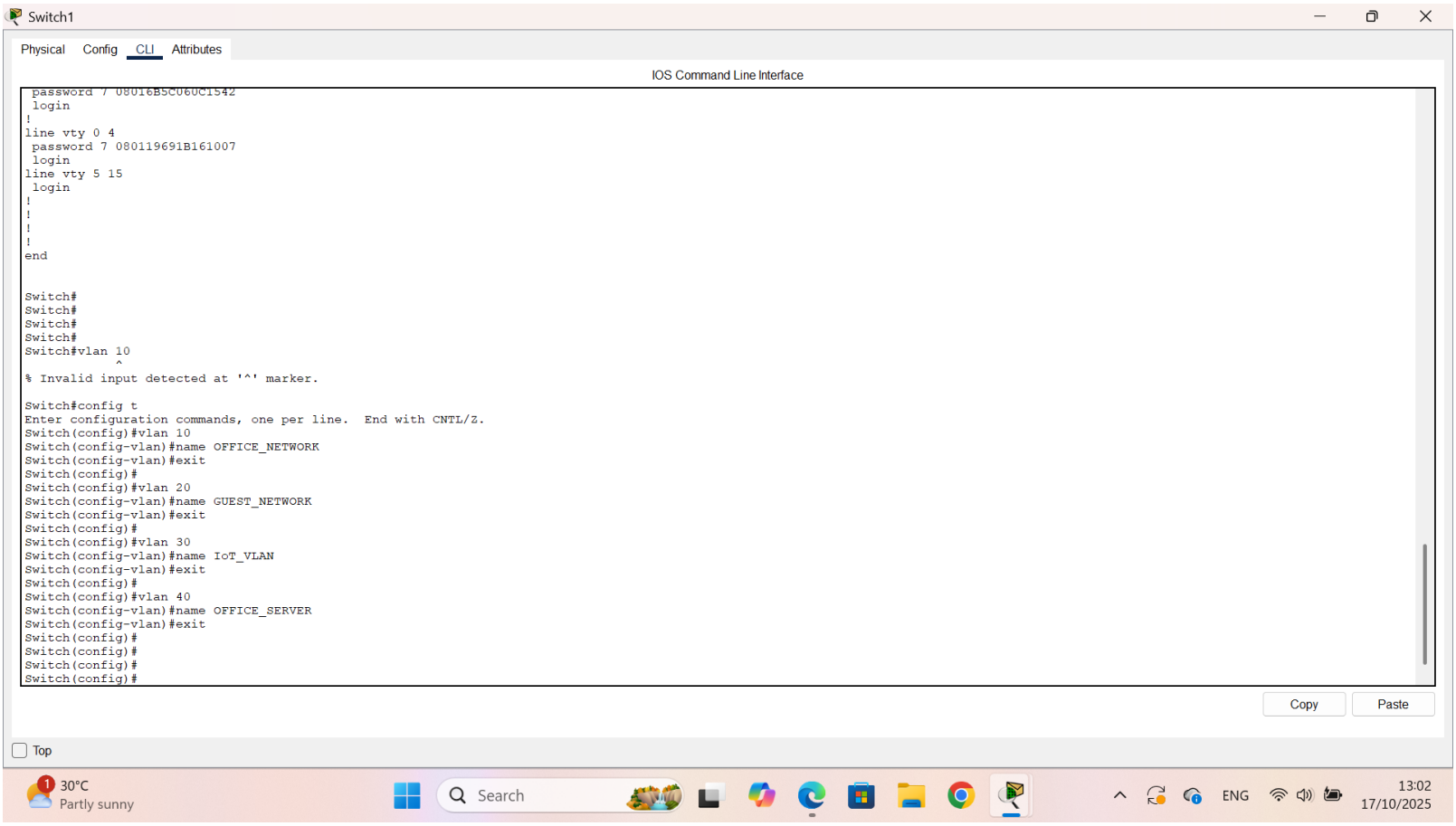
For each VLAN, we assigned a name, an IP address, and a security level. The security level defines the level of trust. 100 means fully trusted (inside), and 0 means untrusted (outside). This concept ensures that traffic from a higher security level can go to a lower level by default, but not vice versa, unless specifically allowed by security rules.

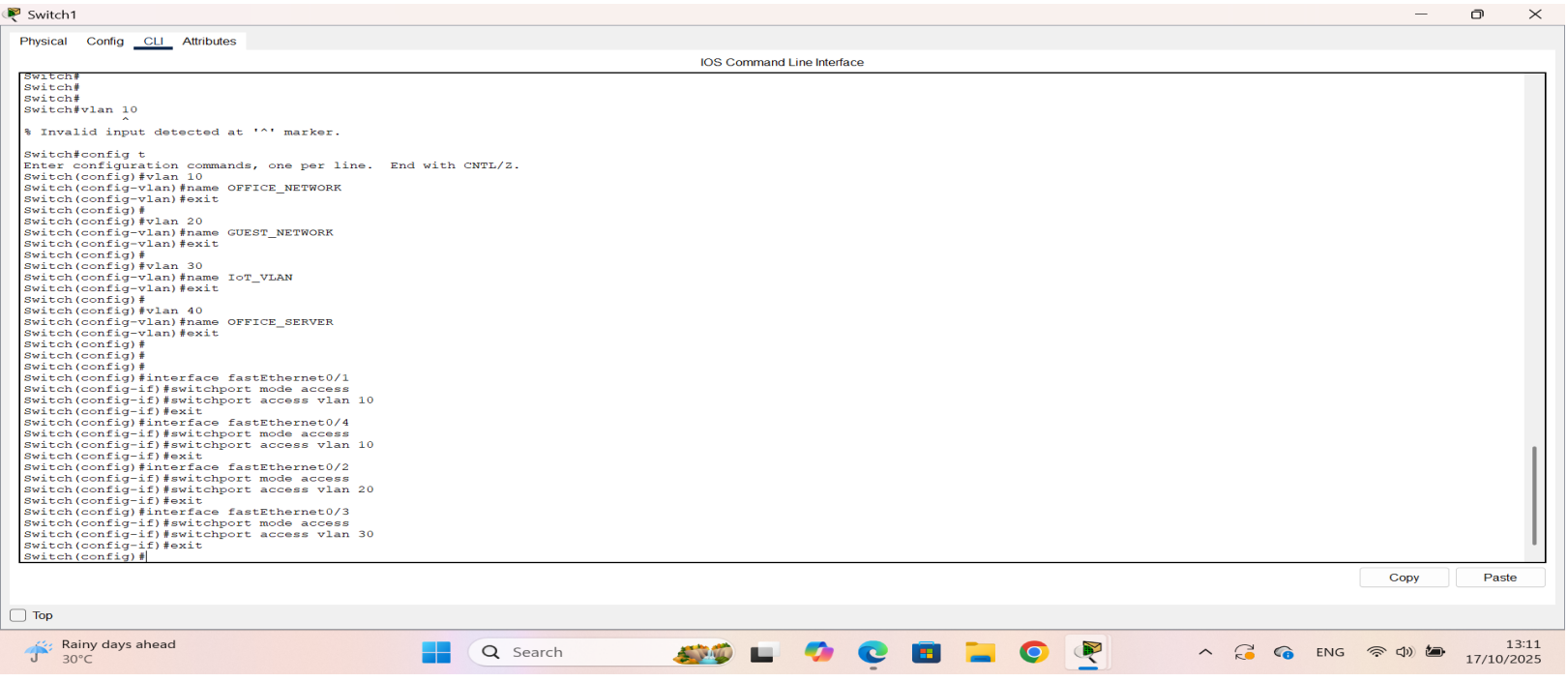
Creating VLANs and Assigning Ports

We began by accessing the switch through the console connection. After entering privileged mode, we moved into the global configuration mode. From there, we created three VLANs: VLAN 10, VLAN 20, VLAN 30 and VLAN 40 and assigned them descriptive names to identify their purposes clearly.

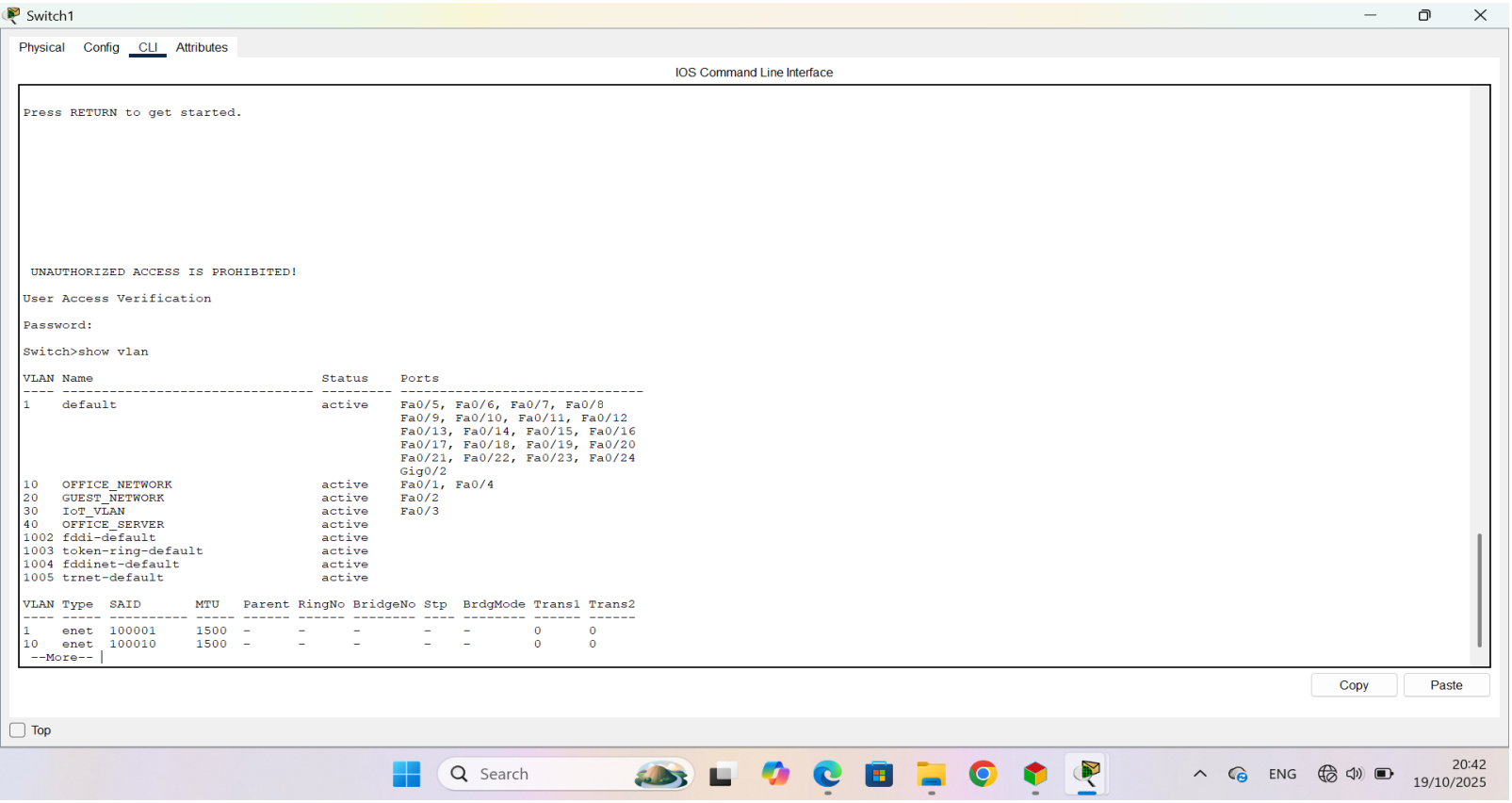
VLAN 10 was named **Office_Network**, VLAN 20 was named **Guest_Network ,** VLAN 30 was name **IoT_Device** and VLAN 40 **Office_Server**. These VLANs represent two separate network zones: one for internal office devices, the other for guest users and the last one for the Smart LED device (IoT).

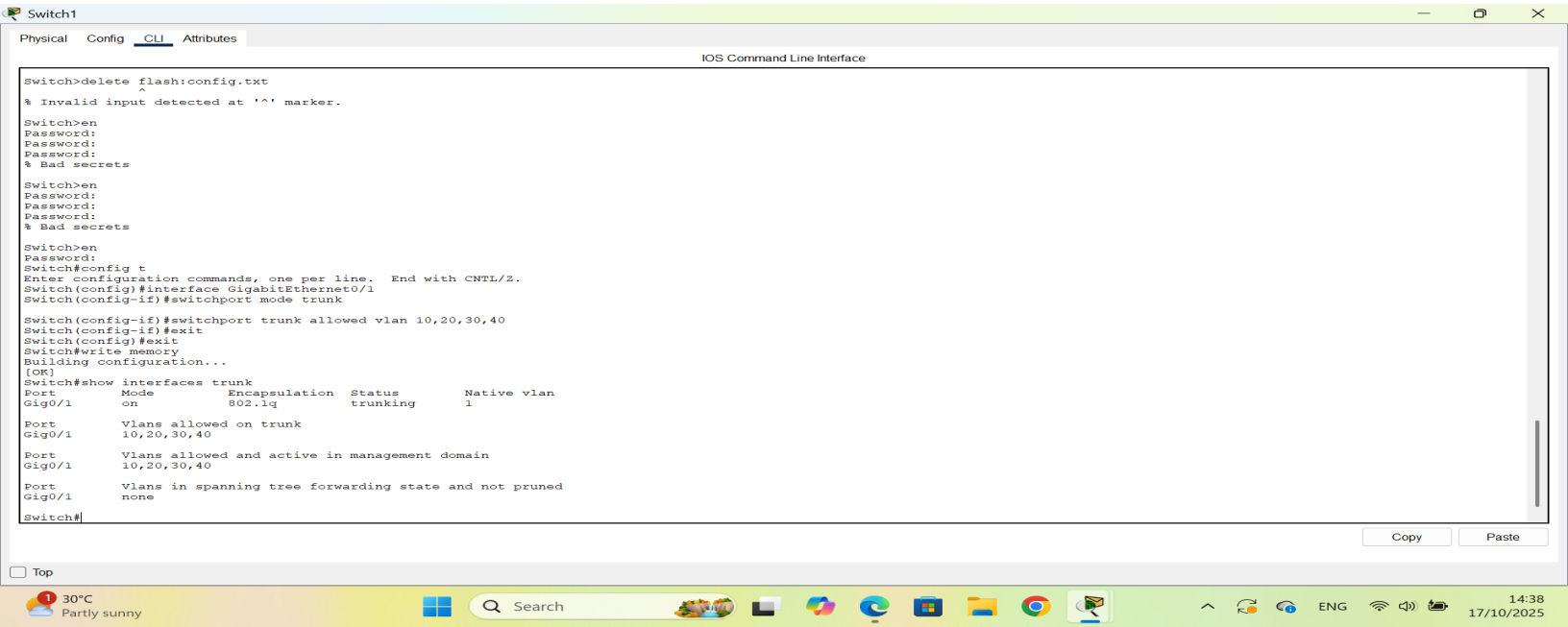
After creating the VLANs, we assigned specific physical ports to each VLAN. Ports FastEthernet0/1 and FastEthernet0/4 were connected to the **Office PC** and Server, so we assigned them to VLAN 10. Port FastEthernet0/2, connected to the **Guest PC**, was assigned to VLAN 20. Port FastEthernet0/3, connected to the **IoT Device**, was assigned to VLAN 30. Port FastEthernet0/4, connected to the **Office_Server**, was assigned to VLAN 40 Below are the commands we applied to the switch:


Switch1
Physical
Config
CLI
Attributes
IOS Command Line Interface
password 7 08016B5C060C1542
login
!
line vty 0 4
password 7 080119691B161007
login
line vty 5 15
login
!
!
!
!
end
Switch#
Switch#
Switch#
Switch#
Switch#vlan 10
^
% Invalid input detected at '^' marker.
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name OFFICE_NETWORK
Switch(config-vlan)#exit
Switch(config)#
Switch(config)#vlan 20
Switch(config-vlan)#name GUEST_NETWORK
Switch(config-vlan)#exit
Switch(config)#
Switch(config)#vlan 30
Switch(config-vlan)#name IoT_VLAN
Switch(config-vlan)#exit
Switch(config)#
Switch(config)#vlan 40
Switch(config-vlan)#name OFFICE_SERVER
Switch(config-vlan)#exit
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#
Copy
Paste
Top
30°C
Partly sunny
Search
ENG
13:02
17/10/2025


Switch1
Physical
Config
CLI
Attributes
IOS Command Line Interface
Switch#
Switch#
Switch#
Switch#vlan 10
^
% Invalid input detected at '^' marker.
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name OFFICE_NETWORK
Switch(config-vlan)#exit
Switch(config)#
Switch(config)#vlan 20
Switch(config-vlan)#name GUEST_NETWORK
Switch(config-vlan)#exit
Switch(config)#
Switch(config)#vlan 30
Switch(config-vlan)#name IoT_VLAN
Switch(config-vlan)#exit
Switch(config)#
Switch(config)#vlan 40
Switch(config-vlan)#name OFFICE_SERVER
Switch(config-vlan)#exit
Switch(config)#
Switch(config)#
Switch(config)#
Switch(config)#interface fastEthernet0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#interface fastEthernet0/4
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#interface fastEthernet0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#exit
Switch(config)#interface fastEthernet0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 30
Switch(config-if)#exit
Switch(config)#
Copy
Paste
Top
Rainy days ahead
30°C
Search
ENG
13:11
17/10/2025

Show VLANs:


Switch1
Physical
Config
CLI
Attributes
IOS Command Line Interface
Press RETURN to get started.
UNAUTHORIZED ACCESS IS PROHIBITED!
User Access Verification
Password:
Switch>show vlan
VLAN Name Status Ports
1 default active Fa0/5, Fa0/6, Fa0/7, Fa0/8
Fa0/9, Fa0/10, Fa0/11, Fa0/12
Fa0/13, Fa0/14, Fa0/15, Fa0/16
Fa0/17, Fa0/18, Fa0/19, Fa0/20
Fa0/21, Fa0/22, Fa0/23, Fa0/24
Gig0/2
10 OFFICE_NETWORK active Fa0/1, Fa0/4
20 GUEST_NETWORK active Fa0/2
30 IoT_VLAN active Fa0/3
40 OFFICE_SERVER active
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active
VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
1 enet 100001 1500 - - - - - 0 0
10 enet 100010 1500 - - - - - 0 0
--More--
Copy
Paste
Top
Search
ENG
20:42
19/10/2025


Switch1
Physical
Config
CLI
Attributes
IOS Command Line Interface
Switch>delete flash:config.txt
^
% Invalid input detected at '^' marker.
Switch>en
Password:
Password:
Password:
% Bad secrets
Switch>en
Password:
Password:
Password:
% Bad secrets
Switch>en
Password:
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface GigabitEthernet0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 10,20,30,40
Switch(config-if)#exit
Switch(config)#exit
Switch#write memory
Building configuration...
[OK]
Switch#show interfaces trunk
Port Mode Encapsulation Status Native vlan
Gig0/1 on 802.1q trunking 1
Port Vlans allowed on trunk
Gig0/1 10,20,30,40
Port Vlans allowed and active in management domain
Gig0/1 10,20,30,40
Port Vlans in spanning tree forwarding state and not pruned
Gig0/1 none
Switch#
Copy
Paste
Top
30°C
Partly sunny
Search
ENG
14:38
17/10/2025

Trunking is a method used on network Switches to carry traffic for multiple VLANs over a single physical link between Switches,Routers, or other devices.

We carried this command so that all the VLANs can communicate through one connection GigabitEthernet0/1.

By completing this step, we successfully separated the office and guest devices into two distinct VLANs. This logical separation prevents unauthorized communication between the Guest PC and the Office devices, thereby strengthening network security.

5.2 Assigning Management IP Addresses to VLAN Interfaces

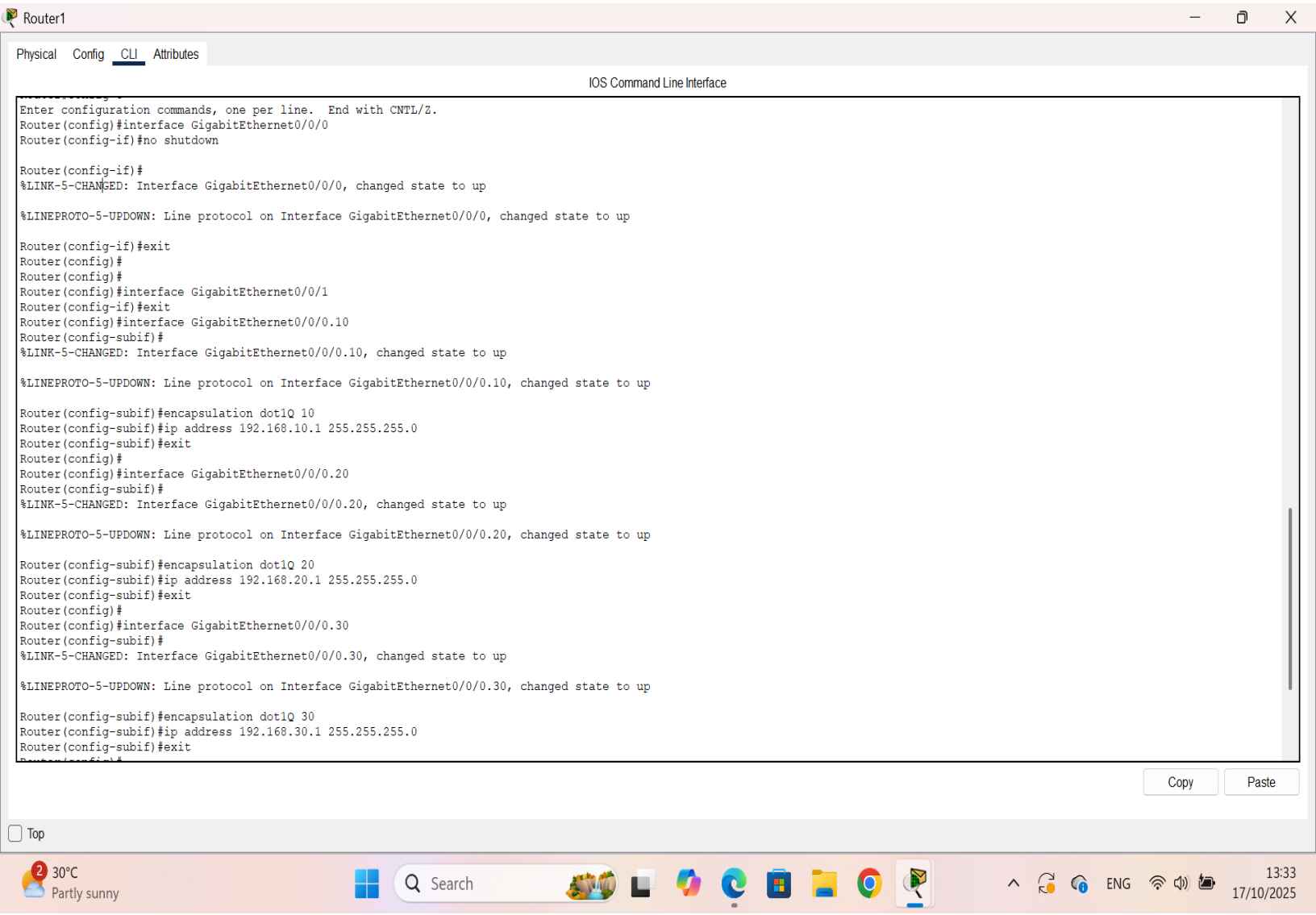
After creating the VLANs, we configured each VLAN with an IP address to enable network management and monitoring. We assigned IP addresses directly to the VLAN interfaces, rather than to physical ports, because VLAN interfaces act as the logical gateways for each segment. We assigned:

- 1. 192.168.10.2/24 to VLAN 10 (Office Network)
- 192.168.20.3/24 to VLAN 20 (Guest Network)
- 192.168.30.4/24 to VLAN 30 (IoT Device)
- 192.168.10.5/24 to VLAN 40 (Server)

These IP addresses allow administrators to manage the switch remotely, using tools such as Telnet or SSH, while maintaining network segmentation.

The commands we used on the Router are as follows:

First we had to configure the password as we did on the Switch to the Router. Then, the following command bellow were carried out:

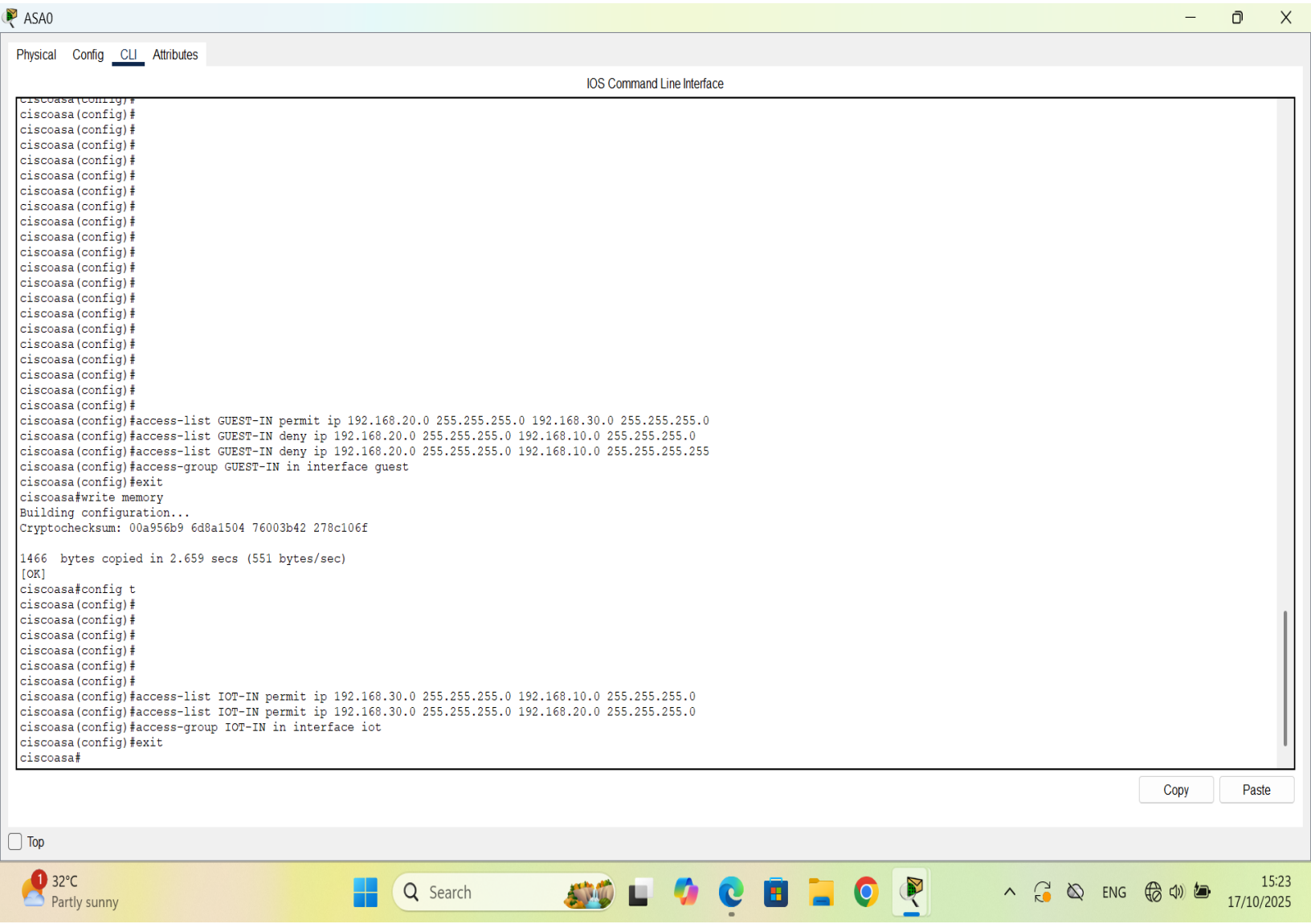


After entering these commands, both VLAN interfaces became active and ready for management traffic. The no shutdown command was essential because it activated each VLAN interface. Without it, the interface would remain in a shutdown (inactive) state.

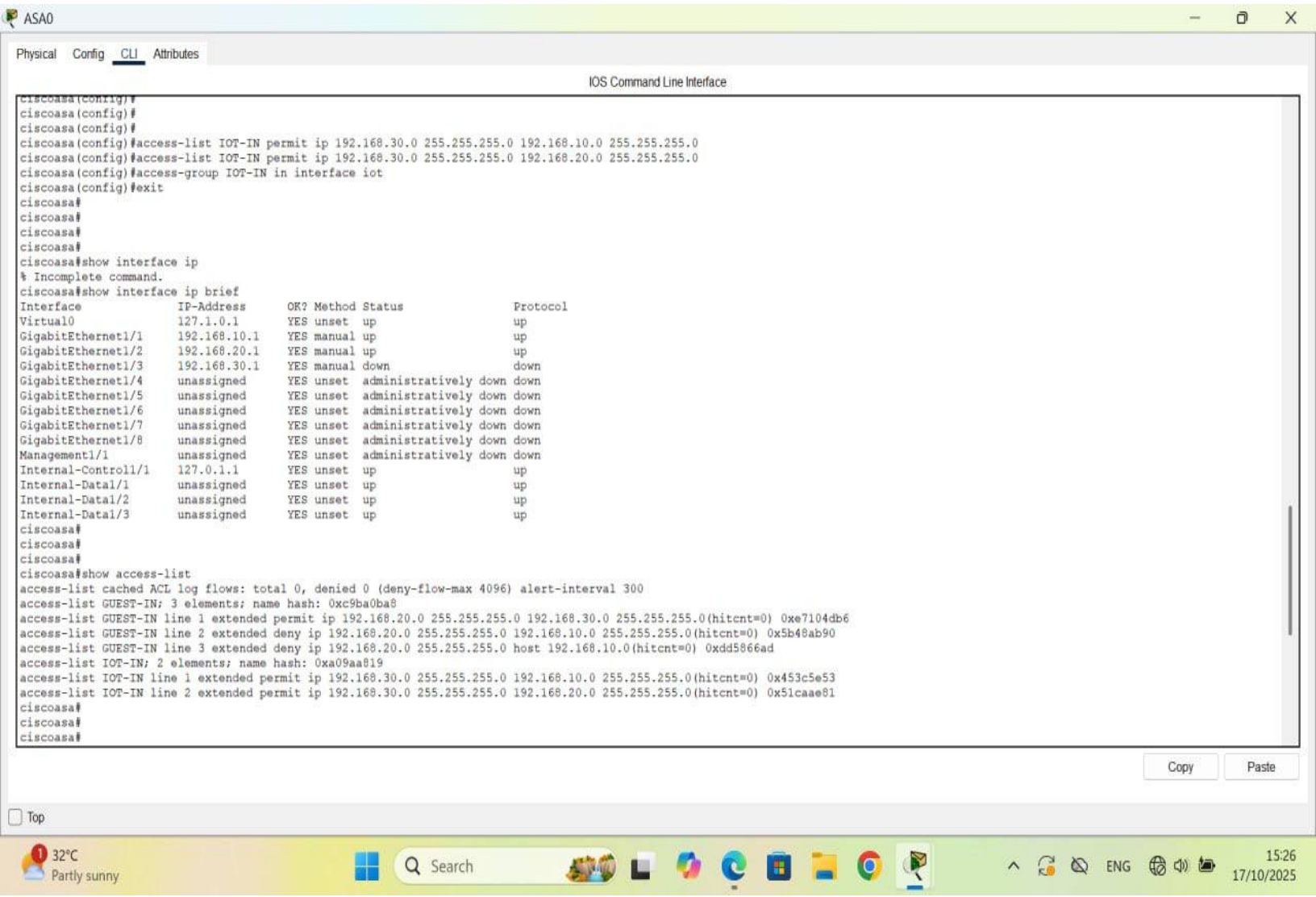
6. **Access Control**

We accessed the Firewall's command-line interface and entered privileged mode using the enable command, then moved into global configuration mode with configure terminal. We created an access control list (ACL) with ip access-list to enhance network security by first denying any IP traffic originating from the Guest Network (192.168.20.3) destined for the Office Network (192.168.10.2), and then allowing all other traffic with a general permit rule. After defining the ACL, we applied it inbound on interface GigabitEthernet1/1, which connects to the internal switch, using the ip access-group 110 in command. This setup ensured that any attempt by a guest device to reach the office network would be blocked, while legitimate Internet traffic would still

pass through. Finally, we exited configuration mode and saved the settings permanently using the write memory command.



Check:



Explanation:

- The first command blocks any traffic going from the Guest VLAN (192.168.20.3) to the Office VLAN (192.168.10.2).
- The second command allows all other traffic. This means guests can access the Internet but cannot access office computers or servers.
- We did not assign any access to the Office_Network. Hence by it has general access by default

6.2 Firewall Rules

In this part of our project, we configured the firewall to serve as a protective barrier between the trusted internal network and the untrusted external network (Internet). The firewall's main purpose in our design was to inspect, control, and filter traffic flowing in and out of the network to prevent unauthorized access and protect internal systems from external threats.

Understanding the Role of the Firewall

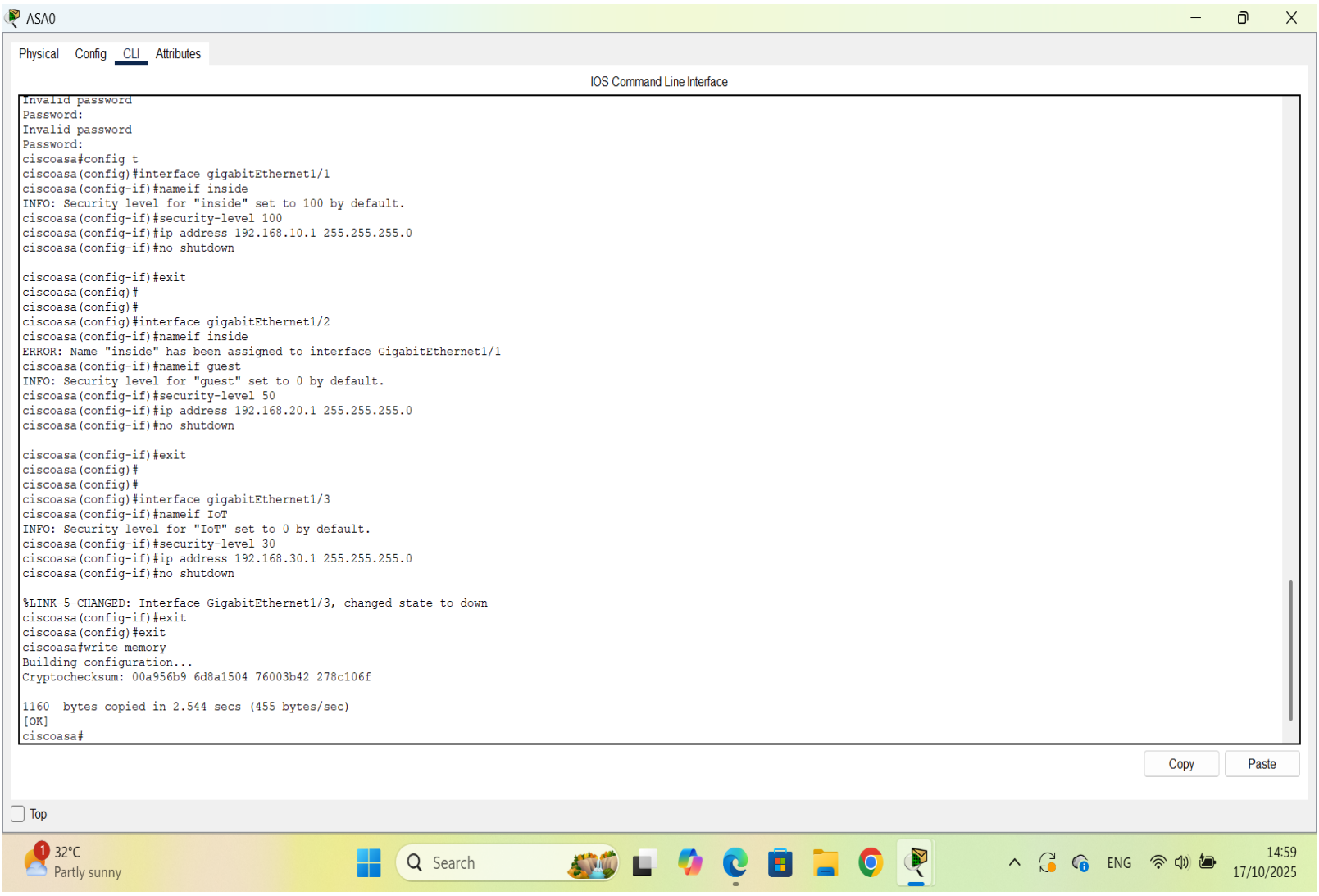
In any real-world organization, a firewall plays a critical role as the first line of defense between the internal private network (used by staff and office devices) and the external public Internet. The firewall ensures that only permitted traffic can pass through, based on security policies and defined 8 rules. In our setup, the firewall was placed between the router (internal side) and the cloud (external side), allowing it to filter packets and enforce access control.

Naming the Firewall and Configuring Physical Interfaces

We began by entering privileged mode using the en command and then moved into configuration mode with configure terminal. We set the hostname of the device to Firewall to make it easily identifiable in the network. Next, we configured the physical Ethernet interfaces. **We assigned:**

- GigabitEthernet1/1 to VLAN 10 (inside interface) for the trusted network.
- GigabitEthernet1/2 to VLAN 20 (outside interface) for the untrusted internal network(internet).
- GigabitEthernet1/3 to VLAN 30 (outside interface)

For each interface, we set it as an access port to the correct VLAN using the switchport access vlan command and activated the interfaces using no shutdown. This ensures that the physical interfaces are operational and correctly assigned to their respective VLANs.



Configuration for VLAN 10

- We set the security level to 100, marking it as fully trusted.
- We assigned the IP address 192.168.10.1/24 for the internal network.
- We named the interface outside using nameif inside.
- We activated the interface using no shutdown.

Configuration for VLAN 20

- We set the security level to 50, marking it as untrusted.
- We assigned the IP address 192.168.20.1/24 for the internal network.

- We named the interface outside using nameif Group.
- We activated the interface using no shutdown.

Configuration for VLAN 30

- We set the security level to 30, marking it as untrusted.
- We assigned the IP address 192.168.30.1/24 for the internal network.
- We named the interface outside using nameif IoT.
- We activated the interface using no shutdown.

6.3 Firewall Security Behavior

By default, the firewall allowed traffic from the Inside zone (security level 100) to reach the Outside zone (security level 0) but blocked all unsolicited traffic coming from the Outside to the Inside. This setup ensured that internal users could access the Internet safely, while external attackers could not directly reach the private network. In real-life networks, this is how organizations protect their systems from Internet-based threats. For example, employees inside a company can browse websites or send emails, but hackers from outside cannot initiate direct connections to internal computers unless permitted through specific firewall rules. This type of configuration also enables stateful packet inspection, which means the firewall keeps track of all active connections and only allows responses to legitimate, initiated requests. Real-World Application In real-world networks, this kind of firewall configuration is very common in small and medium-sized offices. For instance, the inside network would host business computers, servers, and printers, while the outside network would connect to an Internet Service Provider (ISP) through a public IP address. This structure ensures that while users can safely connect to external resources such as websites or cloud services, no external host can directly access or exploit the internal devices. Such protection is critical for preventing unauthorized access, malware infiltration, and data breaches.

7. **Simulation Steps**

To simulate this threat, we followed these steps in Cisco Packet Tracer:

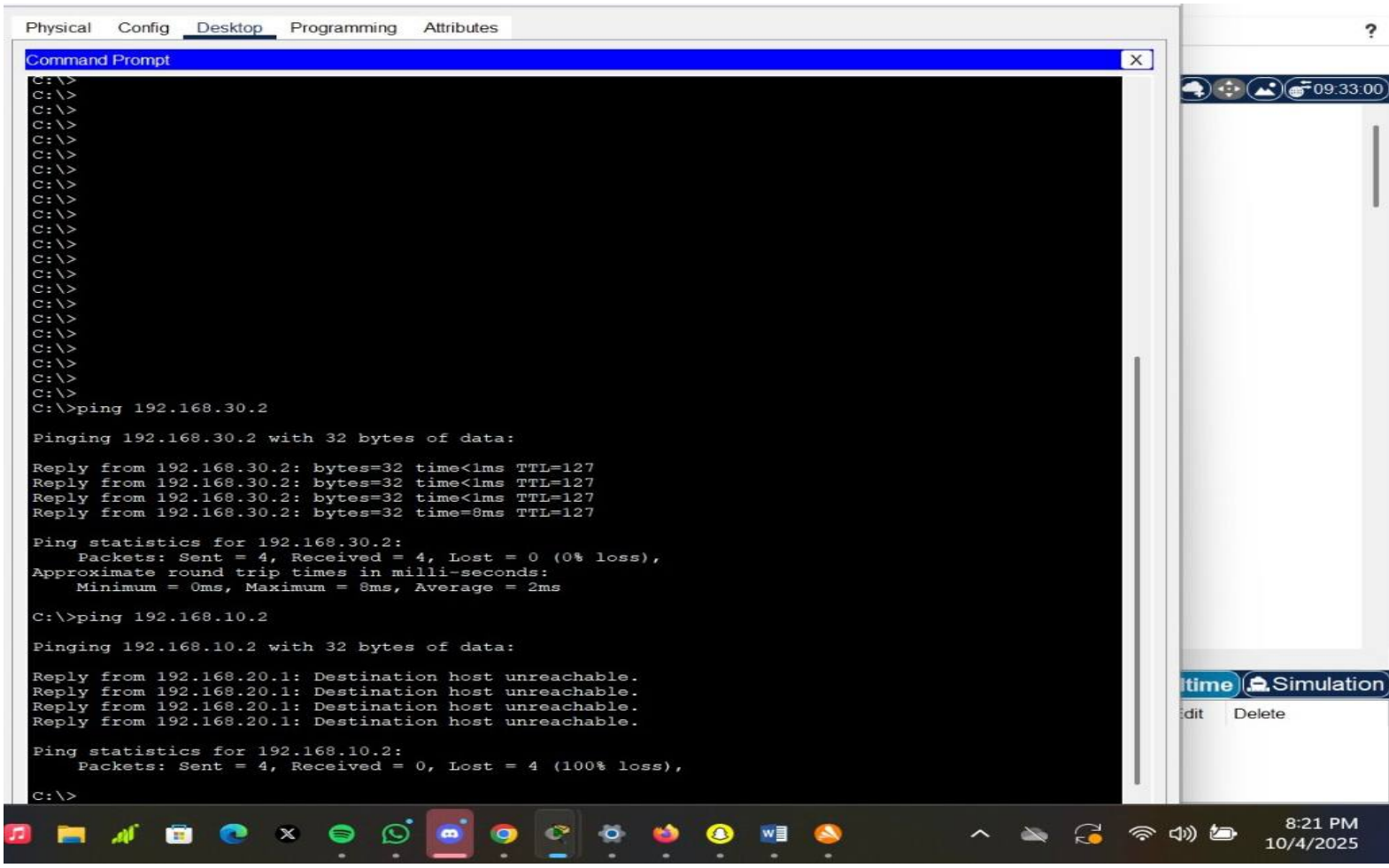
- We selected the Guest PC in the simulation and opened the command prompt.
- We typed the command:

  ping 192.168.10.20

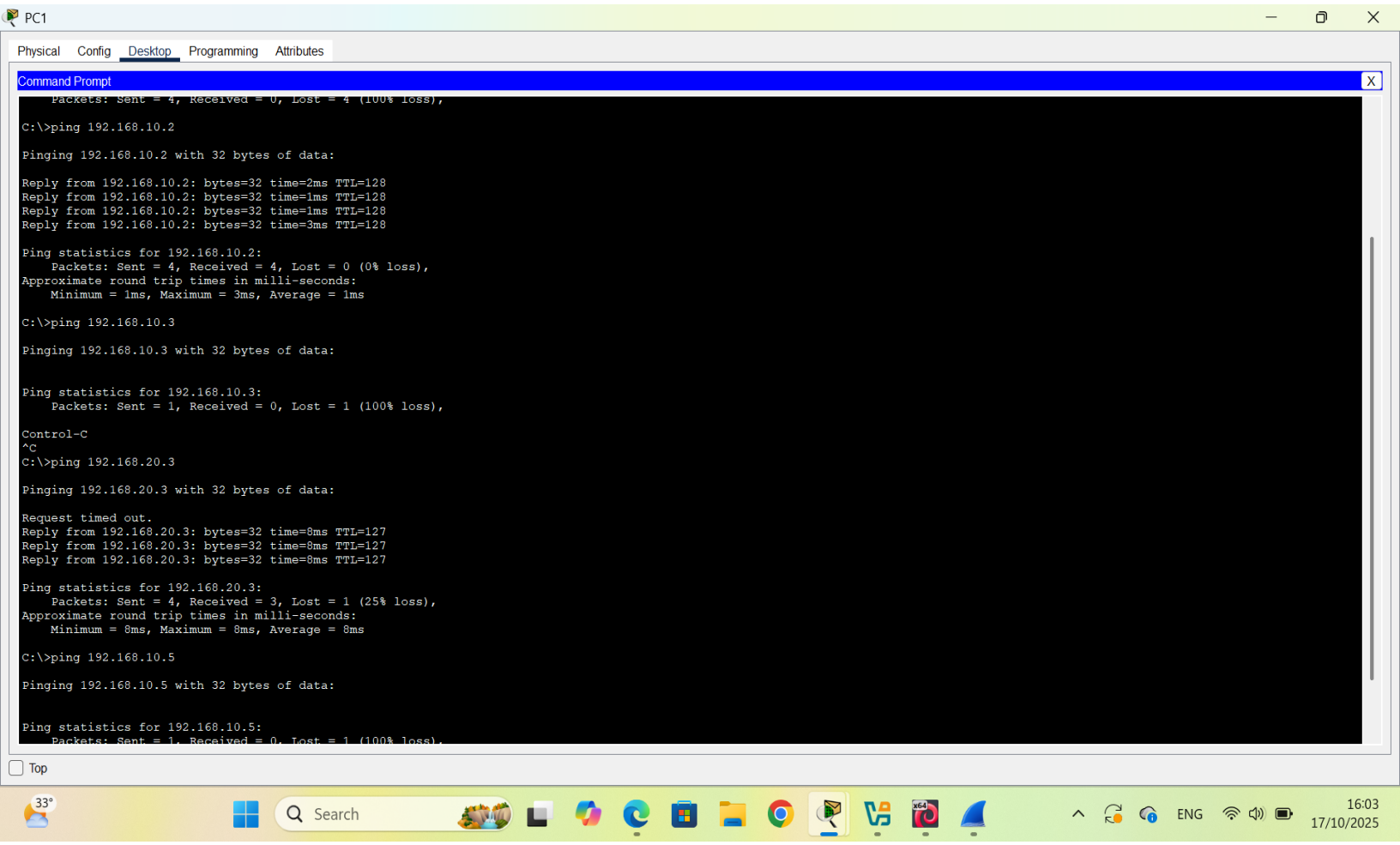
  We observed the response.
- The ping should fail, showing “Destination Unreachable,” because the access control list (ACL) configured on the Firewall and Router blocks traffic from the Guest VLAN to the Office VLAN.
- We confirmed that while the Guest PC cannot access the Office Server, it can still reach the Internet. This shows that our firewall and ACL rules allow legitimate external communication but prevent unauthorized internal access.

Guest PC command prompt showing “Destination Unreachable” when trying to ping the Office

Server.



Check for PC1 (Office_Network)



It was observed it was able to ping all Networks in respect to the default access granted.

8. Port Scanning using Nmap

Nmap was used to identify open ports and services across the network devices.
The goal was to detect and harden unnecessary open ports (e.g., port 22 for SSH).

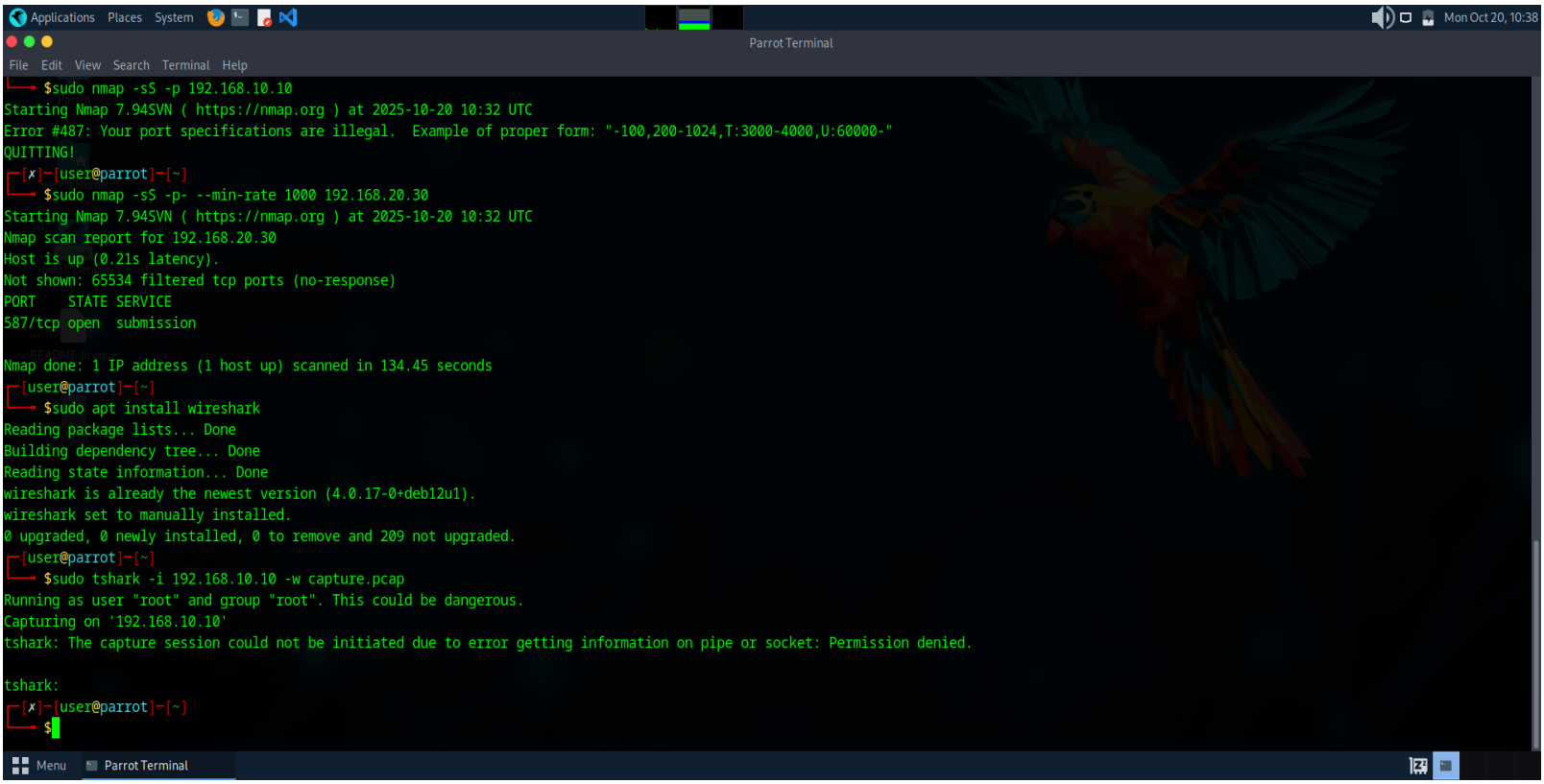
Using the Parrot OS we prompted the following command:
sudo apt update && sudo apt upgrade

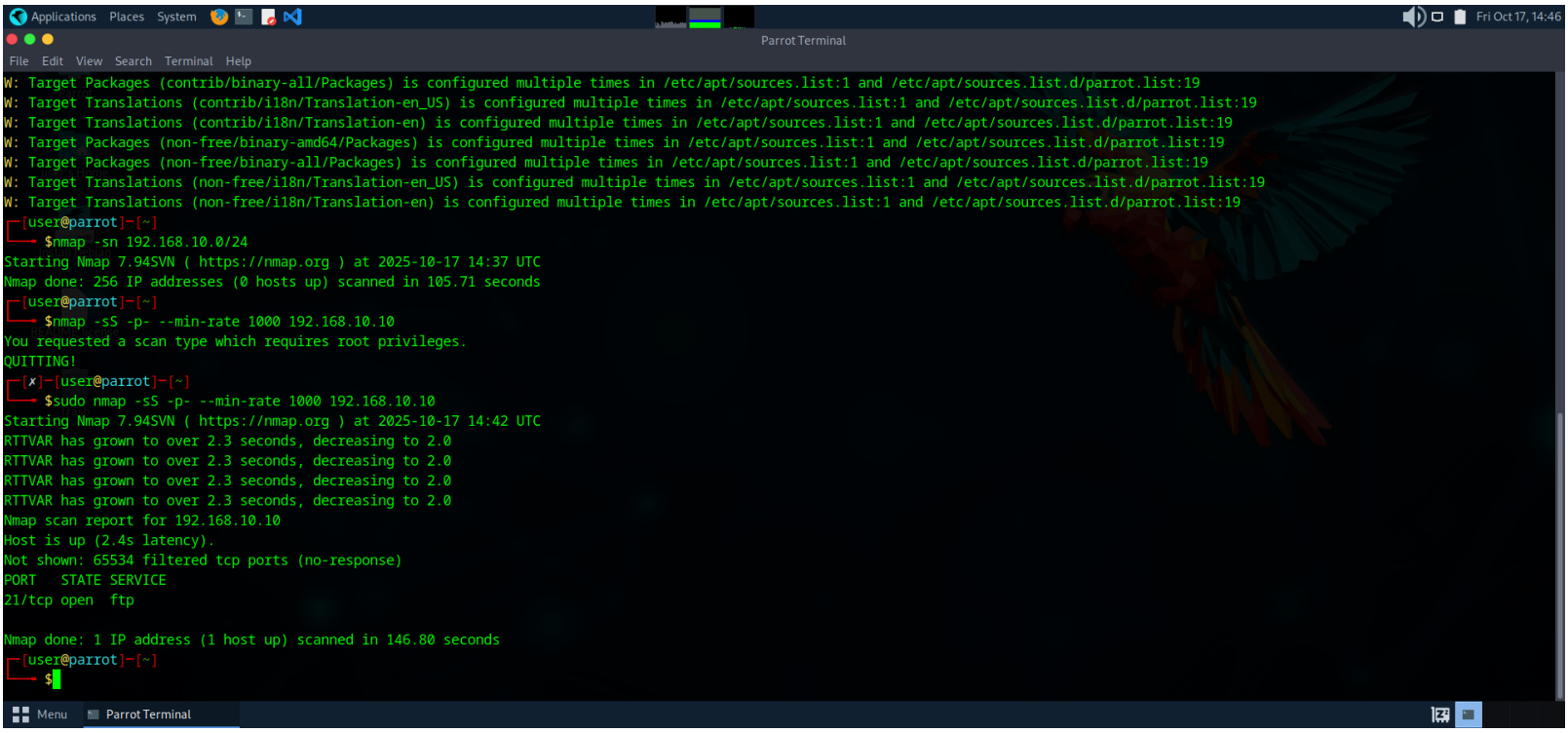
sudo apt install nmap

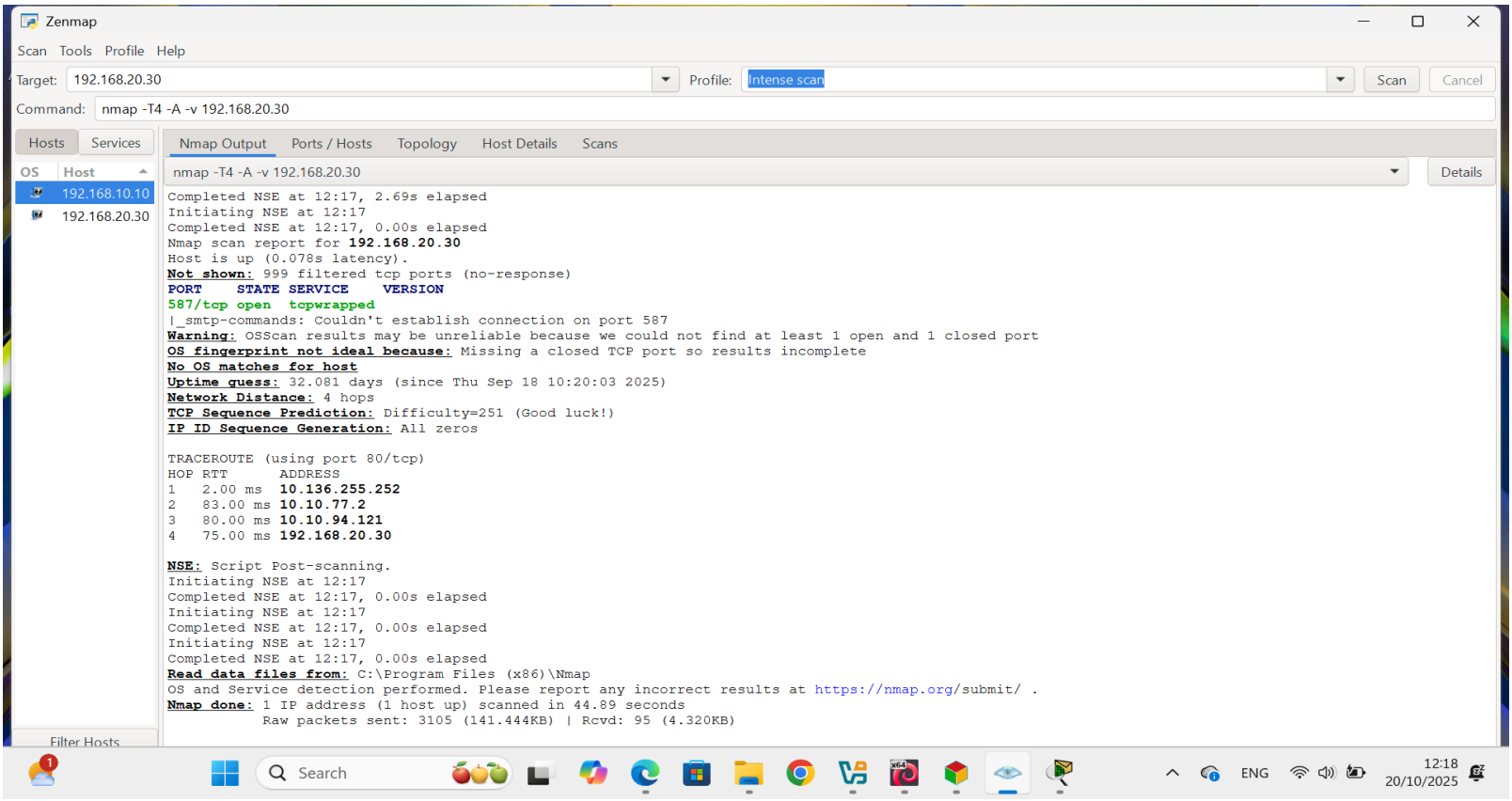
sudo nmap -sS -p- --min-rate 1000 192.168.10.10

Example output interpretation:

HOST	PORT	STATE	SERVICES
192.168.10.10	21	open	FTP Command
192.168.10.10	587	open	SMPT SUBMISSION
192.168.10.10	80	open	HTTP
192.168.10.10	22	open	SSH
192.168.10.10	-----	open	ICMP


Applications Places System
Mon Oct 20, 10:38
Parrot Terminal
File Edit View Search Terminal Help
$sudo nmap -sS -p 192.168.10.10
Starting Nmap 7.94SVN (https://nmap.org) at 2025-10-20 10:32 UTC
Error #487: Your port specifications are illegal. Example of proper form: "-100,200-1024,T:3000-4000,U:60000-"
QUITTING!
[x]-[user@parrot]-[~]
$sudo nmap -sS -p- --min-rate 1000 192.168.20.30
Starting Nmap 7.94SVN (https://nmap.org) at 2025-10-20 10:32 UTC
Nmap scan report for 192.168.20.30
Host is up (0.21s latency).
Not shown: 65534 filtered tcp ports (no-response)
PORT STATE SERVICE
587/tcp open submission
Nmap done: 1 IP address (1 host up) scanned in 134.45 seconds
[user@parrot]-[~]
$sudo apt install wireshark
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
wireshark is already the newest version (4.0.17-0+deb12u1).
wireshark set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 209 not upgraded.
[user@parrot]-[~]
$sudo tshark -i 192.168.10.10 -w capture.pcap
Running as user "root" and group "root". This could be dangerous.
Capturing on '192.168.10.10'
tshark: The capture session could not be initiated due to error getting information on pipe or socket: Permission denied.
tshark:
[x]-[user@parrot]-[~]
$
Menu
Parrot Terminal


Applications Places System
Fri Oct 17, 14:46
Parrot Terminal
File Edit View Search Terminal Help
W: Target Packages (contrib/binary-all/Packages) is configured multiple times in /etc/apt/sources.list:1 and /etc/apt/sources.list.d/parrot.list:19
W: Target Translations (contrib/i18n/Translation-en_US) is configured multiple times in /etc/apt/sources.list:1 and /etc/apt/sources.list.d/parrot.list:19
W: Target Translations (contrib/i18n/Translation-en) is configured multiple times in /etc/apt/sources.list:1 and /etc/apt/sources.list.d/parrot.list:19
W: Target Packages (non-free/binary-amd64/Packages) is configured multiple times in /etc/apt/sources.list:1 and /etc/apt/sources.list.d/parrot.list:19
W: Target Packages (non-free/binary-all/Packages) is configured multiple times in /etc/apt/sources.list:1 and /etc/apt/sources.list.d/parrot.list:19
W: Target Translations (non-free/i18n/Translation-en_US) is configured multiple times in /etc/apt/sources.list:1 and /etc/apt/sources.list.d/parrot.list:19
W: Target Translations (non-free/i18n/Translation-en) is configured multiple times in /etc/apt/sources.list:1 and /etc/apt/sources.list.d/parrot.list:19
[user@parrot]-[~]
$nmap -sn 192.168.10.0/24
Starting Nmap 7.94SVN (https://nmap.org) at 2025-10-17 14:37 UTC
Nmap done: 256 IP addresses (0 hosts up) scanned in 105.71 seconds
[user@parrot]-[~]
$nmap -sS -p- --min-rate 1000 192.168.10.10
You requested a scan type which requires root privileges.
QUITTING!
[x]-[user@parrot]-[~]
$sudo nmap -sS -p- --min-rate 1000 192.168.10.10
Starting Nmap 7.94SVN (https://nmap.org) at 2025-10-17 14:42 UTC
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
Nmap scan report for 192.168.10.10
Host is up (2.4s latency).
Not shown: 65534 filtered tcp ports (no-response)
PORT STATE SERVICE
21/tcp open ftp
Nmap done: 1 IP address (1 host up) scanned in 146.80 seconds
[user@parrot]-[~]
$
Menu
Parrot Terminal



Explanation:

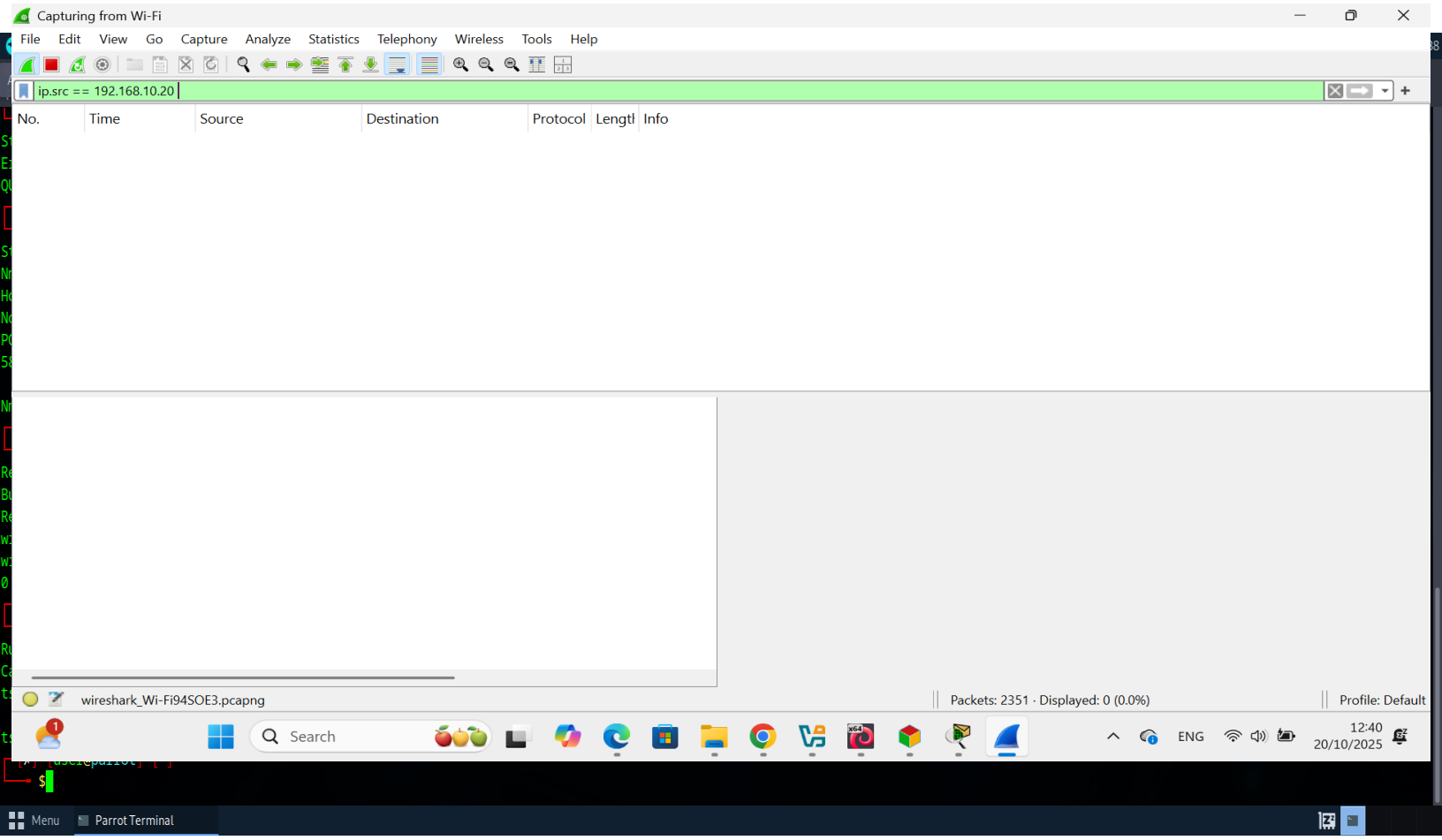
- Internet Control Message Protocol (ICMP) (Layer 3 of the OSI model) is up and running; how do we know this, because we were able to ping networks and traceroute.
- We have the HTTP port 80 which controls the web traffic
- File Transfer Protocol (FTP) Command port 21, for login and control.
- Simple Mail Transfer Protocol (SMTP) port 587, used for mail submission from users to mail servers.
- Secure Shell(SSH) port 22, since we were able to Secure remote login and command execution between devices.

9. Packet Capture and Analysis using Wireshark

Wireshark was used to capture network packets and analyze communications between VLANs. Filters were applied to monitor specific traffic such as ICMP, HTTP, and SSH.

Example display filters used:
- ICMP: icmp
- HTTP: tcp.port == 80
- SSH: tcp.port == 22
- VLAN 10 to VLAN 20 traffic: ip.src==192.168.10.0/24 && ip.dst==192.168.20.0/24

Captured results showed successful and blocked communication as per firewall configuration.



Captured results showed blank and blocked communication as per firewall configuration.

10. Results and Discussion

The following observations were made from the network simulation:
- VLAN segmentation successfully isolated traffic between networks.
- The firewall enforced rules preventing Guest access to the Office and Server networks.
- Nmap scans confirmed open and closed ports, allowing for targeted hardening.
- Wireshark captured no traffic due to firewall restrictions.

11. CONCLUSION

This project successfully demonstrated the configuration and security of a segmented network environment.
We gained hands-on experience using Cisco Packet Tracer for design, Nmap for vulnerability scanning, and Wireshark for packet analysis.
The setup emphasizes the importance of access control, monitoring, and ongoing security testing in real-world network defense.