

VICTOR AKINODE UNIVERSITY

NETWORK EXPANSION

AltSchool CyberSecurity Tinyuka 2024

GROUP 1

Submission date: August 22nd, 2025

TABLE OF CONTENT

TABLE OF CONTENT	1-2
1. MEET THE TEAM	3
TEAM	3
MEMBERS	3
2. EXECUTIVE SUMMARY	5
2.1. Project Overview	5
2.2. Project Result Summary	5
2.3. Technology Used	5
3. INTRODUCTION	6
3.1. Project Background	6
3.2. Project Objectives	6
3.3. Project Scope	6
4. NETWORK DESIGN	7
4.1. Network Design	7
4.2. IP Addressing Scheme	7
4.3. VLAN Design	8
4.4. Routing Configuration	9
4.5. DHCP Implementation	10
4.6. Security Features in Design	11
5. PKT IMPLEMENTATION	12
5.1. Device Setup	12
5.2. Vlan Configuration and Testing	12
5.3. IP Addressing and DHCP	13
5.5. Connectivity Tests	13

6. EVALUATION	16
6.1. Performance	16
6.2. Scalability	16
6.3. Reliability	16
6.4. Security	16
6.5. Limitations	16
7. CONCLUSION	16

1. MEET THE TEAM

TEAM	MEMBERS
Research	ALT/SOE/024/6094 ALT/SOE/024/5006 ALT/SOE/024/2591 ALT/SOE/024/4655
Configuration	ALT/SOE/024/5143 ALT/SOE/024/6109 ALT/SOE/024/4843 ALT/SOE/024/4711 ALT/SOE/024/6056 ALT/SOE/024/4663
Design	ALT/SOE/024/4644 ALT/SOE/024/5274 ALT/SOE/024/1806 ALT/SOE/024/3116 ALT/SOE/024/7819 ALT/SOE/024/3107
Documentation	ALT/SOE/024/4682 ALT/SOE/024/2658 ALT/SOE/024/6127 Oluwatobiloba Aladejare: ALT/SOE/024/5757

2. EXECUTIVE SUMMARY

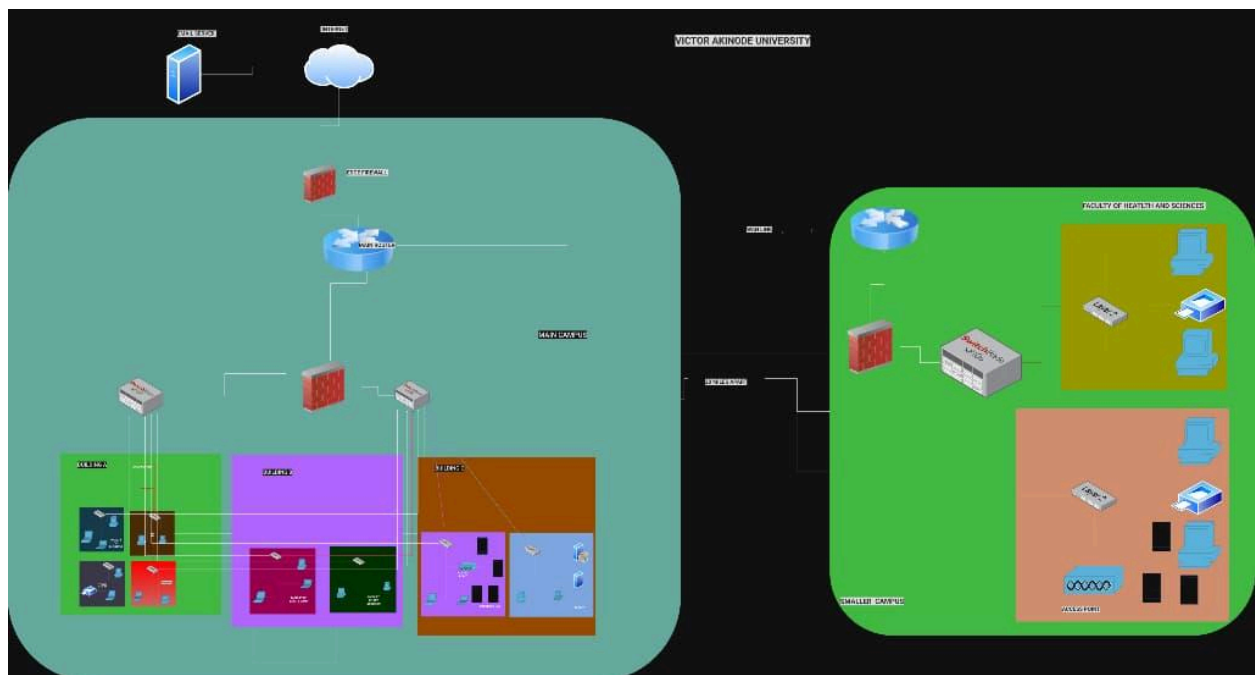
The University is undertaking a network expansion to provide robust, secure and scalable connectivity between two campuses within 20 miles distance. Using Cisco Packet Tracer, the design has been prototyped and tested to ensure end-to-end connectivity. This report outlines the design, configuration and evaluation of the upgraded network..

2.1 Project Overview

This project focuses on the design, configuration, and testing of a new network infrastructure for the University.

The infrastructure included

- Main Campus with three Buildings
- A small/ Branch campus hosting the Faculty of Sciences
- A central internet with email server integration



2.2 Project Result Summary

The final network design for Victor Akinode University delivers a secure, scalable, and high-performance infrastructure across both the Main and Smaller Campuses. DHCP was configured to automate IP allocation across all VLANs, removing manual configuration and improving efficiency. Access Control Lists (ACLs), VLAN segmentation and port security were integrated to restrict unauthorized access and safeguard sensitive resources. Redundancy was also built into the design through the use of dual Layer 3 switches and Hot Standby Router Protocol (HSRP) on the main campus.

The architecture is designed to support future growth without requiring major design through the distributed Layer 3 switching.

2.1. Technology Used

	TECHNOLOGY USED
Network Sketch	Draw.io
Network Simulation	Cisco Packet Tracer
Cisco Devices	Routers (2911), Layer 3 Switches (3560-24P, Layer 2 Switches (2960))
Cabling	Copper straight-through, cross-over and serial DCE
Protocols	RPIv2, HSRP, Static Routing, DHCP, ACLs
Team Meetings	Whatsapp, Google Meets

3. INTRODUCTION

3.1 Project Background

This University needed an infrastructure capable of supporting multiple departments, secure inter-campus communication and future growth. Previous security issues were addressed until the final design was achieved.

3.2 Project Objectives

The primary objective is to design and configure a secure, reliable and scalable network infrastructure for Victor Akinode university.

- Implement VLANS that will isolate departments
- Enable inter-VLAN routing and redundancy.
- Automate IP addressing with DHCP
- Ensure security through ACLs, port security and firewalls
- Validate all implementation using Cisco Packet tracer

3.3 Project Scope

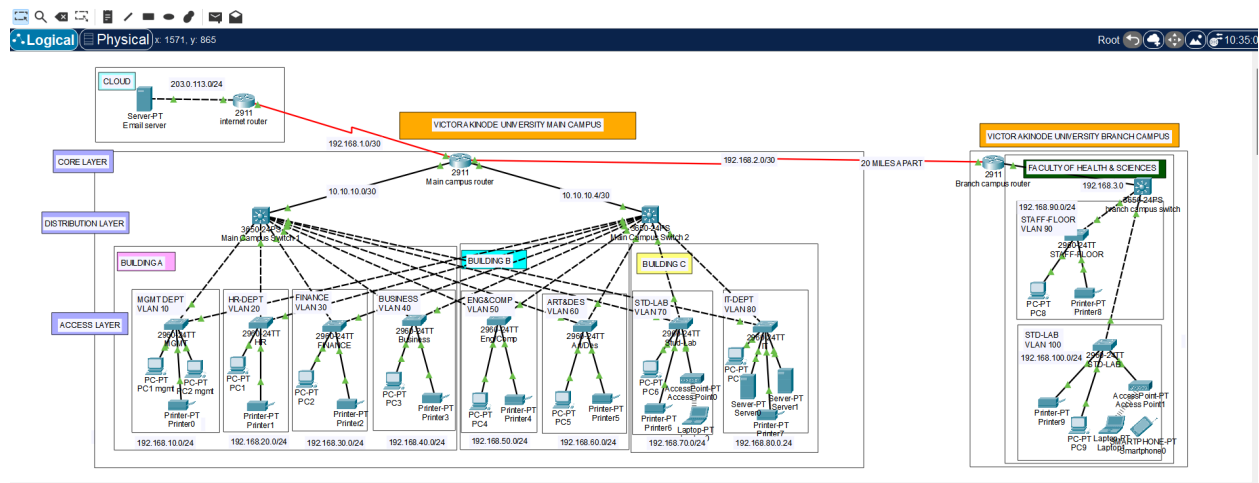
- ☐ The scope covers both the Main Campus and the smaller Campus.
- ☐ It includes cloud connectivity via internet router and email server.
- ☐ Implements LAN, VLAN, routing, DHCP and ACL-based security.

4. NETWORK DESIGN

4.1 Network Design

The design adopts a hierarchical structure with access switches per department, distributed via Layer 3 switches and core routers linking both campuses and the cloud.

- Main campus: Three buildings connected via Layer 3 switches. Building A uses router-based DHCP
- Smaller Campus: One Layer 3 switch manages departmental VLANs
- Inter-campus link: Serial WAN connection
- Cloud integration: External router connects to an email server with static routes.



VLANS	DEPARTMENT	IP ADDRESS	SUBNET
10	Management	192.168.10.0	/24
40	Business Faculty	192.168.40.0	/24
50	Engineering/Computing	192.168.50.0	/24
60	Art/Design	192.168.60.0	/24
70	Student Labs	192.168.70.0	/24
80	IT Department	192.168.80.0	/24

MINI CAMPUS

90	Faculty of science (Staff_Floor)	192.168.90.0	/24
100	Faculty of science (Student_floor)	192.168.100.0	/24

Inter-VLAN and External Connection

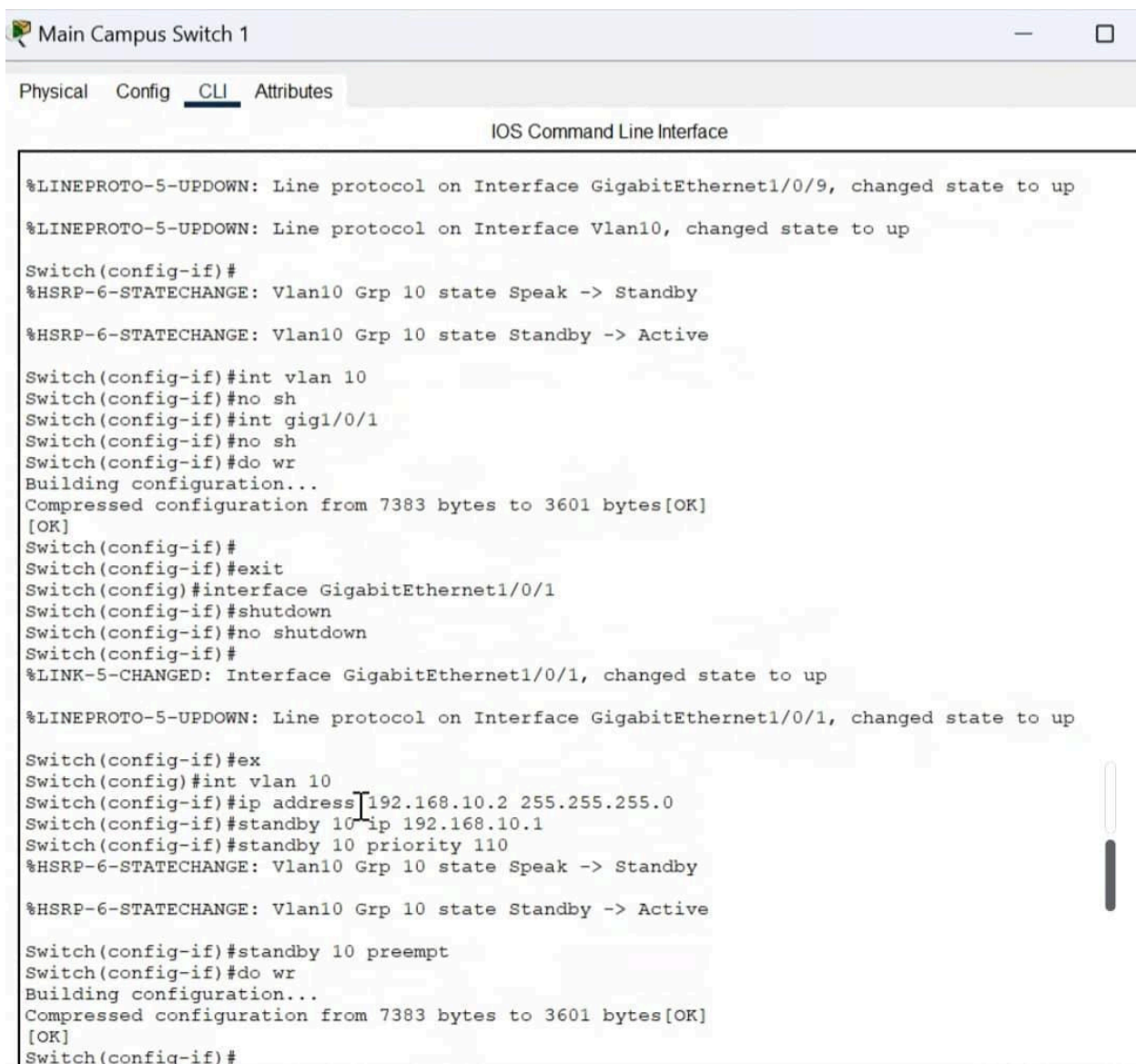
DEVICE	IP ADDRESS	CONNECTED TO
Server 2 (External)	203.0.113.0/24	Router1
Router1	192.168.1.0/30	Router0(Main Router)
Router0 (Main Router)	192.168.2.0/30	Router2 (MiniCampus)

4.3 VLAN Design

Each VLAN corresponds to a faculty to ensure traffic isolation and reduced broadcast domains, enforce security and specialize DHCP pools for different groups.

4.4 Routing Configuration

- RIPv2 is configured on internal routers for the VLAN networks across campuses
- Static Routes is used on the main router and internet router for external email server access
- inter-VLAN Routing is enabled on Layer 3 switches via Switch Virtual interfaces



```

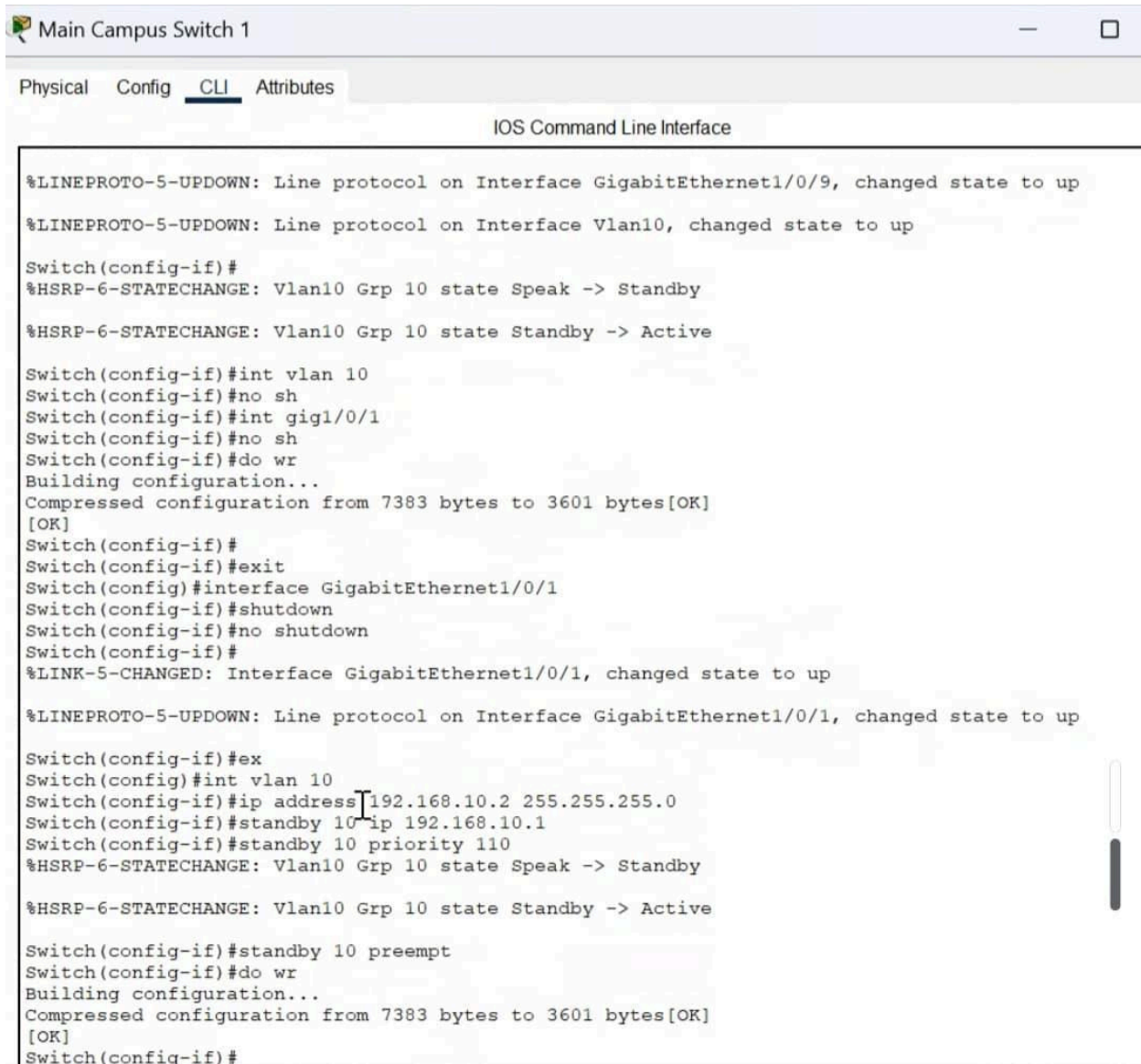
Main Campus Switch 1
Physical Config CLI Attributes
IOS Command Line Interface

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/9, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up
Switch(config-if)#
%HSRP-6-STATECHANGE: Vlan10 Grp 10 state Speak -> Standby
%HSRP-6-STATECHANGE: Vlan10 Grp 10 state Standby -> Active
Switch(config-if)#int vlan 10
Switch(config-if)#no sh
Switch(config-if)#int gig1/0/1
Switch(config-if)#no sh
Switch(config-if)#do wr
Building configuration...
Compressed configuration from 7383 bytes to 3601 bytes[OK]
[OK]
Switch(config-if)#
Switch(config-if)#exit
Switch(config)#interface GigabitEthernet1/0/1
Switch(config-if)#shutdown
Switch(config-if)#no shutdown
Switch(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet1/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed state to up
Switch(config-if)#ex
Switch(config)#int vlan 10
Switch(config-if)#ip address 192.168.10.2 255.255.255.0
Switch(config-if)#standby 10 ip 192.168.10.1
Switch(config-if)#standby 10 priority 110
%HSRP-6-STATECHANGE: Vlan10 Grp 10 state Speak -> Standby
%HSRP-6-STATECHANGE: Vlan10 Grp 10 state Standby -> Active
Switch(config-if)#standby 10 preempt
Switch(config-if)#do wr
Building configuration...
Compressed configuration from 7383 bytes to 3601 bytes[OK]
[OK]
Switch(config-if)#

```

4.1. DHCP Implementation

Layer 3 switches were configured with DHCP pools for each VLAN and ensured automatic assignment of IP addresses, default gateways and DNS. Router-based DHCP is configured in Building A to provide dynamic addressing to Management, HR, Finance and Business.



```

Main Campus Switch 1
Physical Config CLI Attributes
IOS Command Line Interface

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/9, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up
Switch(config-if)#
%HSRP-6-STATECHANGE: Vlan10 Grp 10 state Speak -> Standby
%HSRP-6-STATECHANGE: Vlan10 Grp 10 state Standby -> Active

Switch(config-if)#int vlan 10
Switch(config-if)#no sh
Switch(config-if)#int gig1/0/1
Switch(config-if)#no sh
Switch(config-if)#do wr
Building configuration...
Compressed configuration from 7383 bytes to 3601 bytes[OK]
[OK]
Switch(config-if)#
Switch(config-if)#exit
Switch(config)#interface GigabitEthernet1/0/1
Switch(config-if)#shutdown
Switch(config-if)#no shutdown
Switch(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet1/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1, changed state to up

Switch(config-if)#ex
Switch(config)#int vlan 10
Switch(config-if)#ip address 192.168.10.2 255.255.255.0
Switch(config-if)#standby 10 ip 192.168.10.1
Switch(config-if)#standby 10 priority 110
%HSRP-6-STATECHANGE: Vlan10 Grp 10 state Speak -> Standby
%HSRP-6-STATECHANGE: Vlan10 Grp 10 state Standby -> Active

Switch(config-if)#standby 10 preempt
Switch(config-if)#do wr
Building configuration...
Compressed configuration from 7383 bytes to 3601 bytes[OK]
[OK]
Switch(config-if)#

```

PC0

Physical Config **Desktop** Programming Attributes

IP Configuration [X]

Interface: FastEthernet0

IP Configuration

☒ DHCP ☐ Static DHCP request successful.

IPv4 Address: 192.168.10.4

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.10.1

DNS Server: 192.168.10.1

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address: /

Link Local Address: FE80::207:ECFF:FE7A:D56B

Default Gateway:

DNS Server:

802.1X

☐ Use 802.1X Security

Authentication: MD5

Username:

Password:

☐ Top

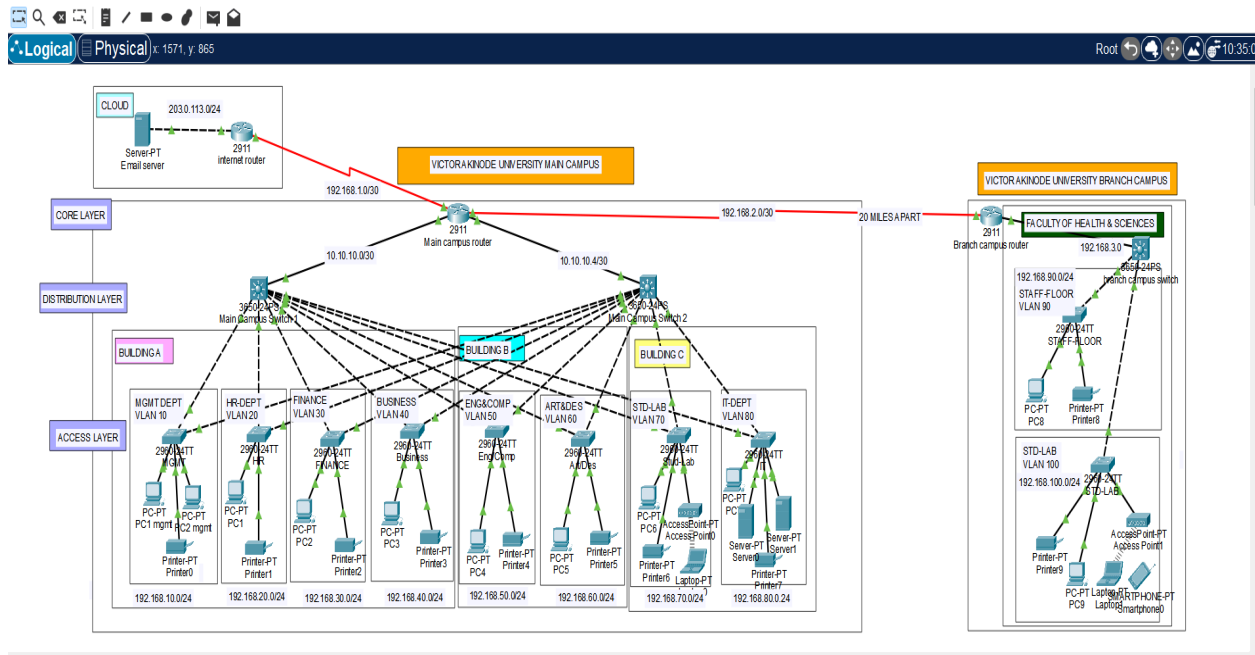
4.2 Security Features in Design

The network incorporates multiple layers of security to protect sensitive data, ensure system availability and reduce threats.

- VLAN segmentation for isolation of sensitive departments like Finance and IT

- Port Security on access switches to prevent unauthorized access
- ACLs for access control; only IT department can SSH/Telnet to routers
- Blocked P2P/torrent traffic

5. Packet Tracer Implementation



5.1. Device Setup

Routers, switches, servers, PSc and wireless access points are configured

- Main Campus: 3 Layer 2 switches (access), 2 Layer 3 switches (distribution) and 1 router
- Smaller Campus: 2 access switches, 1 Layer 3 switch and 1 router
- Cloud: 1 internet router and email server

5.2. VLAN Configuration and Testing

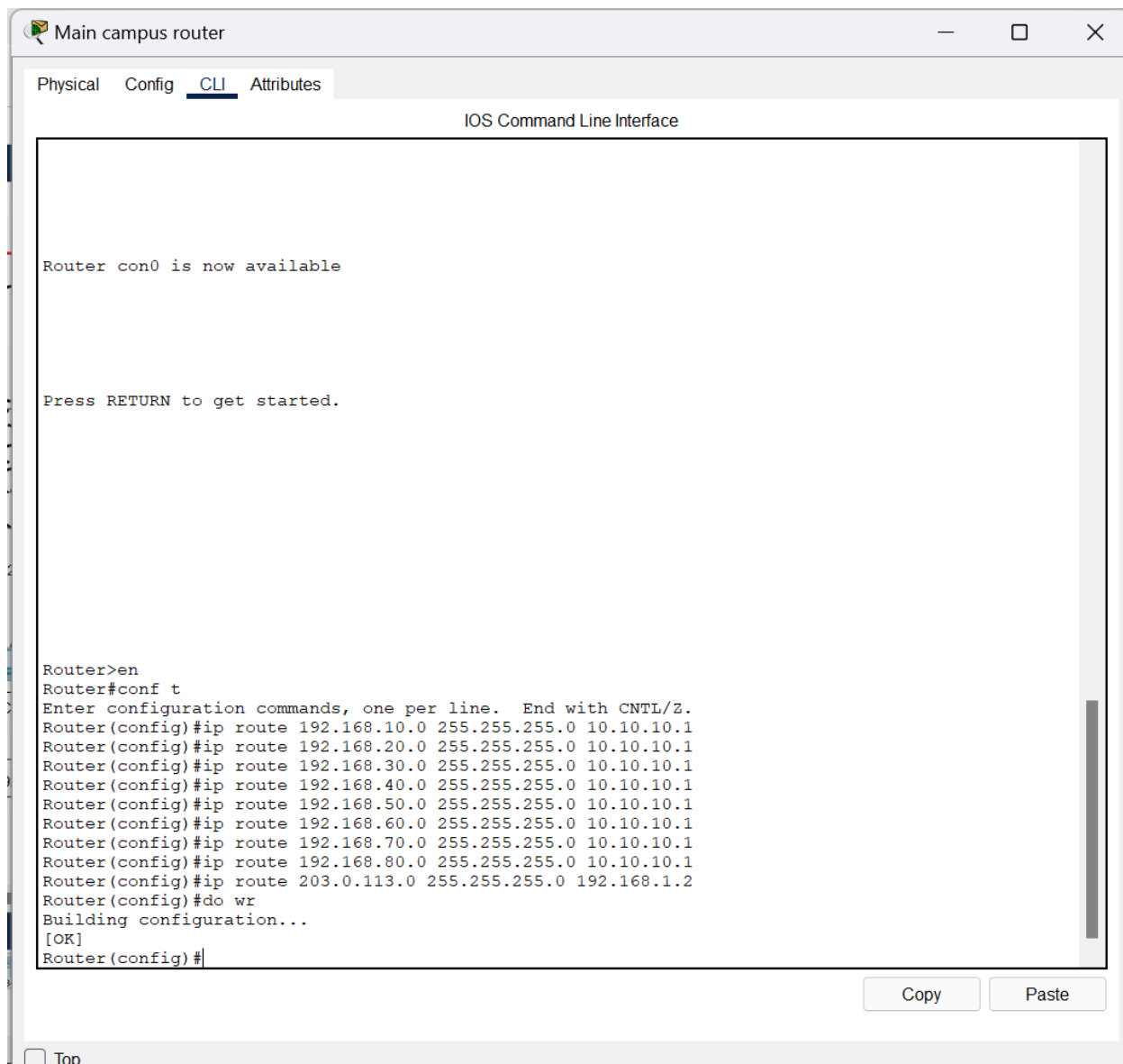
VLANs were created and assigned to access switch ports. Testing confirmed devices in the same VLAN could communicate while inter-VLAN communication required routing.

5.3. IP Addressing and DHCPs

Devices automatically received IPs from DHCP pools configured on the Layer 3 switches while End devices in Building A dynamically received IPs via router-based DHCP.

5.4. Connectivity testing

- Ping test confirmed inter-VLAN communication



The screenshot shows the CLI interface of a 'Main campus router'. The interface has tabs for 'Physical', 'Config', 'CLI' (selected), and 'Attributes'. The main area displays the 'IOS Command Line Interface' with the following text:

```
Router con0 is now available

Press RETURN to get started.

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip route 192.168.10.0 255.255.255.0 10.10.10.1
Router(config)#ip route 192.168.20.0 255.255.255.0 10.10.10.1
Router(config)#ip route 192.168.30.0 255.255.255.0 10.10.10.1
Router(config)#ip route 192.168.40.0 255.255.255.0 10.10.10.1
Router(config)#ip route 192.168.50.0 255.255.255.0 10.10.10.1
Router(config)#ip route 192.168.60.0 255.255.255.0 10.10.10.1
Router(config)#ip route 192.168.70.0 255.255.255.0 10.10.10.1
Router(config)#ip route 192.168.80.0 255.255.255.0 10.10.10.1
Router(config)#ip route 203.0.113.0 255.255.255.0 192.168.1.2
Router(config)#do wr
Building configuration...
[OK]
Router(config)#
```

At the bottom right of the CLI window, there are 'Copy' and 'Paste' buttons. At the bottom left, there is a 'Top' button.

- Branch-Main campus connectivity was successful

WEB SERVER

Physical Config Services Desktop Programming Attributes

IP Configuration

IP Configuration

☐ DHCP ☒ Static

IPv4 Address 192.168.80.45

Subnet Mask 255.255.255.0

Default Gateway 192.168.80.1

DNS Server 192.168.80.1

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address /

Link Local Address FE80::260:3EFF:FE34:D68E

Default Gateway

DNS Server

802.1X

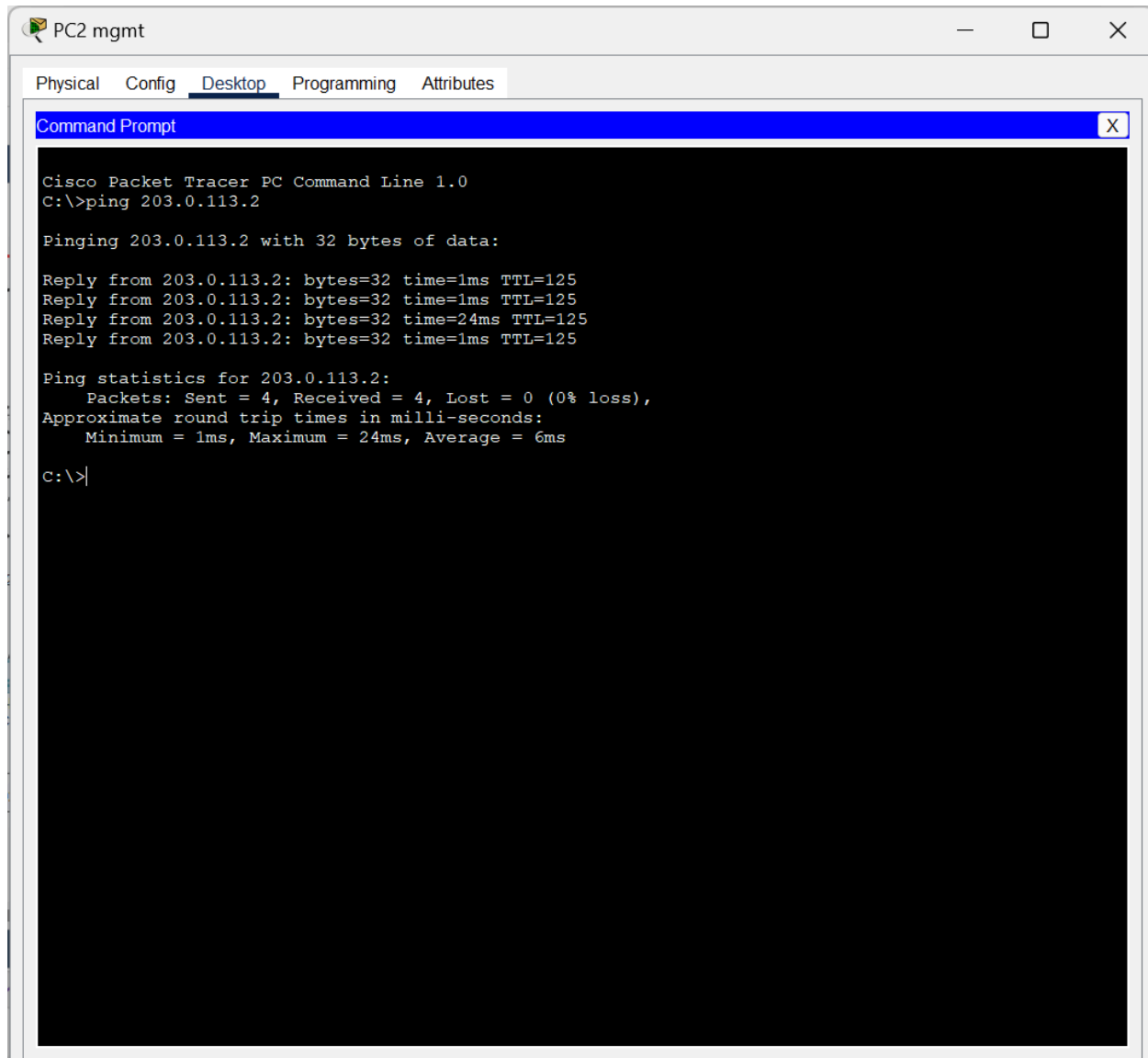
☐ Use 802.1X Security

Authentication MD5

Username

Password

- External email server is accessible from internal clients



The screenshot shows a window titled "PC2 mgmt" with tabs for Physical, Config, Desktop, Programming, and Attributes. The "Desktop" tab is active, displaying a "Command Prompt" window. The command prompt shows the execution of a ping command to the IP address 203.0.113.2. The output indicates that the ping was successful, with 4 packets sent and received, and a 0% loss rate. The round trip times are also displayed.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 203.0.113.2

Pinging 203.0.113.2 with 32 bytes of data:

Reply from 203.0.113.2: bytes=32 time=1ms TTL=125
Reply from 203.0.113.2: bytes=32 time=1ms TTL=125
Reply from 203.0.113.2: bytes=32 time=24ms TTL=125
Reply from 203.0.113.2: bytes=32 time=1ms TTL=125

Ping statistics for 203.0.113.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 24ms, Average = 6ms

C:\>|
```


6. EVALUATION

6.1. Performance

- Hierarchical design reduced latency and congestion.
- Redundant gateways minimized downtime risk.

6.2. Scalability

- Distributed architecture allows seamless addition of new buildings/departments.

6.3. Reliability

- HSRP and redundant links ensure high availability.
- Packet Tracer tests confirmed fault tolerance.

6.4. Security

- VLAN isolation, ACLs and firewalls enforces strict access policies.
- Reduced exposure to internal/external threats.

6.5. Limitations

- The simulation environment may not capture all real-time failures and performance conditions.
- The use of RIPv2 presents scalability challenges as it is more suitable for small or medium sized networks. Large scale networks may require more advanced protocols.
- Wireless security configurations were also not extensively tested.

7. CONCLUSION

The network design for Victor Akinode University successfully meets the objectives of being scalable, secure, and resilient. Through the segmentation of departments using VLANs, assigning of dynamic IP addresses via DHCP, deployment of redundant gateways, and the enforcement of ACL-based security controls, the design ensures efficient traffic flow and reliable access to resources. The inclusion of HSRP further provides redundancy and guarantees that services remain available even in the event of

device failure.

For a real-life deployment, additional measures will be essential. It is important to strengthen security with firewall rules, ACLs, and authentication systems like IEEE 802.1X which will provide greater protection against internal and external threats. Also, implementing monitoring and intrusion tools will detect and respond to anomalies quickly. Planning for hardware upgrades will also ensure that the network can handle future growth and evolving security threats.