APEX SOLUTIONS

NETWORK DESIGN REPORT

Prepared by: Sanjeel Shrestha

IT Graduate | Networking & Cybersecurity

Sydney, NSW, Australia

May 2026

Tools: Cisco Packet Tracer | Cisco Portfolio Project

1. Introduction

This network is the network infrastructure of Apex Solutions that has separated the access to different categories of users like the staff, management and guests. VLANs ensure each group of users is isolated from one another, preventing unauthorized access between departments. There are three VLANs — 10, 20 and 99 — representing Staff, Guest and Management respectively, with Management being VLAN 99 specifically to avoid accidental access.

2. Network Topology

The network consists of one Cisco 2911 router (Apex-Router), two Cisco 2960 switches (Switch-Staff and Switch-Guest), and seven end devices. The router connects to both switches via GigabitEthernet ports and handles inter-VLAN routing through subinterfaces.

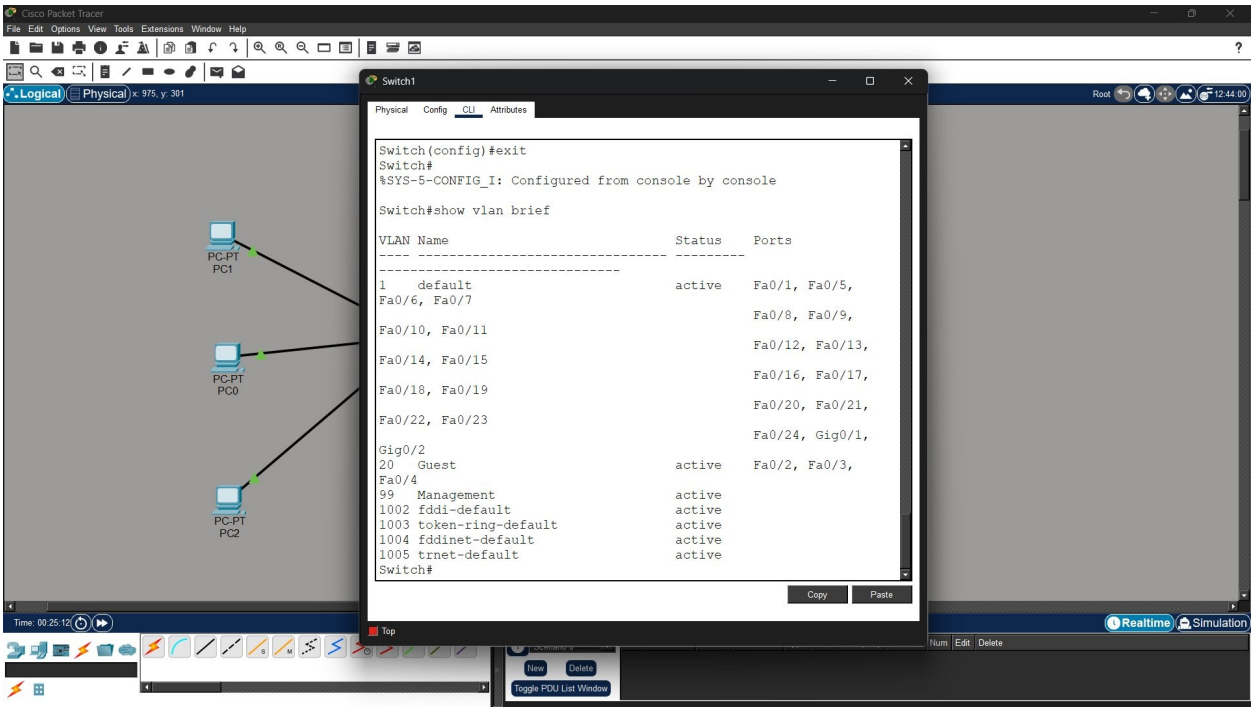

Figure 1 — Apex Solutions Network Topology in Cisco Packet Tracer

3. IP Addressing Table

Device	VLAN	IP Address	Subnet Mask	Default Gateway
Apex-Router Gig0/0.10	10	192.168.10.1	255.255.255.0	—

Device	VLAN	IP Address	Subnet Mask	Default Gateway
Apex-Router Gig0/0.99	99	192.168.99.1	255.255.255.0	—
Apex-Router Gig0/1.20	20	192.168.20.1	255.255.255.0	—
Staff-PC1	10	192.168.10.2	255.255.255.0	192.168.10.1
Staff-PC2	10	192.168.10.3	255.255.255.0	192.168.10.1
Staff-PC3	10	192.168.10.4	255.255.255.0	192.168.10.1
Management-PC	99	192.168.99.2	255.255.255.0	192.168.99.1
Guest-PC1	20	192.168.20.2	255.255.255.0	192.168.20.1
Guest-PC2	20	192.168.20.3	255.255.255.0	192.168.20.1
Guest-PC3	20	192.168.20.4	255.255.255.0	192.168.20.1

4. VLAN Configuration

4.1 VLAN Assignments

VLAN ID	Name	Switch	Ports Assigned
10	Staff	Switch-Staff	Fa0/2, Fa0/3, Fa0/4
99	Management	Switch-Staff	Fa0/5
20	Guest	Switch-Guest	Fa0/2, Fa0/3, Fa0/4

4.2 Trunk Ports

Switch	Trunk Port	Connected To	VLANs Allowed
Switch-Staff	Fa0/1	Apex-Router Gig0/0	10, 99
Switch-Guest	Fa0/1	Apex-Router Gig0/1	20

5. Device Configuration

5.1 Switch-Staff Configuration

Switch-Staff was configured with VLAN 10 (Staff) and VLAN 99 (Management). Ports Fa0/2–Fa0/4 were assigned to VLAN 10 as access ports. Port Fa0/5 was assigned to VLAN 99. Port Fa0/1 was configured as a trunk port to carry all VLANs to the router.

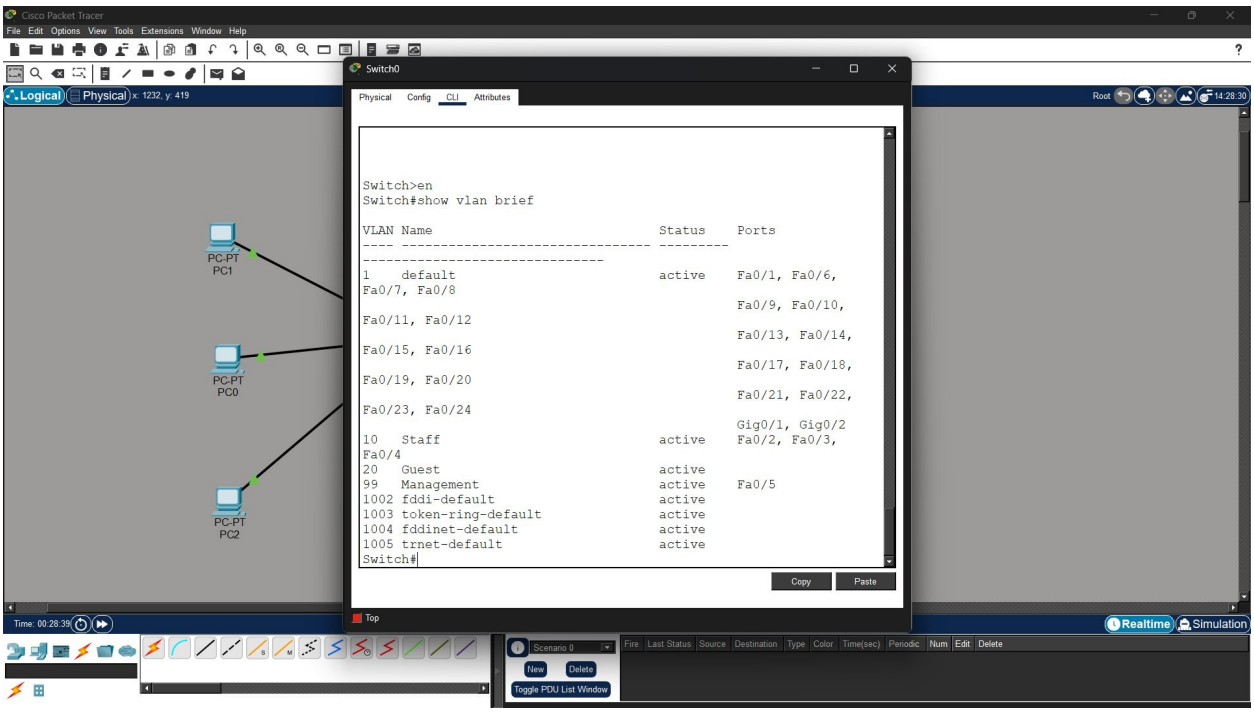

Figure 2 — Switch-Staff VLAN configuration commands

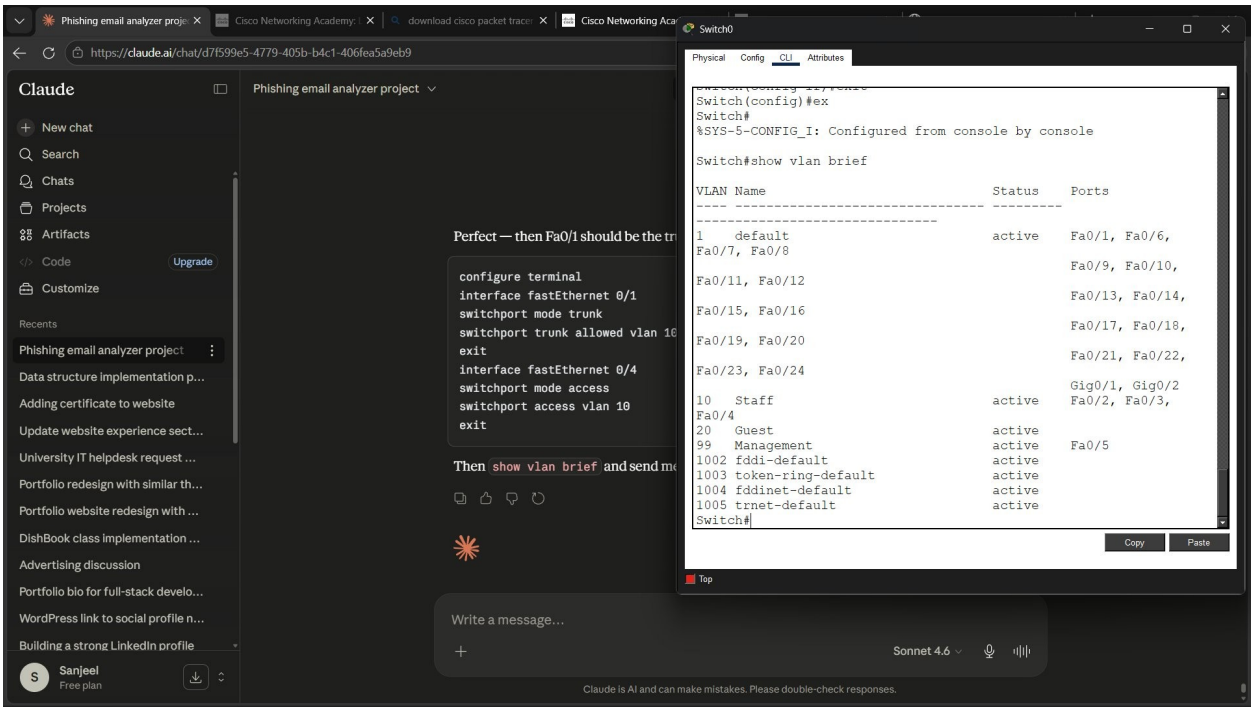

Figure 3 — Switch-Staff show vlan brief output

5.2 Switch-Guest Configuration

Switch-Guest was configured with VLAN 20 (Guest). Ports Fa0/2–Fa0/4 were assigned to VLAN 20 as access ports. Port Fa0/1 was configured as a trunk port to the router.

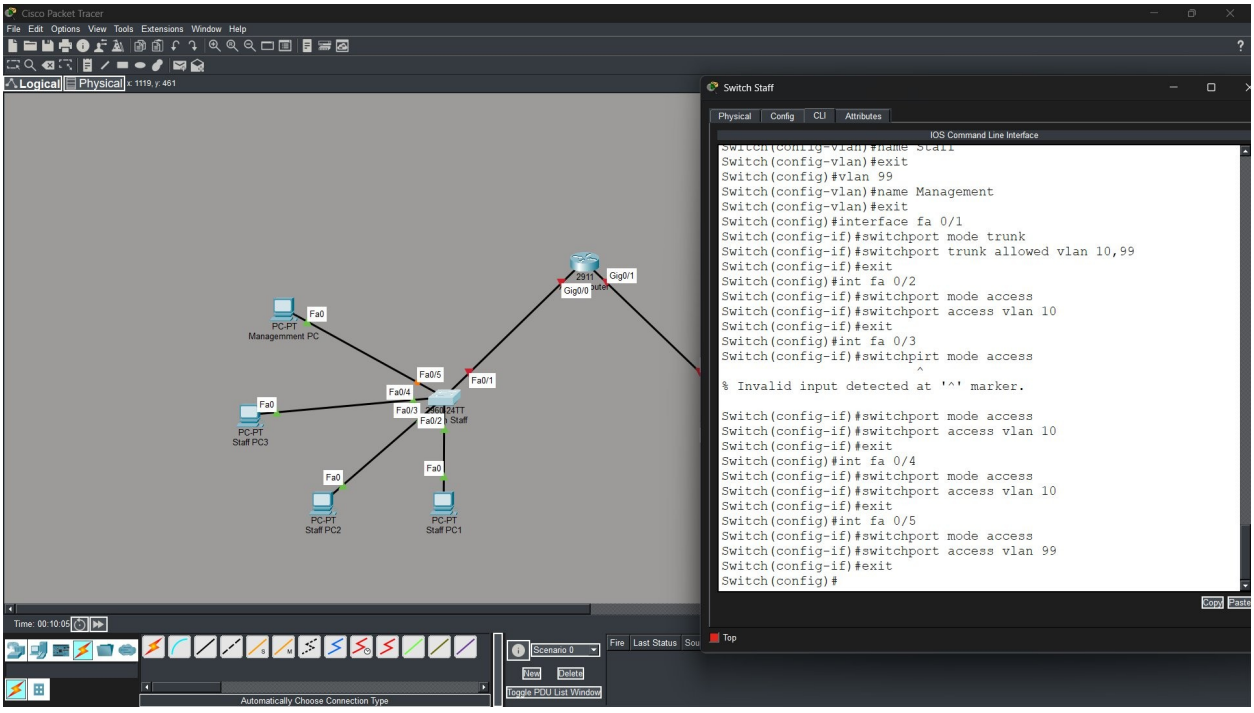

Figure 4 — Switch-Guest VLAN configuration commands

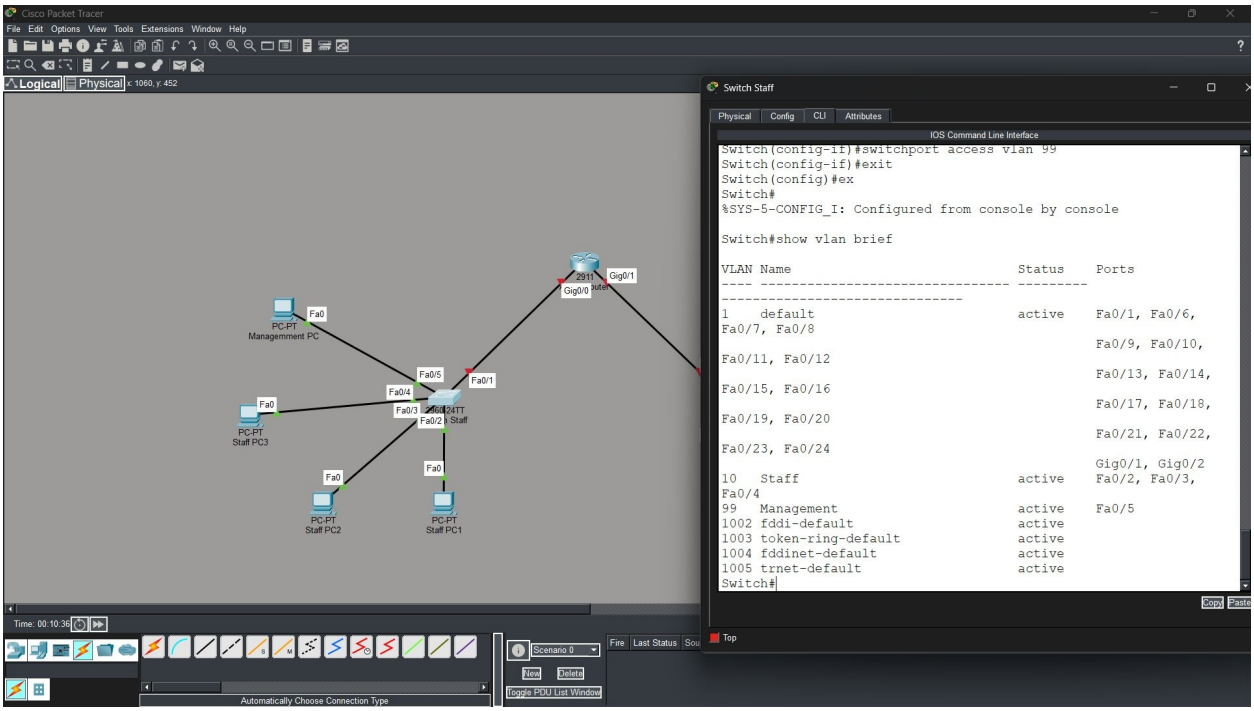

Figure 5 — Switch-Guest show vlan brief output

5.3 Apex-Router Configuration

The router was configured with subinterfaces on Gig0/0 for VLANs 10 and 99, and on Gig0/1 for VLAN 20. Each subinterface was assigned an IP address to serve as the default gateway for its respective VLAN. encapsulation dot1Q was used to tag VLAN traffic on each subinterface.

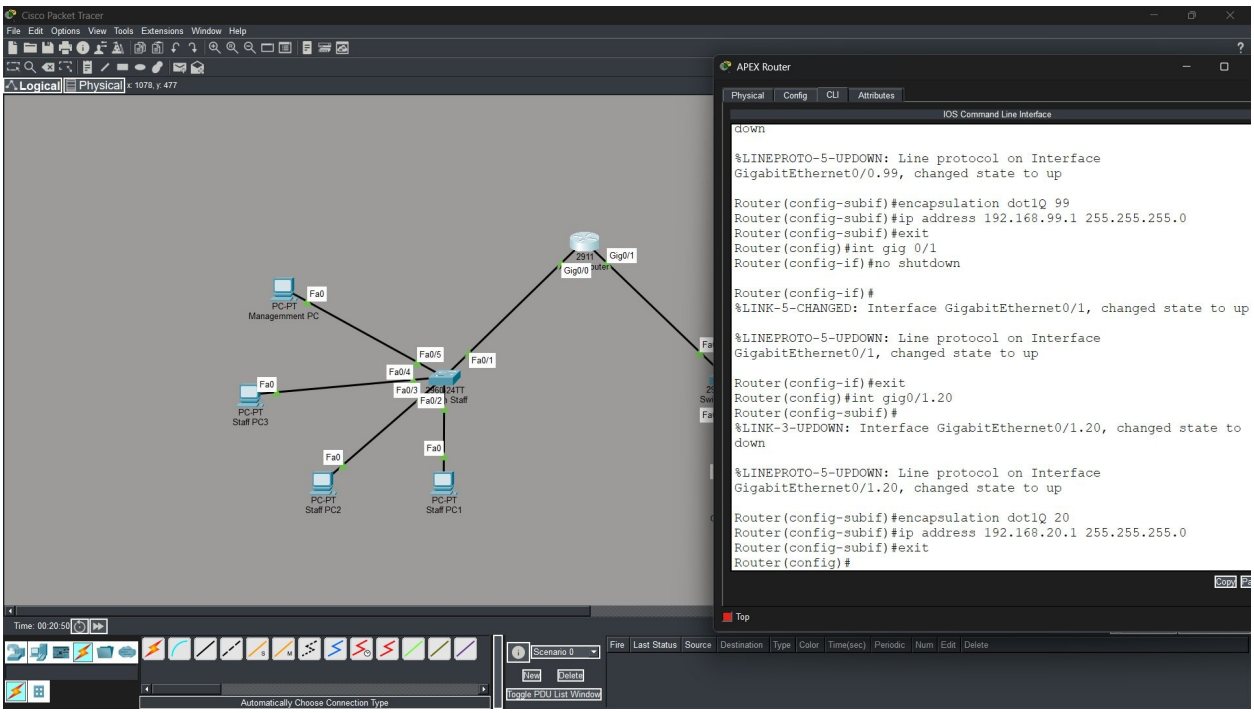

Figure 6 — Apex-Router subinterface configuration

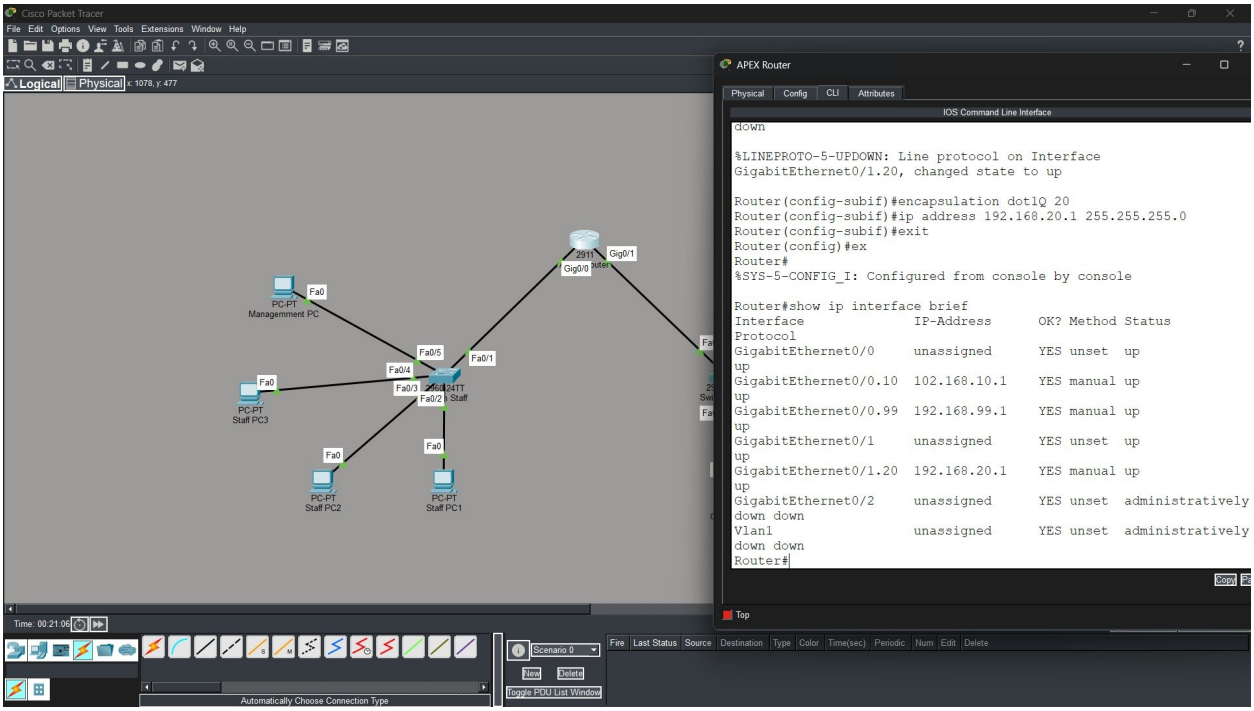

Figure 7 — Apex-Router show ip interface brief output

6. Testing Results

Connectivity was verified using ICMP ping tests between devices across all VLANs. The 25% packet loss on some tests is expected and is caused by the ARP resolution process on the first packet — all subsequent packets were successful.

- ✓ **Staff-PC1 → Staff Gateway (192.168.10.1):** 4/4 packets received — 0% loss
- ✓ **Staff-PC1 → Guest-PC1 (192.168.20.2):** 3/4 packets received — 25% loss (ARP)
- ✓ **Staff-PC1 → Management-PC (192.168.99.2):** 3/4 packets received — 25% loss (ARP)
- ✓ **Guest-PC1 → Management-PC (192.168.99.2):** 4/4 packets received — 0% loss
- ✓ **Guest-PC1 → Staff-PC1 (192.168.10.2):** 4/4 packets received — 0% loss

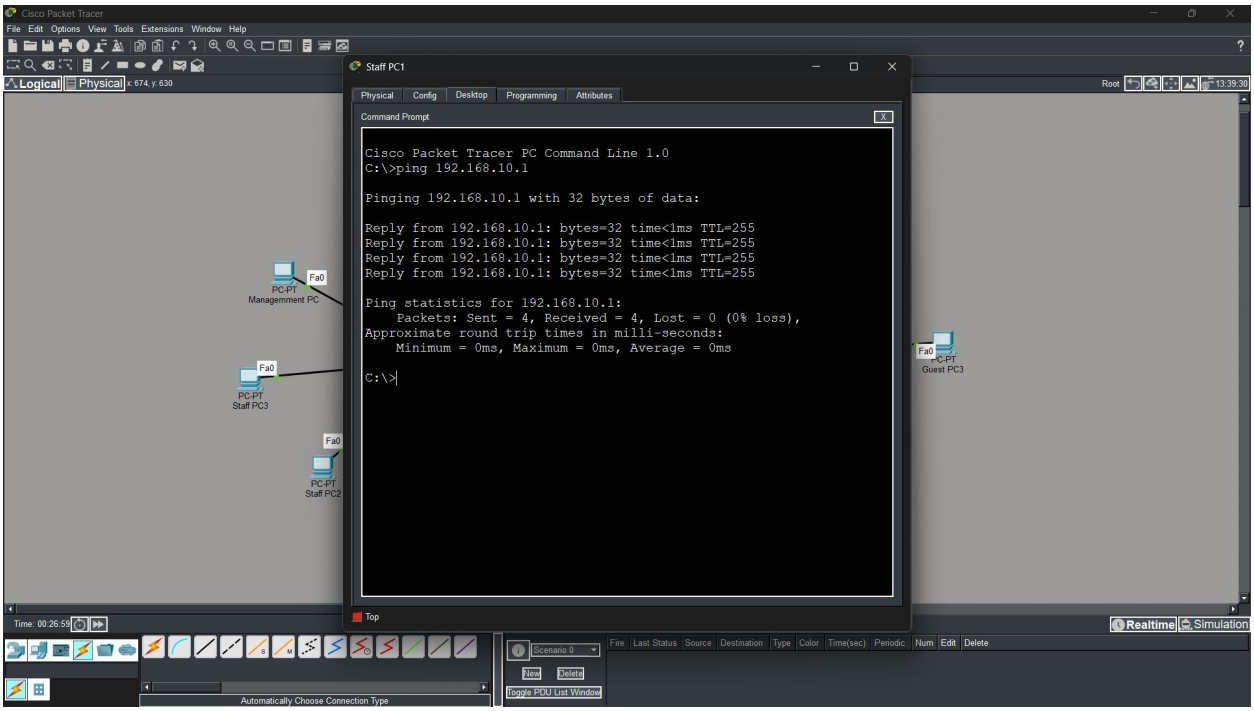

Figure 8 — Staff-PC1 pinging the Staff gateway successfully

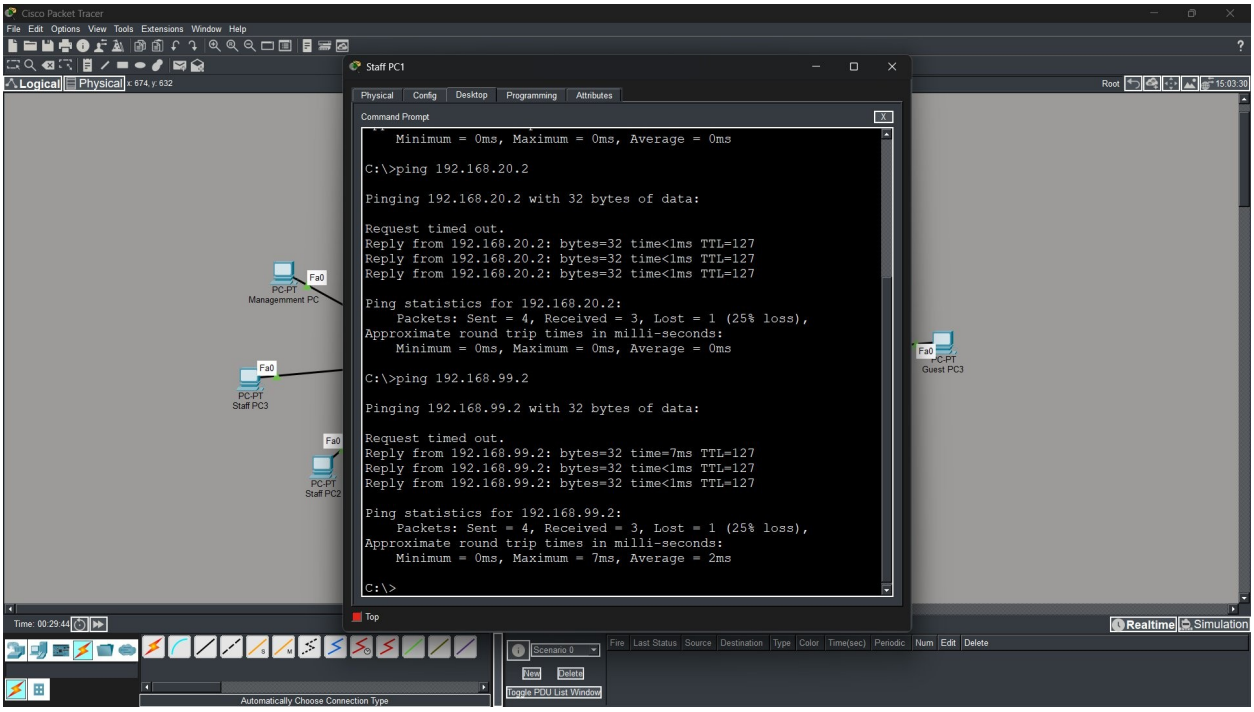

Figure 9 — Inter-VLAN ping results showing successful routing

7. Conclusion

A network infrastructure with two switches, one router, three Staff PCs, three Guest PCs and one Management PC was successfully built and configured in Cisco Packet Tracer. VLANs ensured the prevention of unauthorized access between different categories of users, with each group isolated to its own network segment. In the future, a firewall can be added to further control traffic between VLANs, and internet connectivity can be provided to all users through the router.