UNIVERSITY OF GONDAR

COLLEGE OF INFORMATICS

DEPARTMENT OF COMPUTER SCIENCE

DATA COMMUNICATION AND COMPUTER NETWORKS(CoSc2032)

GROUP ASSIGNMENT

Student Name	*ID*
Birhanu Fiseha	*GUR/02498/15*
Bihoney Gebremeskel	*GUR/01020/16*
Atinaw Dessie	*GUR/22848/16*
Miheretu Mulunehe	*GUR/00341/16*
Temesegen dessie	*GUR/ 01339/16*

Submitted to: Mr. Hailu

Submission Date: 11/10/2017 E.C

❖ Network Design & IP Addressing

1. How did you divide your network segments (VLANs)?

Answer:
The University network was segmented using Virtual Local Area Networks (VLANs) to separate different departments logically. Each department has its own VLAN to isolate traffic, improve security, and allow for better control and performance. The segmentation was based on organizational roles:

- **VLAN 10 (ADMIN_VLAN)**: For administrative offices
- **VLAN 20 (STAFF_VLAN)**: For academic and technical staff
- **VLAN 30 (STUDENT_VLAN)**: For student computer labs and dormitories
- **VLAN 40 (LIB_VLAN)**: For the digital library
- **VLAN 50 (SERVER_VLAN)**: For all servers like DHCP, DNS, FTP, and Web

This structure simplifies troubleshooting, monitoring, and access control while enabling scalability for future expansion.

2. Explain how you assigned IP addresses and gateways to each segment.

Answer:
Each VLAN was assigned a different **/24 subnet** from a private IP range. The **first usable IP address** in each subnet was used as the **default gateway**, which is configured on the router subinterface using **Router-on-a-Stick**.

VLAN Name	Subnet	Default Gateway
ADMIN_VLAN	192.168.10.0/24	192.168.10.1
STAFF_VLAN	192.168.20.0/24	192.168.20.1
STUDENT_VLAN	192.168.30.0/24	192.168.30.1
LIB_VLAN	192.168.40.0/24	192.168.40.1
SERVER_VLAN	192.168.50.0/24	192.168.50.1

Clients (PCs and servers) were then given IPs from the respective subnet ranges.

3. What is the advantage of using subnetting in a university environment?

Answer:
Subnetting offers several key advantages in a university environment:

- **Traffic Isolation**: Prevents broadcast storms by limiting them within each VLAN/subnet.
- **Security**: Easier to implement access control between departments (e.g., firewall rules).
- **Performance**: Reduces network congestion and improves data transfer efficiency.
- **IP Management**: Simplifies IP address planning and avoids wastage.
- **Scalability**: Allows the university to grow the network without disrupting the existing setup.

Figure 1: Network Topology Design (Working Area)

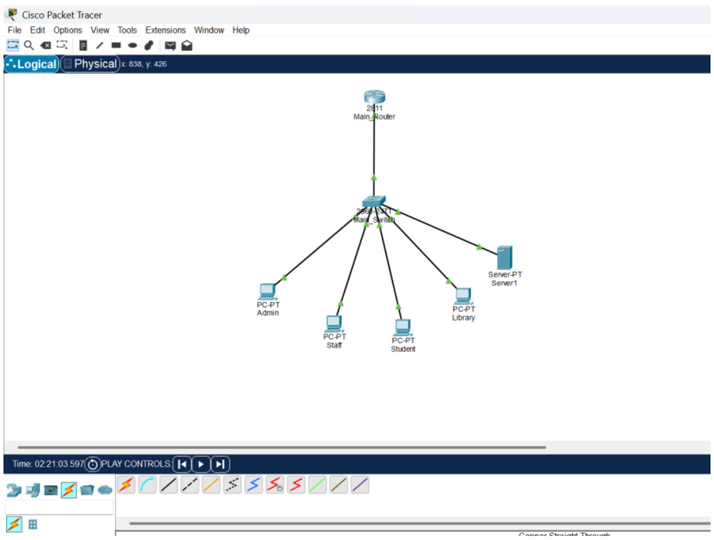


Figure 2: IP Address Configuration on End Devices (PC)

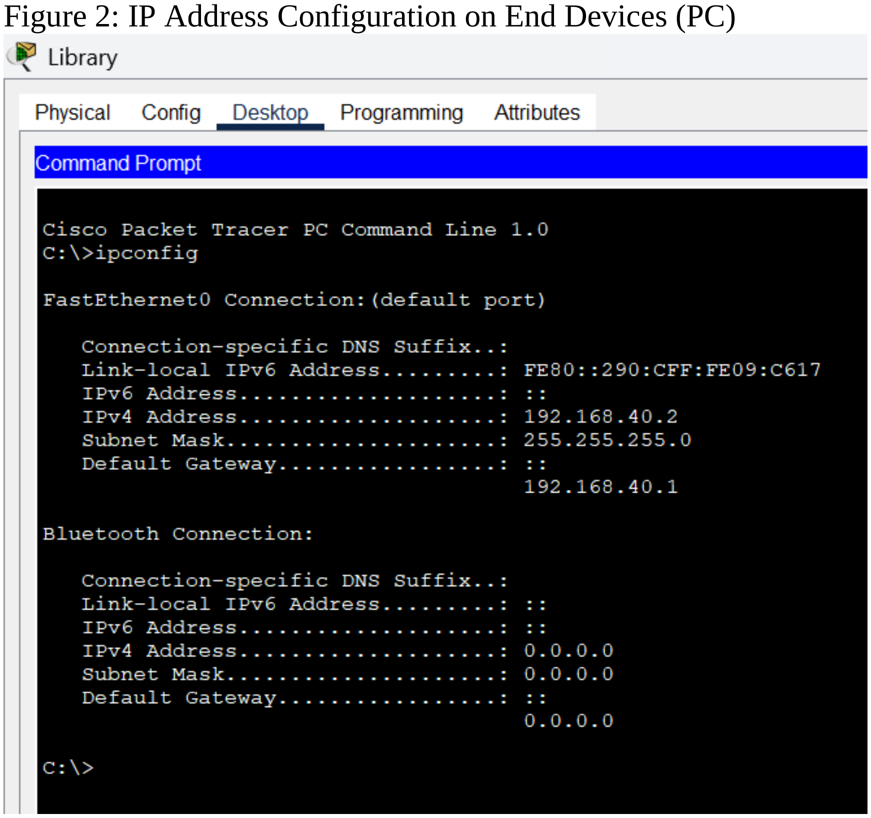
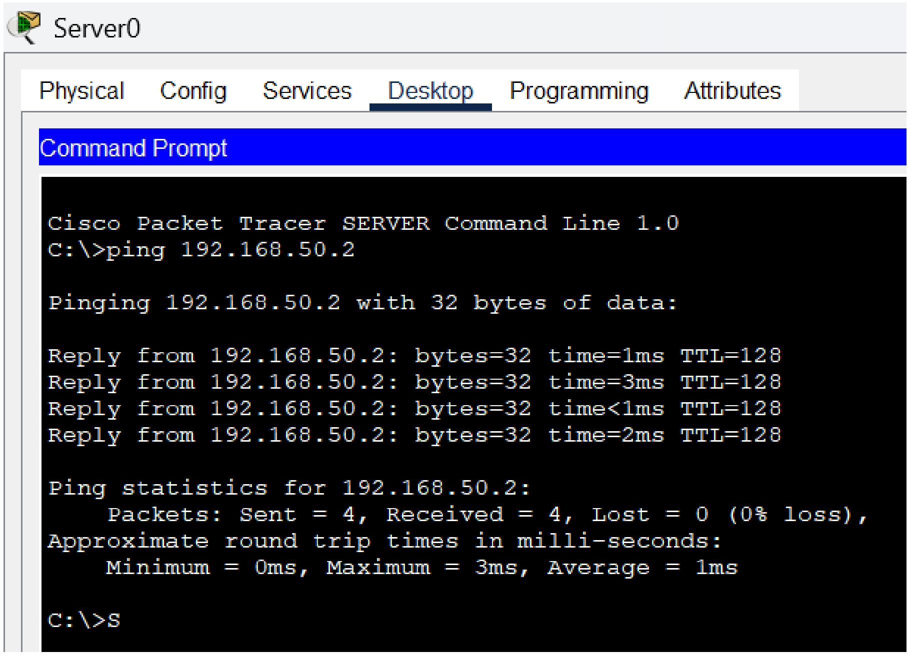


Figure 3: Ping Test Result from Server to PC



❖ Routing

4. What kind of routing did you implement — static, dynamic (e.g., RIP), or default? Why?

In this simulation, **static routing** was implemented. Static routes were manually configured on the router to define specific paths for packet forwarding. This approach is ideal for a small, simple network like this one because it provides control, is easy to manage in limited topologies, and doesn't require routing protocol overhead.

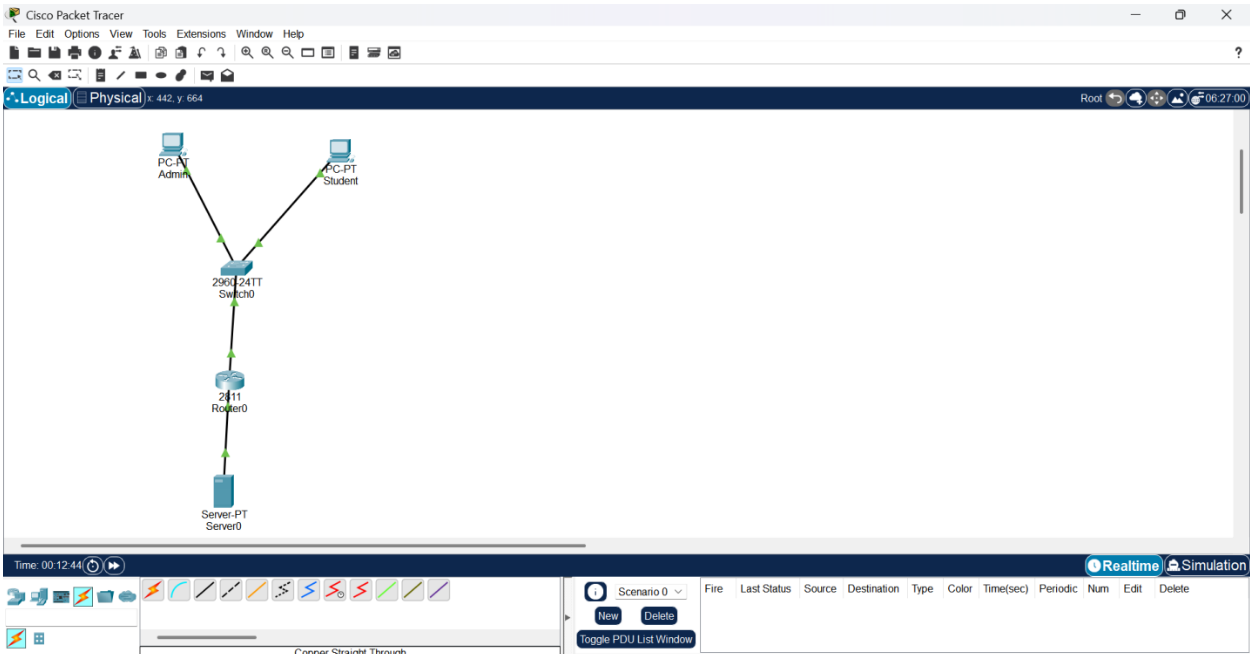
5. What is the purpose of default routing in your topology?

A **default route** acts as a "catch-all" path used when there's no specific route to a destination in the routing table. In this simulation, default routing ensures that traffic meant for external networks (such as the internet or an ISP) can be forwarded correctly, even if individual routes are not defined. It's especially useful in a university network to direct unknown traffic toward an external gateway.

6. How do routers communicate between departments and the ISP?

Routers communicate between internal segments (departments) using IP addresses and static routes to forward packets to the correct subnet or device. In a real-world university environment, routers may use VLANs and routing protocols (like OSPF or EIGRP) to manage internal communication, and then use **default routing** or a **WAN link** to connect to the ISP router, allowing access to the internet and external services.

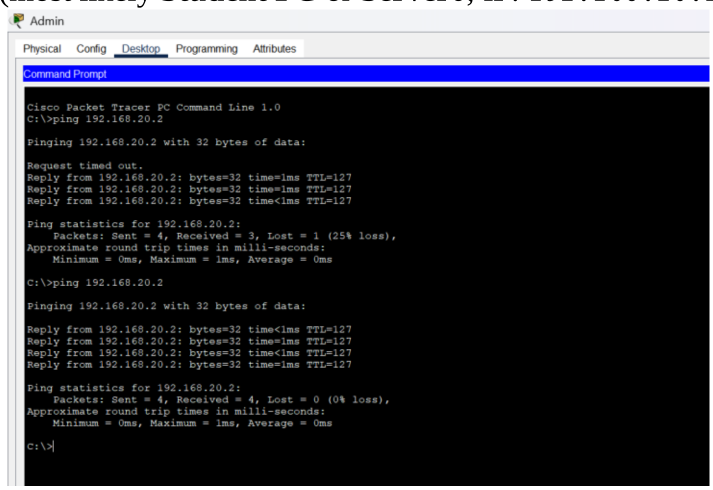
Figure 4: Routing Topology Setup



All devices are linked with green (active) **copper straight-through** connections. The topology represents a basic routing scenario where end devices communicate through a router to reach the server, typically across different subnets.

Figure 5: Ping Test from Admin PC

This screenshot shows the result of a successful `ping` test from **Admin PC** to another device (most likely **Student PC** or **Server0**, IP: `192.168.20.2`).



❖ Device & Server Configuration

We'll follow the exact detailed format of 1111.docx — with clear answers, Cisco Packet Tracer steps, and verification procedures.

1. Which servers did you configure (e.g., DHCP, FTP, DNS, Web)?

Answer:

The following servers were configured in the SERVER_VLAN (VLAN 50: 192.168.50.0/24):

- DHCP Server – Automatically assigns IP addresses to PCs in all VLANs.
- FTP Server – Provides file-sharing services to users.
- DNS Server – Resolves domain names into IP addresses.
- Web Server – Hosts internal university website.

All servers are assigned static IPs and connected to Switch SW1 via access port in VLAN 50.

2. Explain how you configured the FTP server and tested it

In this simulation, a single server was configured to provide FTP services. It was assigned a static IP address in the Server VLAN (VLAN 50: 192.168.50.0/24) and connected to the main switch. FTP service was enabled, and a user account was added. The server was tested from a PC in another VLAN using the ftp command from the command prompt to verify successful login and file transfer.

Figure 6: FTP Topology Setup

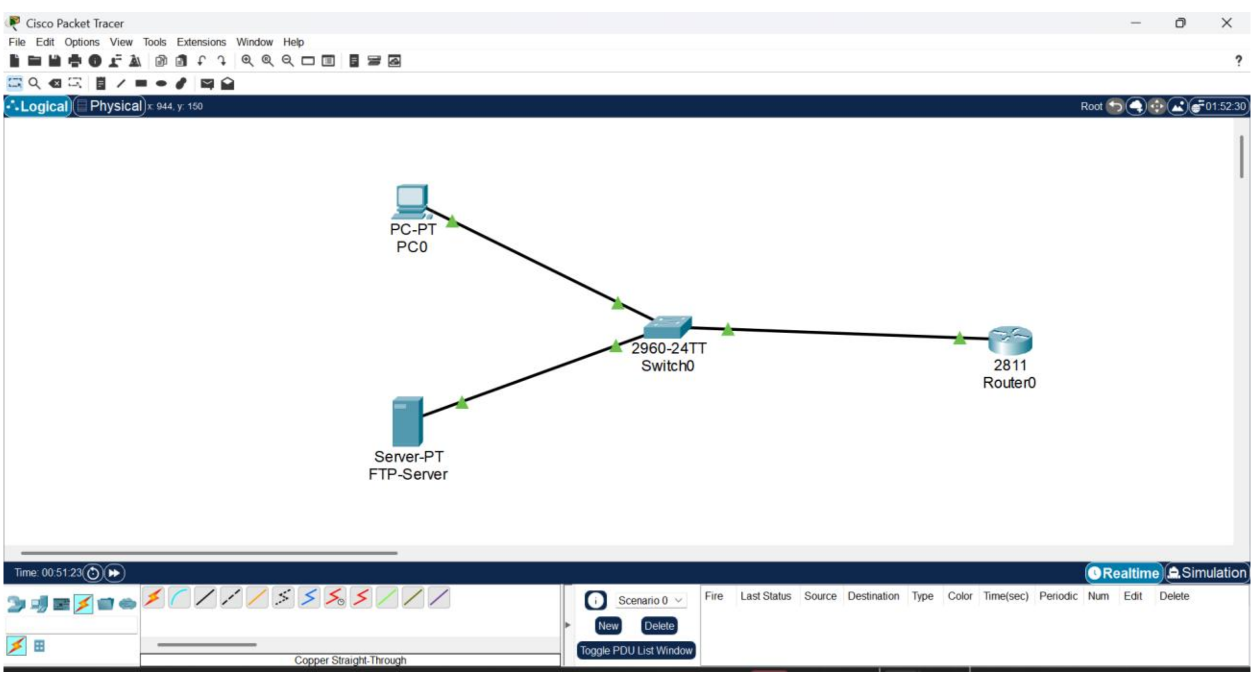


Figure 7: FTP Server Login and Directory Listing Test

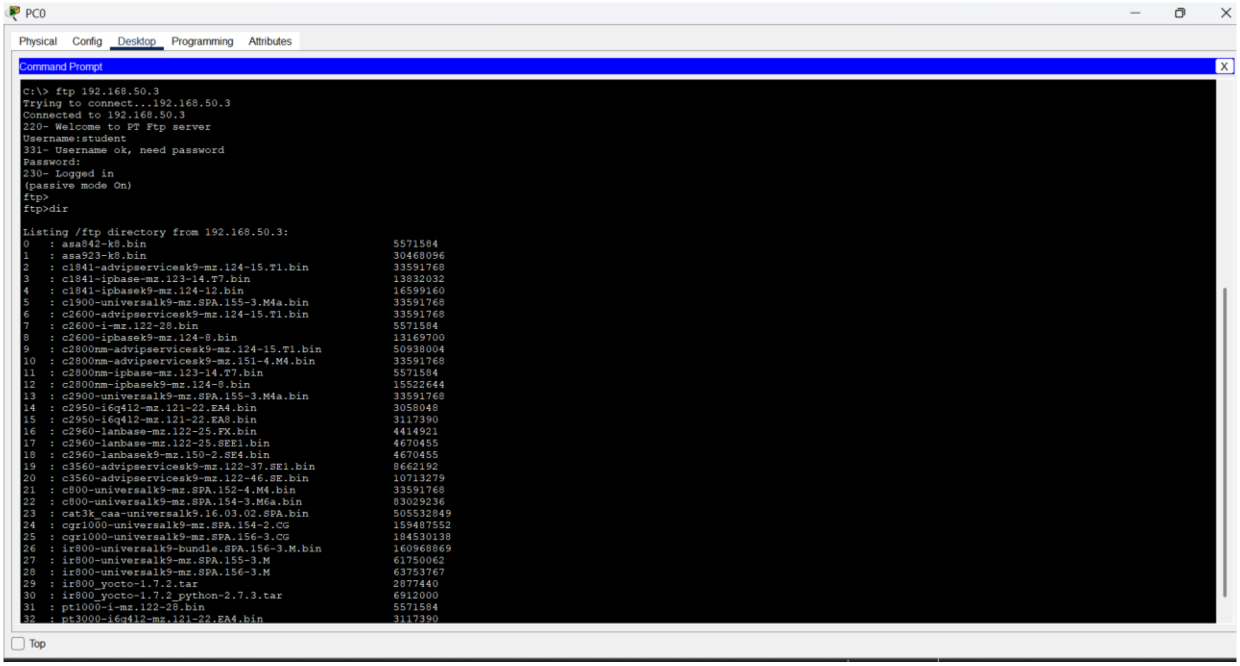


Figure 7: Successful FTP connection from the client PC to the FTP server (192.168.50.3) using the ftp command. The image shows that the user student logged in successfully and was able to execute the dir command to list available files on the server. This confirms both authentication and access to FTP server contents over the configured VLANs.

3.How does DHCP work in your network? Did you test automatic IP assignment?

The DHCP server was configured to automatically assign IP addresses to all PCs across VLANs. A static IP was given to the DHCP server in VLAN 50, and DHCP pools were created for each VLAN. Each PC was set to use DHCP, and they successfully received an IP address from the correct pool. This ensured automatic and centralized IP management.

Figure 8: DHCP Topology Setup

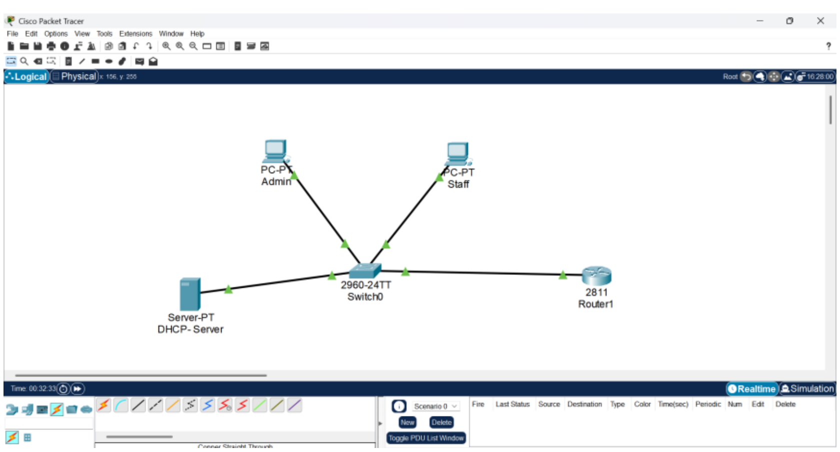


Figure 9: Ping Test Result From admin

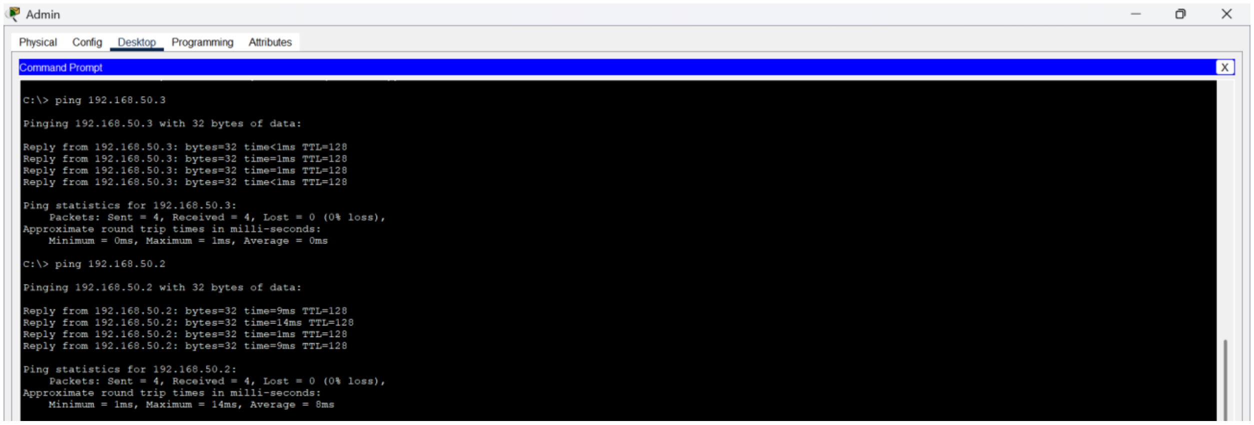
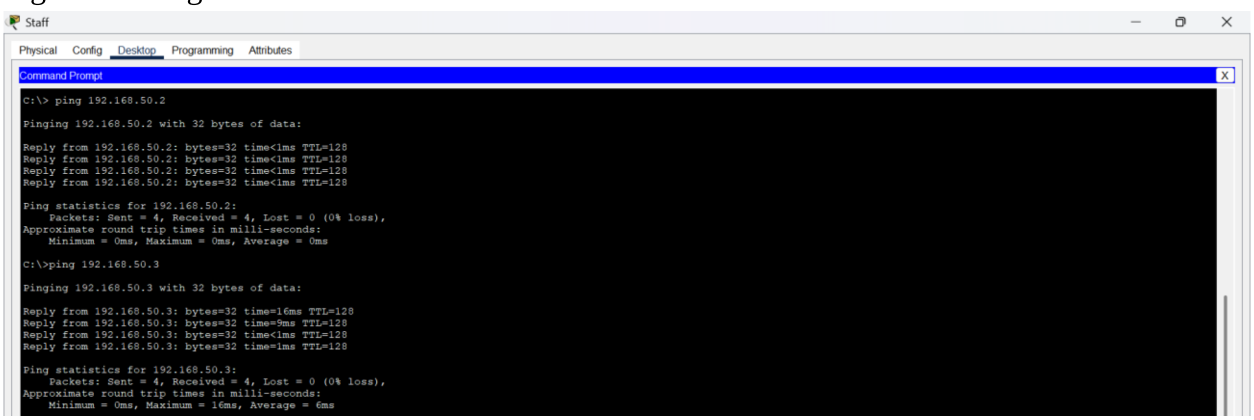


Figure 10: Ping Test Result From Staff



Conclusion from Ping Test Results

The successful ping replies from both the Admin and Staff PCs to the same target IP addresses — specifically 192.168.50.2 (DHCP server) and 192.168.50.3 (FTP server) — confirm that the devices received valid IP addresses via DHCP and were correctly placed in their respective VLANs. The consistent reply from both PCs to the same servers also demonstrates that inter-VLAN routing is fully functional, and the router is correctly forwarding packets between VLAN 10, VLAN 20, and VLAN 50.

Additionally, the fact that no packets were lost and all responses were received within minimal time validates the stability and performance of the network setup in this simulation.

❖ Troubleshooting & Testing

1: How did you verify inter-VLAN communication?

Inter-VLAN communication was verified using the ping command from the Admin PC (VLAN 10) to the Staff PC (VLAN 20), as well as to the DHCP and FTP servers in VLAN 50. All ping replies were successful with 0% packet loss, confirming that the router-on-a-stick configuration using subinterfaces was correctly implemented. This test confirmed that the router is routing traffic between VLANs properly.

2: How did you test connectivity to the internet (ISP router)?

In this simulation, the internet was represented by a second router (ISP). A default route was configured on the university router (R1) using the command ip route 0.0.0.0 0.0.0.0 200.200.200.1, pointing to the ISP's IP address. A ping test from a client PC to the ISP router was successful, confirming that unknown (external) traffic could reach the next hop through the default gateway.

3: What tools did you use inside Packet Tracer to test communication (e.g., ping, web browser)?

The main tools used for testing communication were:

- Command Prompt for ping and ftp commands.
- Web Browser (optional, for testing DNS and HTTP services).
- Simulation Mode, to visually inspect packet flow and detect dropped or misrouted packets.

These tools helped verify inter-VLAN routing, DHCP assignment, FTP access, and server reachability.

4: What is the role of a switch in your simulation?

The switch acted as the central connecting point for all devices in different VLANs. It handled frame forwarding, MAC address learning, and VLAN separation. It also provided a trunk link to the router, allowing tagged traffic to pass between the router and end devices via router-on-a-stick.

5: What is the purpose of Router-on-a-Stick?

Router-on-a-Stick enables a single physical interface on the router to route between multiple VLANs by using subinterfaces. In this simulation, subinterfaces for VLAN 10, 20, and 50 were created on fa0/0 with 802.1Q encapsulation. This allowed all VLANs to communicate through one router port while maintaining network segmentation.

6: Why is DNS important in the university network?

DNS is essential for translating human-friendly domain name (e.g.www.university.com](http://www.university.com)) into IP addresses (e.g., 192.168.50.3). It allows users to access services more easily and is necessary for both internal and external web communication. A local DNS server improves speed and reliability for internal services.

7: If you were to expand this network to multiple campuses, what would you change?

For a multi-campus setup, I would implement:

- Dynamic routing protocols like OSPF or EIGRP for scalable inter-campus routing.
- Multiple switches and routers with redundancy.
- VPN or leased line connections between campuses.
- Centralized servers with failover options.
- VLAN trunking over WAN links using router subinterfaces or Layer 3 switches.

This would ensure stability, scalability, and centralized control over a larger infrastructure.

8: What are the limitations of your current simulation?

- Single router and switch: No redundancy.
- No firewall or access control.
- No backup DHCP or DNS.
- Simulation-only: no external internet connection.
- No VLAN hopping or security filtering implemented.

9: What security measures would you implement to protect the servers and network?

- Enable port security on switch ports.
- Use Access Control Lists (ACLs) on the router to filter traffic between VLANs.
- Isolate servers in a dedicated VLAN.
- Use strong passwords and secure services (disable unused ones).
- Add a firewall or IDS between LAN and ISP.
- Regularly backup server configurations.

Figure 11: Inter-VLAN Connectivity and Server Reachability Test Result