National University
of computer and emerging sciences

DEPARTMENT OF ELECTRICAL ENGINEERING

DATA COMMUNICATION AND NETWORKS LAB (EL-2007)

PROJECT REPORT

"UNIVERSITY CAMPUS NETWORK"

- **GROUP MEMBERS:**
  1. SHAYAN HASHMI (22K-4865)
  2. SYED AMMAR ZULFIQAR (22K-4845)
  3. MUHAMMAD SUFYAN (22K-4868)

- **LAB INSTRUCTOR:**

  Engr. ZAKIR HUSSAIN

➢ INTRODUCTION:

A university campus network serves as the backbone for academic and administrative operations. It interconnects various departments, libraries, labs, and student facilities, ensuring the efficient flow of data and communication. The design of a robust campus network requires careful planning to accommodate future growth, prioritize security, and ensure reliable connectivity.

In this project, we utilize Cisco Packet Tracer, a powerful network simulation tool, to design and simulate the network. The primary goal is to implement a structured topology, enable VLAN segmentation, provide inter-VLAN routing, and integrate security mechanisms to prevent unauthorized access.

➢ ABSTRACT / PROBLEM STATEMENT:

The rapid growth of technology and its integration into educational institutions have created a need for efficient, scalable, and secure campus networks. This project focuses on designing and simulating a university campus network using Cisco Packet Tracer. The objective is to create a network that provides seamless communication among student departments, faculty, and HODs/Dean offices while ensuring data security and high availability. The network must support diverse devices, enable efficient resource sharing, and maintain optimal performance under varying load conditions.

This project focuses on creating a university campus network that fulfills the following requirements:

Requirements:

a) Main campus:

- Building A: Administrative staff in the departments of Computer Science and Software Engineering. The admin staff PCs are distributed in the building offices and it is expected that they will share some networking equipment.
- Building B: Faculty of Engineering, Cyber/AI and Fintech. The admin staff PCs are distributed in the building offices and it is expected that they will share some networking equipment.
- Building C: Students' labs, Cafe/Auditorium and One-Stop (Enquiry).
- There is also an email server hosted externally on the cloud.

b).

To configure the core devices and few end devices to provide end- to-end connectivity and access to the internal servers and the external server.

Each department/faculty will have its own separate IP network. The switches should be configured with appropriate VLANs and security settings.

RIPv2 will be used to provide routing for the routers in the internal network and static routing for the external server. The devices in building A will be expected to acquire dynamic IP addresses from a router-based DHCP server.

➢ METHODOLOGY (IMPLEMENTATION OVERVIEW):

1. Main Campus Router (Router 1):

Connected to a 3650 switch.

The 3650 switch connects to 8 2960 switches representing departments/buildings. Each switch has a PC and a printer.

2. Branch Network Router (Router 2):

Connected to another 3650 switch.

The switch is connected to 2 2960 switches for smaller campus offices, each having a PC and a printer.

3. Cloud Router (Router 3):

Directly connected to an email server hosted externally.

- **<u>Main Campus:</u>**

Building A:

Computer Science and Software Engineering admin staff are covered.

Ensure shared networking equipment (e.g., printers) is accessible for both departments.

Building B:

Includes admin staff for Engineering, Cyber/AI, and FinTech.

Your setup covers these through the switches, but VLAN separation for departments may be necessary.

Building C:

Covers Labs, Cafe/Auditorium, and Enquiry.

This is represented, but the cafe/auditorium might need fewer devices, primarily for shared access.

- **<u>Smaller Campus:</u>**

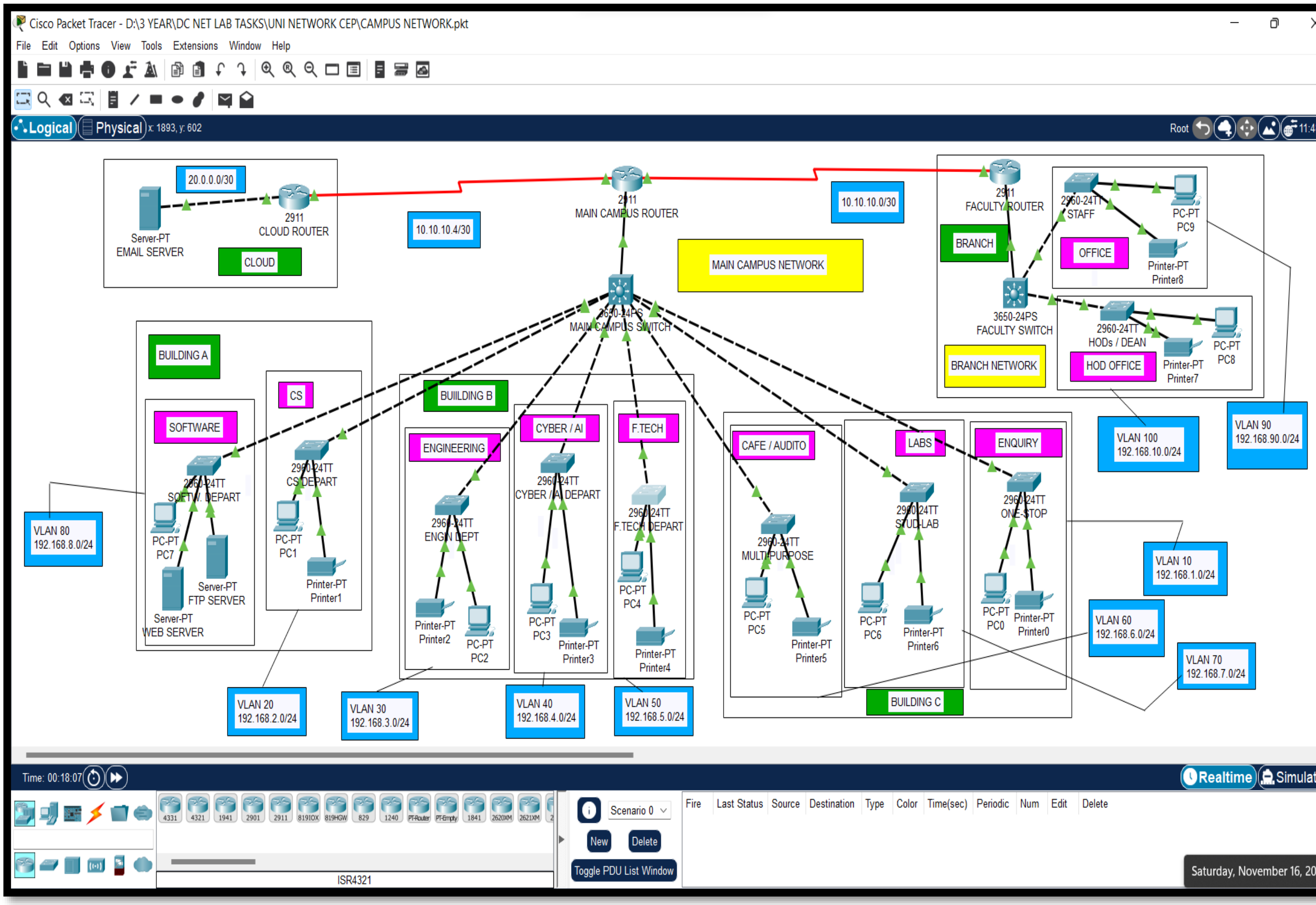
Faculty and HODs/Dean offices:

Properly separated using VLANs or switches for each floor.

- **<u>Email Server:</u>**

Hosted externally via the cloud router, as required.

- **NETWORK DESIGN:**



- **Why Use the 2911 Router?**

The Cisco 2911 router is designed for mid-sized enterprise networks, making it ideal for managing the complex interconnections between your main campus, branch campus, and external cloud.

With support for high-speed data transfer, it ensures efficient routing for the devices and VLANs across your network.

It is suitable for expanding networks, making it a good choice for your future needs if the campus grows or new branches are added.

- **<u>Why Use the 3650 Switch</u>**

  The Cisco 3650 switch is a Layer 3 switch, which means it can perform routing functions. This reduces the load on the router for inter-VLAN communication within the main campus.

  As a central switch, it efficiently aggregates traffic from the 2960 switches and forwards it to the router or other network segments.

- **<u>Why This Combination?</u>**

  Cisco 2911 Router: Handles WAN connectivity, inter-campus communication, inter-VLAN routing, and external cloud access.

  Cisco 3650 Switch: Acts as the central hub for connecting multiple departments and devices while providing advanced Layer 3 switching, scalability, and efficient traffic management.

- **<u>HWIC-2T Module in the Router:</u>**

  The **HWIC-2T (High-Speed WAN Interface Card, 2-Port Serial)** module provides additional serial ports for your Cisco 2911 router. Here's why you used it:

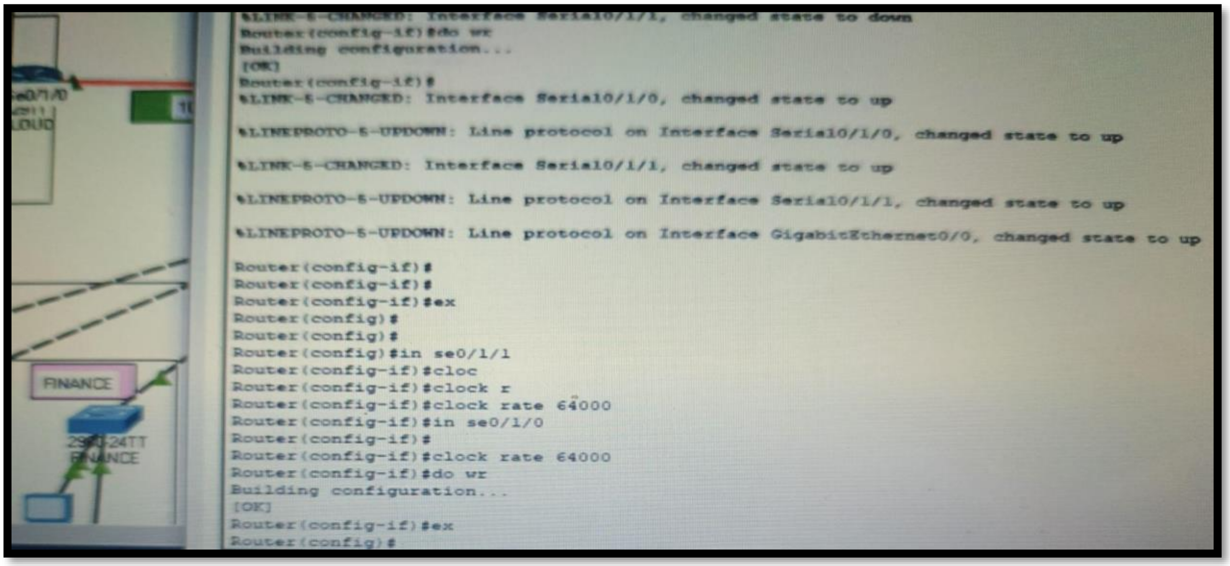
  The HWIC-2T allows the router to connect to legacy serial WAN links (e.g., leased lines, Frame Relay, or MPLS circuits). If your network includes such a WAN technology, this module is essential for connecting external sites or legacy infrastructure.

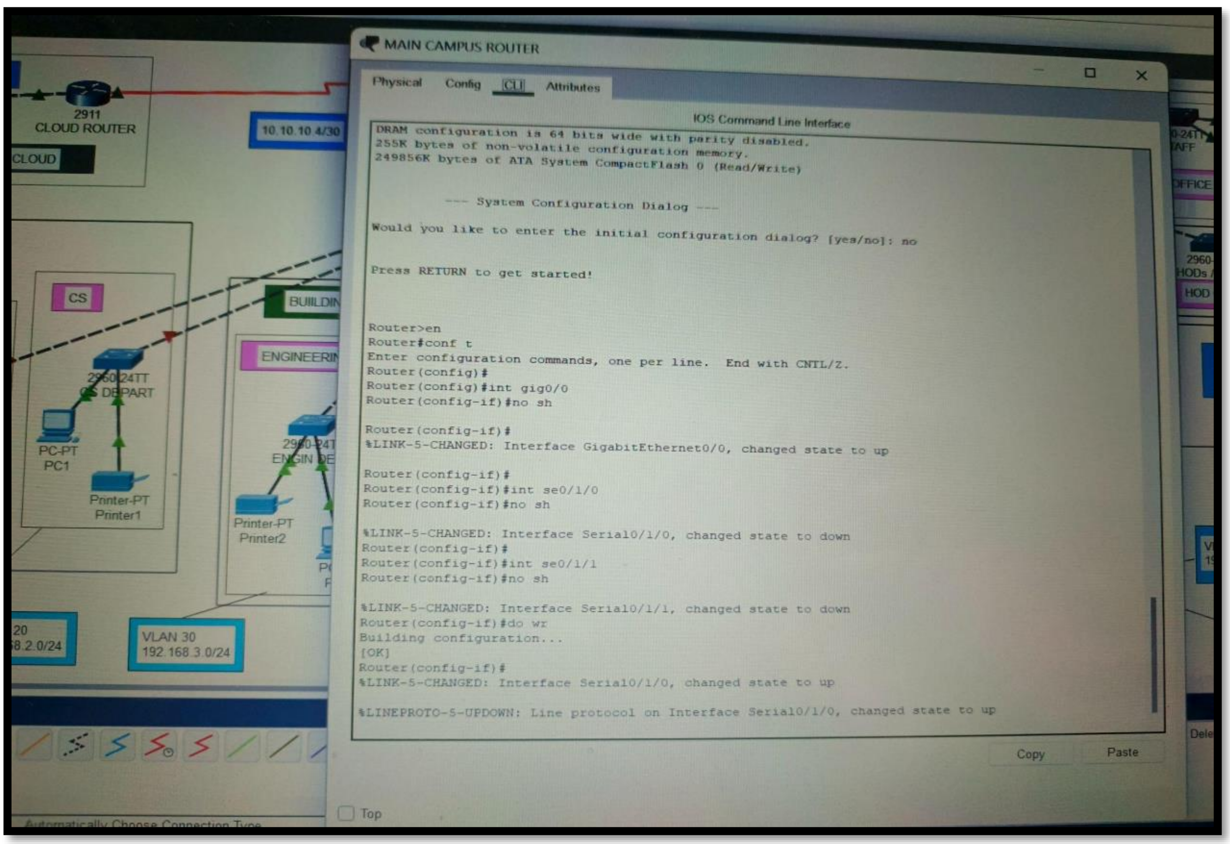
- **<u>AC Power Supply in the Switch:</u>**

  The **AC power supply** for your Cisco 3650 switch was chosen for the following reasons:

  The switch needs a stable power source to operate. Since most enterprise environments have AC power readily available, using an AC power supply is standard.

➢ SIMULATION RESULTS:





- **<u>Image 1: CLOCK RATE CONFIGURATION:</u>**

1. **Serial Interface:**

   Mention**s <u>interface serial 0/1/1</u>** and **<u>serial 0/1/0</u>** states transitioning between up and down. This indicates you're activating these interfaces for connectivity.

2. **Clock Rate Command:**

   This is used to configure the clock rate on the DCE (Data Communication Equipment) side of the serial connection.

   One end of a serial link (usually the DCE side) provides the clock signal to synchronize data transmission between the two devices.

   Serial0/1/1 and Serial0/1/0 are being configured with the same **clock rate 64000**, which is typical for standard synchronous serial communication.

3. **Why Needed?**

   Without a clock rate, the serial link will not function because the router won't generate timing for data transmission on the DCE side.

- **<u>Image 2: MAIN CAMPUS ROUTER CONFIGURATION:</u>**

1. **Gigabit Ethernet Interface Activation:**

   Command: int gig0/0 followed by no shutdown

   Line protocol on **Interface Gigabit Ethernet0/0**, changed state to up

   This enables the Gigabit Ethernet 0/0 interface. It's likely being used to connect the router to a core switch (e.g., Cisco 3650).

   This confirms the interface is now operational.

2. **Serial Interface Activation:**

   Command: int serial 0/1/1 and serial 0/1/0 followed by no shutdown.

Line protocol on Interface Serial0/1/0, changed state to up

These commands activate the serial interfaces for WAN or inter-campus connections.

Indicates that the serial connection has been successfully activated.

3. **Saving Configuration:**

   Command**: <u>do wr (write).</u>**

   Saves the current configuration to the router's non-volatile memory, ensuring it persists after a reboot.

- **<u>Additional Configuration: Cloud Router and Branch Campus Router:</u>**

  We performed the same steps on the cloud router and the branch campus router, configuring their Gigabit Ethernet and serial interfaces to ensure smooth connectivity between the main campus, branch campus, and the cloud server.

- **<u>Creating VLANS:</u>**

  VLANs 10, 20, 30, 40, 50, 60, 70, and 80 are created and assigned to specific switch ports.

  The comman D **switch port mode access** is used to configure the ports as access ports for these VLANs.

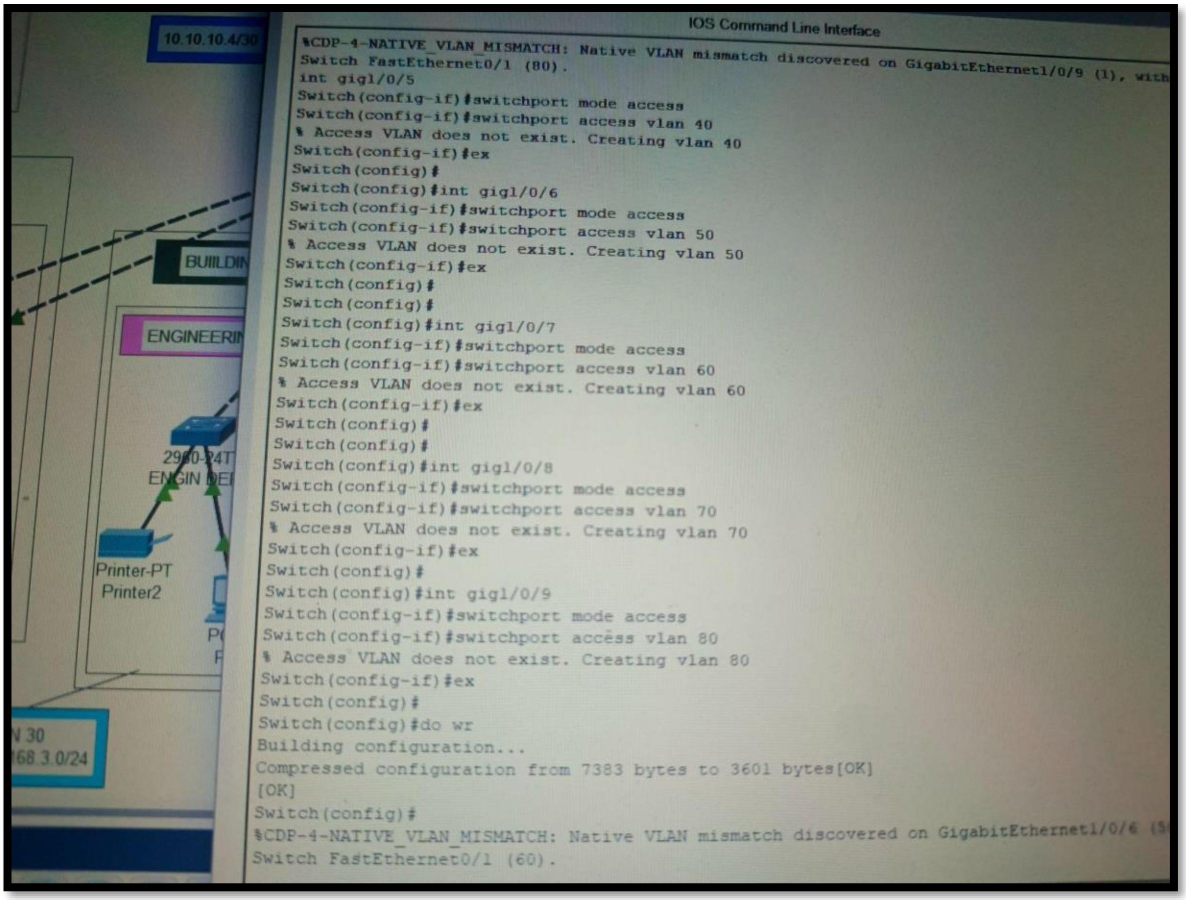
Assigning VLANs:

Specific interfaces (e.g. GigabitEthernet1/0/5, GigabitEthernet1/0/6 etc. are assigned to their respective VLANs using switch port access VLAN 50 or 60.

Saving Configuration:

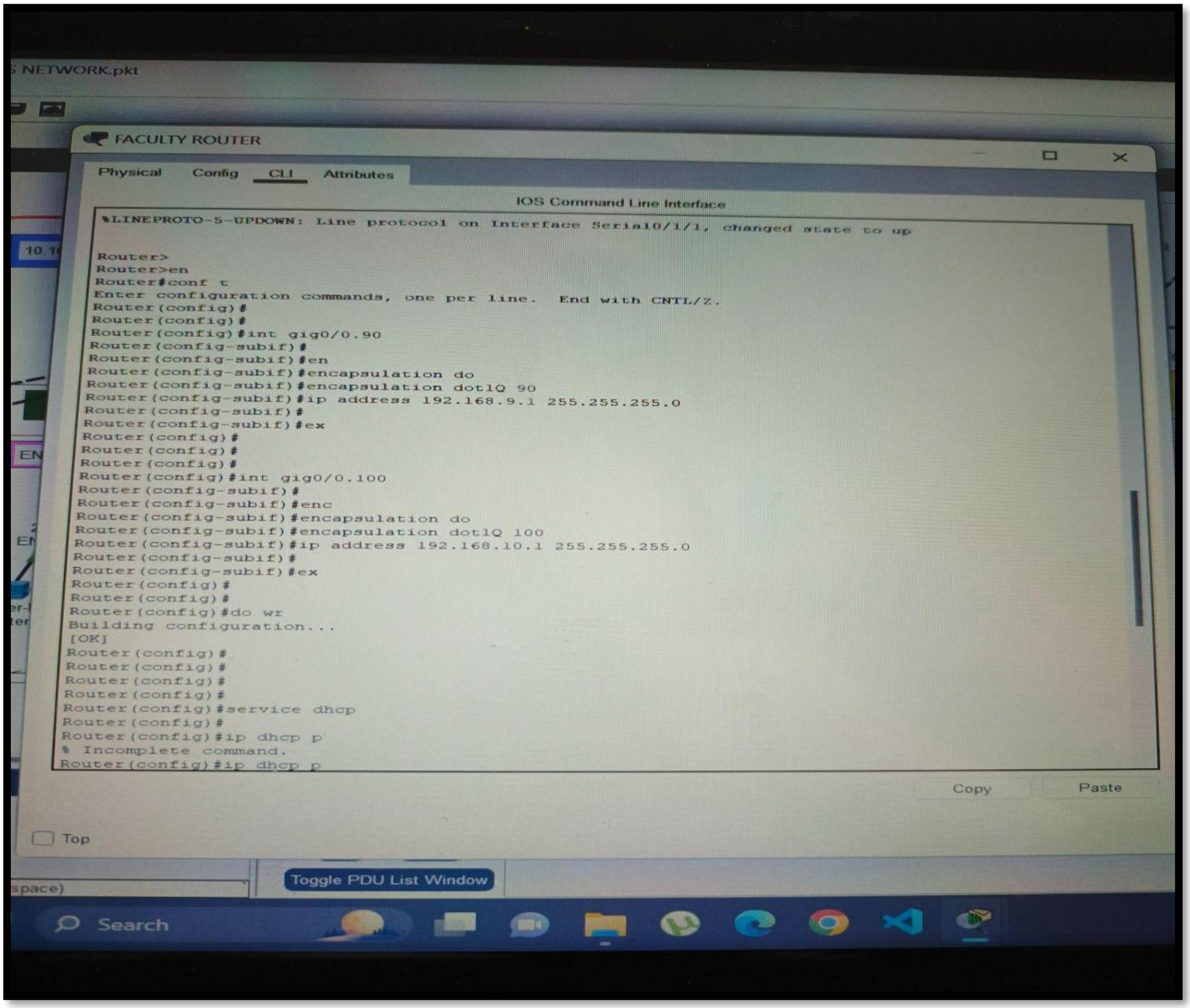
Command: do wr.

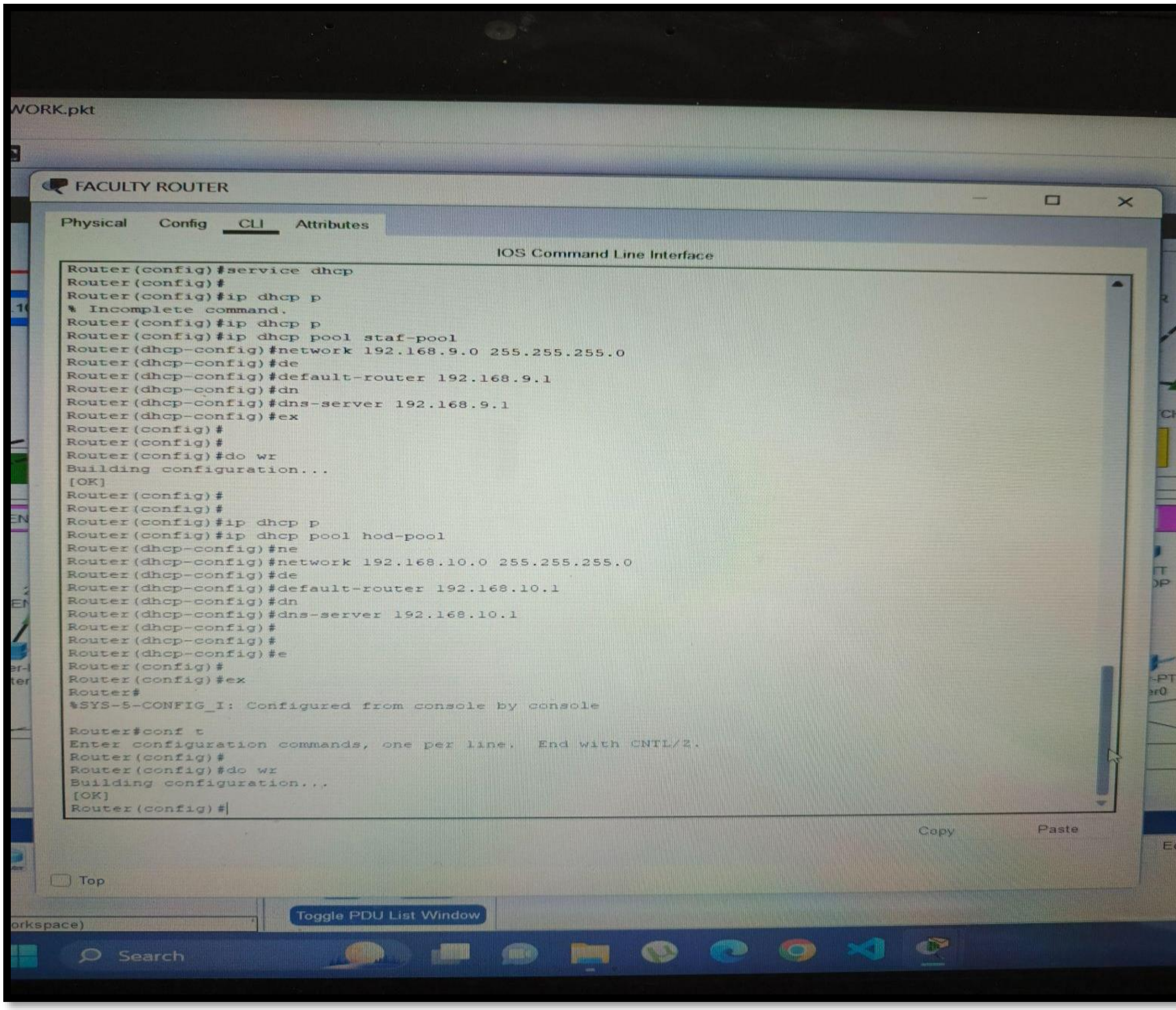
All configuration changes are saved to the switch's memory to ensure persistence after a reboot.




```
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet1/0/9 (1), with
Switch FastEthernet0/1 (80).
int gig1/0/5
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 40
% Access VLAN does not exist. Creating vlan 40
Switch(config-if)#ex
Switch(config)#
Switch(config)#int gig1/0/6
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 50
% Access VLAN does not exist. Creating vlan 50
Switch(config-if)#ex
Switch(config)#
Switch(config)#
Switch(config)#int gig1/0/7
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 60
% Access VLAN does not exist. Creating vlan 60
Switch(config-if)#ex
Switch(config)#
Switch(config)#
Switch(config)#int gig1/0/8
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 70
% Access VLAN does not exist. Creating vlan 70
Switch(config-if)#ex
Switch(config)#
Switch(config)#int gig1/0/9
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 80
% Access VLAN does not exist. Creating vlan 80
Switch(config-if)#ex
Switch(config)#
Switch(config)#do wr
Building configuration...
Compressed configuration from 7383 bytes to 3601 bytes[OK]
[OK]
Switch(config)#
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet1/0/6 (5
Switch FastEthernet0/1 (60).
```

- <u>**NETWORK CONFIGURATION ON FACULTY ROUTER:**</u>




FACULTY ROUTER
Physical
Config
CLI
Attributes
IOS Command Line Interface
Router(config)#service dhcp
Router(config)#
Router(config)#ip dhcp p
% Incomplete command.
Router(config)#ip dhcp p
Router(config)#ip dhcp pool staf-pool
Router(dhcp-config)#network 192.168.9.0 255.255.255.0
Router(dhcp-config)#de
Router(dhcp-config)#default-router 192.168.9.1
Router(dhcp-config)#dn
Router(dhcp-config)#dns-server 192.168.9.1
Router(dhcp-config)#ex
Router(config)#
Router(config)#
Router(config)#do wr
Building configuration...
[OK]
Router(config)#
Router(config)#
Router(config)#ip dhcp p
Router(config)#ip dhcp pool hod-pool
Router(dhcp-config)#ne
Router(dhcp-config)#network 192.168.10.0 255.255.255.0
Router(dhcp-config)#de
Router(dhcp-config)#default-router 192.168.10.1
Router(dhcp-config)#dn
Router(dhcp-config)#dns-server 192.168.10.1
Router(dhcp-config)#
Router(dhcp-config)#
Router(dhcp-config)#e
Router(config)#
Router(config)#ex
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#do wr
Building configuration...
[OK]
Router(config)#
Copy
Paste
Top
Toggle PDU List Window
Search

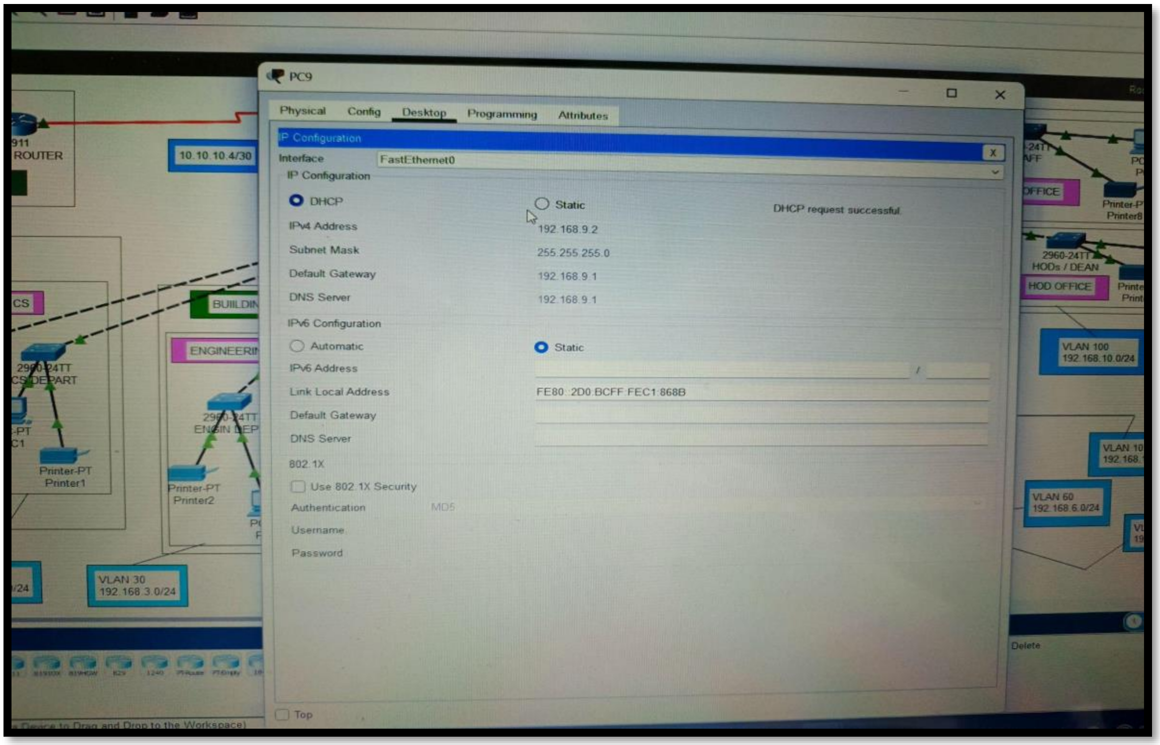


Image 1 (Starting Point)

The router is configured to enable inter-VLAN communication:

Sub-interfaces are created on GIGABITETHERNET0/0 for VLANs:

VLAN 90 is configured with **192.168.9.1/24**

VLAN 100 is configured with **192.168.10.1/24**

The **dot1q encapsulation** is used to tag VLAN traffic, enabling the router to handle traffic for each VLAN.

Image 2 (DHCP Configuration)

Next, DHCP pools are created on the router to automate IP allocation:

STAFF Pool (VLAN 90):

Network: **192.168.9.0/24**

Gateway: **192.168.9.1**

DNS Server: **192.168.9.1**

HOD Pool (VLAN 100):

Network: **192.168.10.0/24**

Gateway: **192.168.10.1**

DNS Server: **192.168.10.1**

The DHCP service ensures devices in both VLANs get their respective IP configurations automatically.

Image 3 (End Point)

A PC (PC9) in VLAN 90 is shown with its static IP configuration:

IP Address: **192.168.9.2**

Gateway: **192.168.9.1**

This demonstrates the setup is functional, but in practice, DHCP would assign these settings dynamically unless static IPs are explicitly needed. Same as on PC8.

Purpose of This Sequence:

Image 1 sets up VLAN routing.

Image 2 adds DHCP to simplify IP management.

Image 3 verifies device configuration within the network.

Why configure VLANs and sub interfaces?

Network Segmentation: VLANs (e.g., STAFF, HOD) separate network traffic for different departments or purposes, improving security and organization.

Inter-VLAN Routing: By configuring sub interfaces on the router with dot1q encapsulation devices in different VLANs can communicate through the router.

Efficient Use of IPs: Each VLAN gets its own IP range (e.g. 192.168.9.0/24, and 192.168.10.0/24), avoiding IP conflicts and maintaining clear traffic boundaries.

Why use DHCP?

Automated IP Assignment: DHCP eliminates the need to manually assign IP addresses to every device. It dynamically provides IPs, subnet masks, gateways, and DNS information.

Saves Time and Reduces Errors: In large networks with many devices, manual configuration is tedious and prone to mistakes. DHCP simplifies this.

- **NETWORK CONFIGURATION ON MAIN CAMPUS ROUTER:**

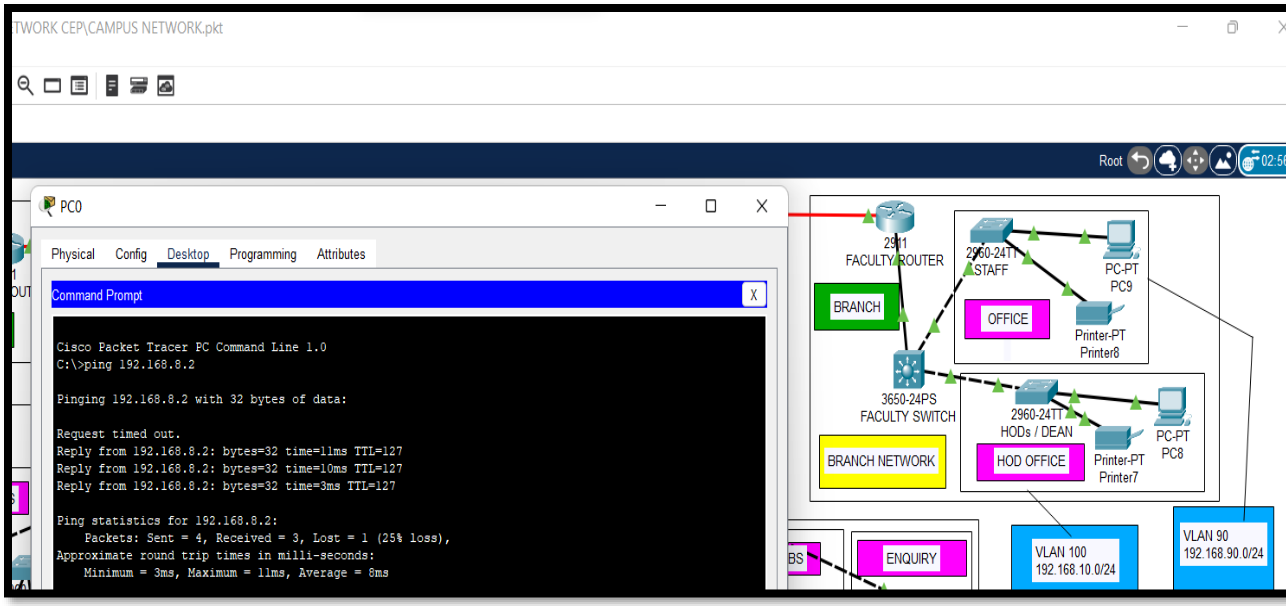
  On the Main Campus Router, the same setup would be applied to support all 8 switches and VLANs (10-80).
  Sub-Interfaces Configuration: Sub-interfaces for each VLAN (10-80) will be created on the router, each with its own IP address to act as the default gateway for that VLAN.

  DHCP Pools: Separate DHCP pools will be configured for each VLAN to automatically assign IP addresses, gateways, and DNS information to devices in their respective VLANs.

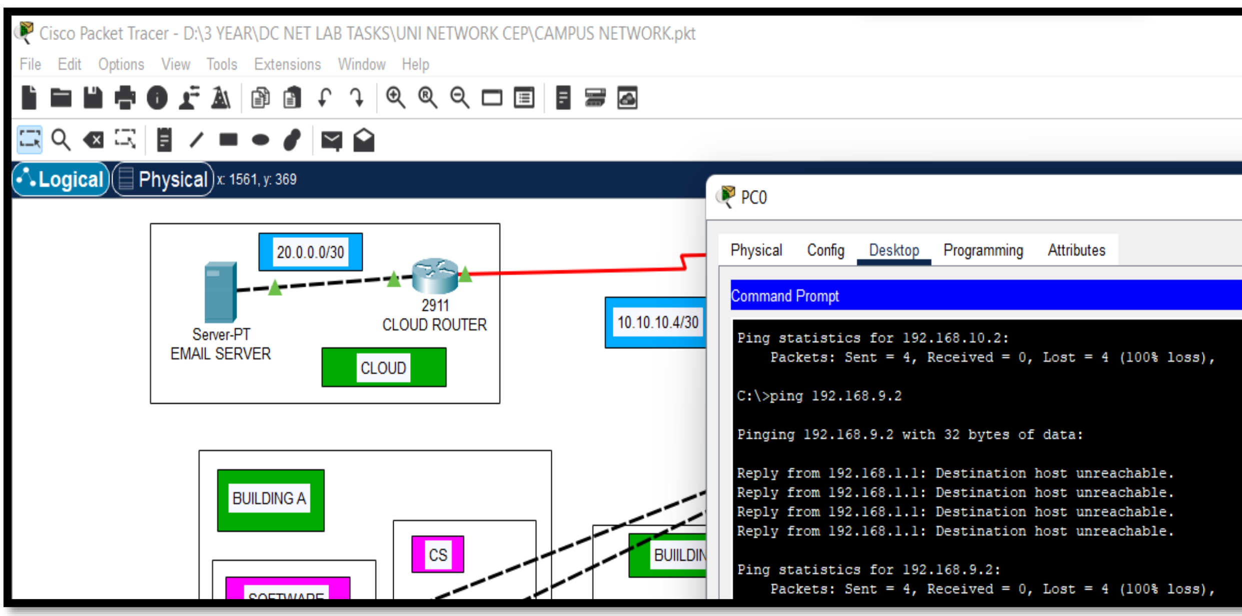
  Trunk Links: The router will be connected to all 8 switches via trunk ports, allowing it to manage traffic for all VLANs.

  Outcome: Devices in all VLANs will have inter-VLAN communication via the router, with dynamic IP allocation ensuring efficient and scalable network management.

- **PINGING :**



Pinging was successful from PC0 to PC8 by pinging the PC8 IP address i.e. **192.168.8.2.**

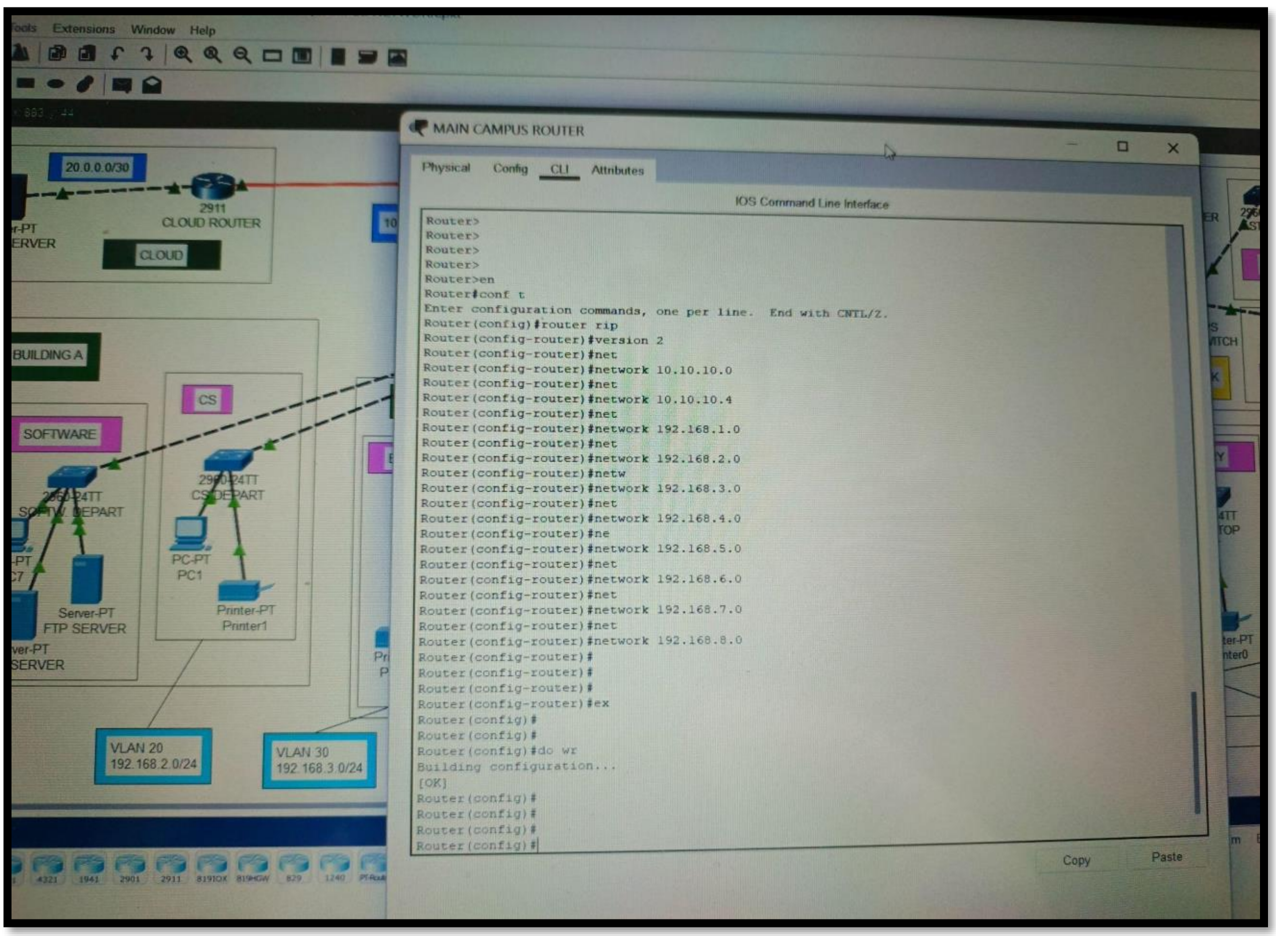


Problem:

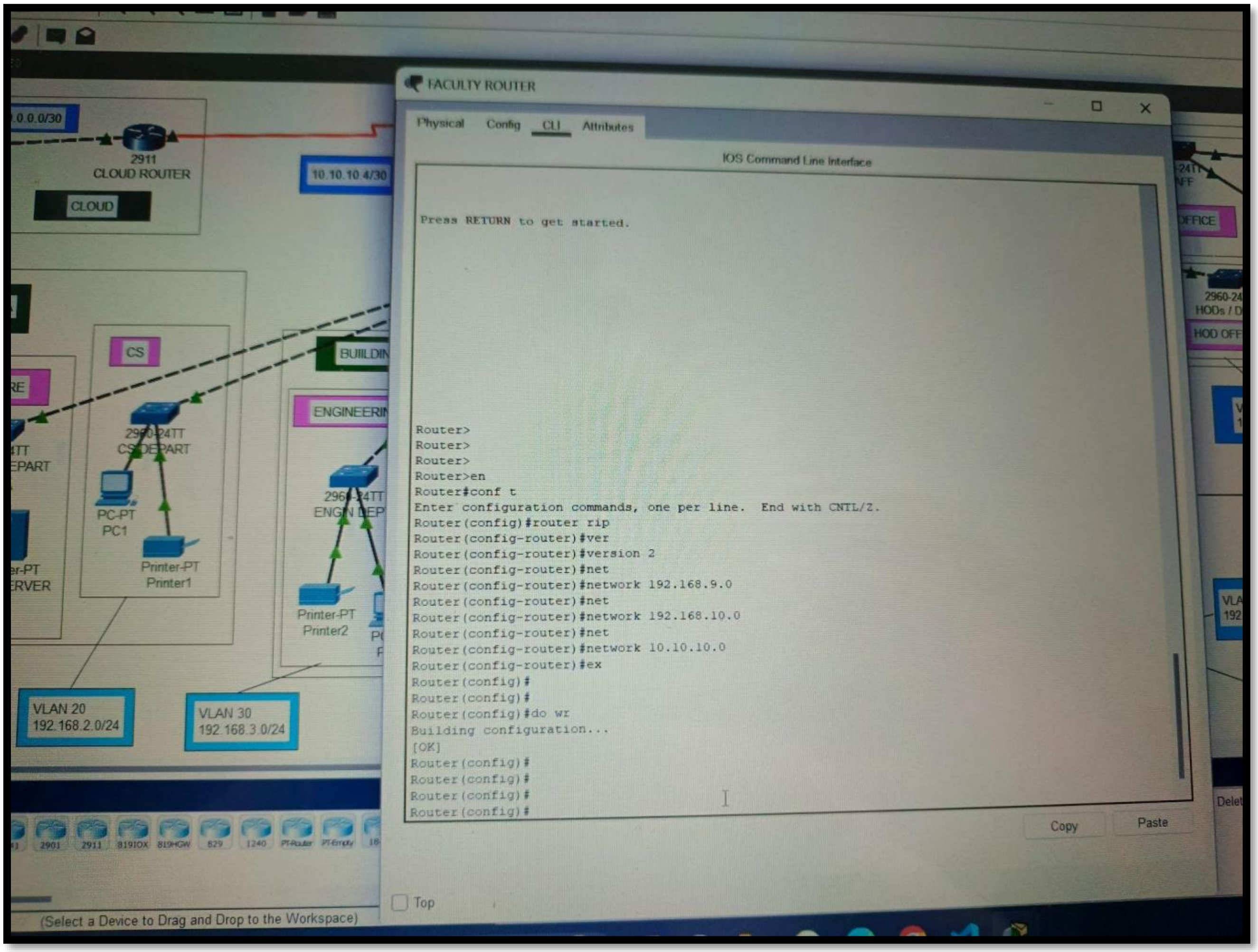
As we are working with 3 routers (Main Campus Router, Faculty Router and Cloud Router) each having their respective PCs which they are connected to. We want each PC to be able to ping the other PC, but
facing the "Destination Host Unreachable" message (assuming we have done the router and IP configuration of PCs correctly otherwise we have to check that as well too).

Enable and Configure RIP on All Routers:
You need to configure RIP on each router to dynamically share routing information between routers.
Here’s the configuration you need to apply on each router:

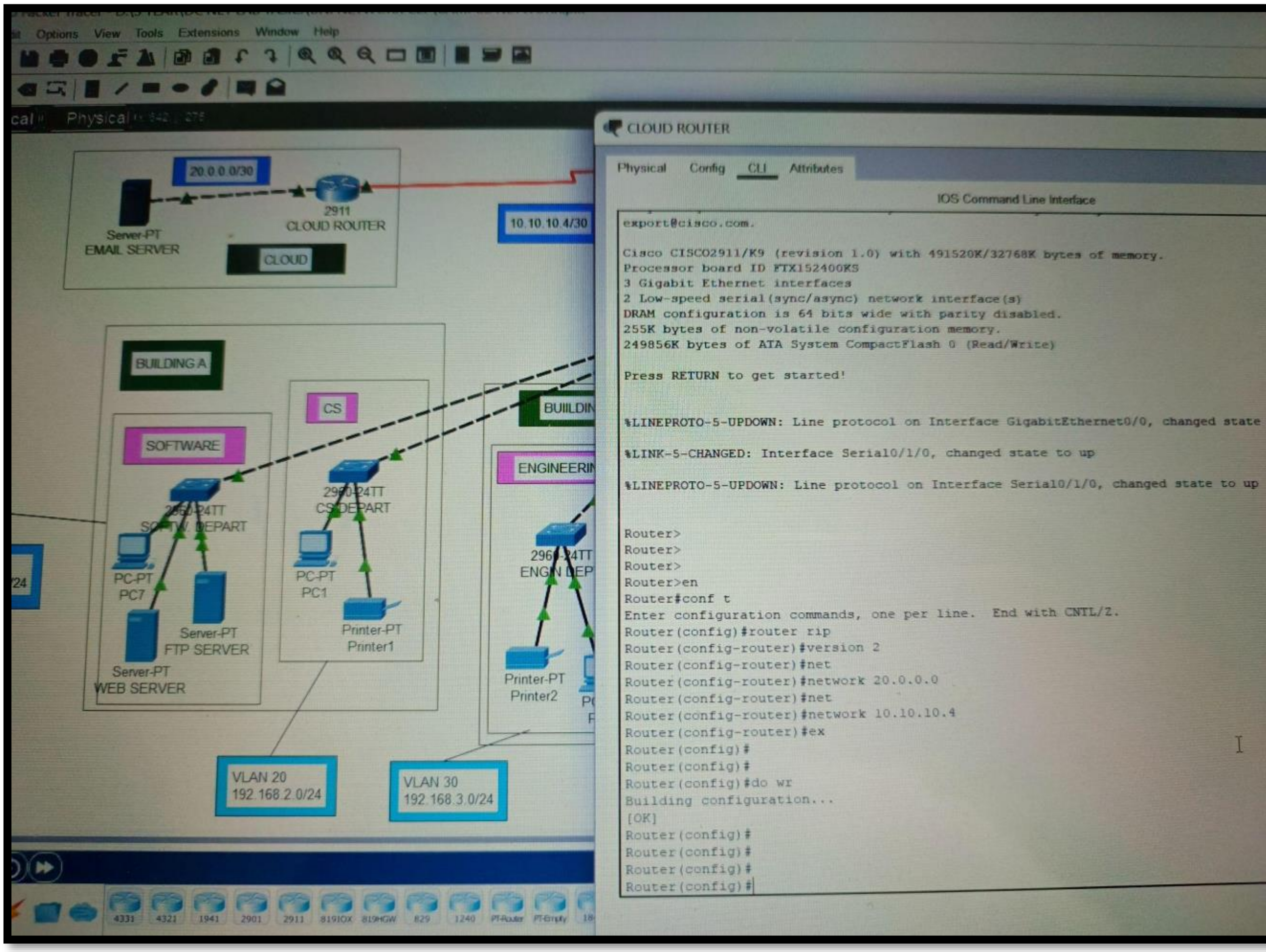
- **Main Campus Router:**



- **Faculty Router:**



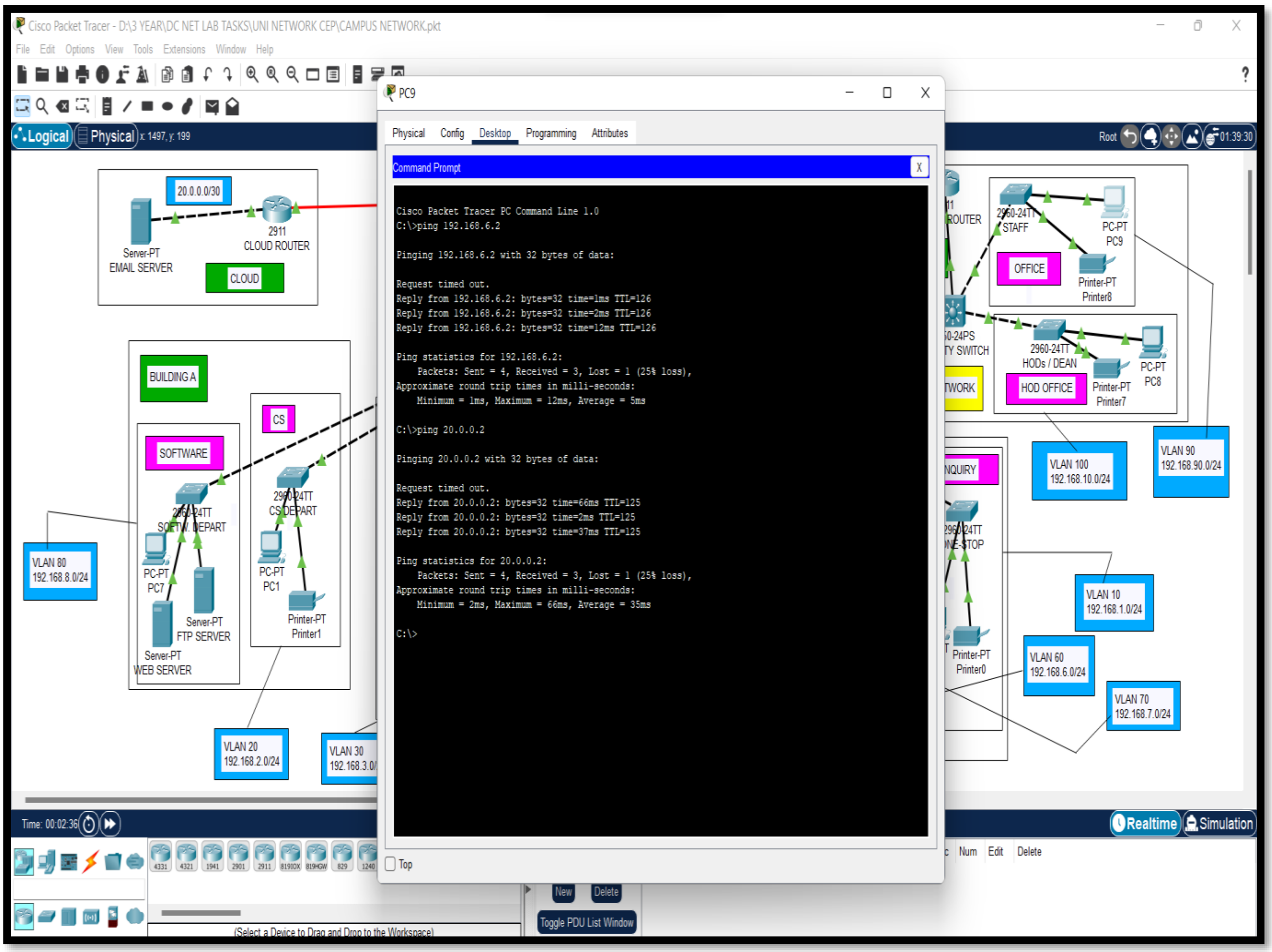
- **Cloud Router:**



Test Connectivity:

Once RIP is configured and the routers are correctly advertising routes, try to ping from each PC to the others to any of the router's PCs.

Let's try to ping PC5 of the Main Campus Router and Server of Cloud router from the Faculty Router's PC9.



Pinging was successful from PC9 to PC5 IP address i.e. **192.168.6.2.**
Pinging was successful from PC9 to Server IP address i.e. **20.0.0.2.**

➢ SDGs:

- **SDG 4 - Quality Education:** A robust campus network facilitates access to online educational resources, digital libraries, and e-learning platforms, ensuring students and staff can collaborate effectively and access quality education.

- **SDG 9 – Industry, Innovation And Infrastructure:** The network represents innovative infrastructure that supports a smart campus, enabling seamless communication and fostering technological advancements in education and research. Emphasize the use of VLANs and advanced switching/routing technologies as part of building a resilient and forward-thinking digital infrastructure.