

**COMPUTER NETWORKS**

**FINAL PROJECT REPORT**

SUBMITTED TO:

**DR. MARIUM AKBAR**

By:

**Muhammad Ahmad FA23-BDS-048**

**Huzaima Imtiaz FA23-BDS-017**

JUNE 12, 2025.

hgf



Table of Contents

[**PHYSICAL NETWORK ARCHETICTURE**](#_Toc195219414)

1. Introduction **…………………………………………………………………………………………………..… 3**

2. Problem Statement **………………………………………………………………………………………….….. 3**

3. Problem Solution **…………………………………………………………………………………………….… 3**

4. Related System Analysis **…………………………………………..……………………………………….….. 4**

5. Vision Statement **…………………………………………....…………………………………………….….... 4**

6. Scope of project **……………………………………………………………………………………………….. 4**

7. Network Structure Overview **………………………………………………………………….………………. 5**

* 1. Cloud **…………………………………………………………………………………….………………. 5**
  2. ISP Router [**….....………………………………………..…………………...………….….……………..**](#_Toc195219415) **5**
  3. Main Router (Router0)  [**…...………..…………………..……………………………...….……………...**](#_Toc195219415) **5**
  4. Core Switch (or Multilayer Switch)  [**…...………………..…………..…………………….……...……...**](#_Toc195219415) **5**
  5. Wireless Access Point [**…...……………..…………………..………………………………....……..…...**](#_Toc195219415) **5**
  6. End Devices (PCs, Printers, etc.) [**…...…….………………...……..………………..…………………....**](#_Toc195219415) **6**

8. System Limitations **…………...……………………………………………………………………………….. 6**

9. Tools and Technologies **………………………………………………………………………………….……. 7**

10. Project Stakeholders **…………………………………………………………………………………….…….. 7**

11. Configurations with snapshots **………………………………………………………………………….…….. 7**

* 1. Inter-VLAN Routing **…………………………………………………………...………………….…….** **7**
  2. DHCP Configuration **…………………………………………………………………...……………......** **9**
  3. Routing Information Protocol(RIP) **…………………………………….…………………...………….** **10**
  4. NAT **………………………………………………………………………………………….…………** **10**
  5. ACL Configuration **……………………………………………………………...………………….......** **11**
  6. WAP for Guest User **………………………………………………………...…………………………. 11**

12. Testing of all configurations **…………………………………………………………………………………. 11**

* 1. nter-VLAN Routing **……………………………………………………………………………………. 11**
  2. DHCP Configuration **……………………………………………………………………...……………. 12**
  3. Routing Information Protocol(RIP) **…………………………………….………………………...…….. 12**
  4. NAT **………………………………………………………………………………………….…...…….. 12**
  5. ACL Configuration **……………………………………………..………………………………...…...... 12**
  6. WAP for Guest User **…………………………………………………..………………………...……… 13**

13. [Justification](#_Toc195219415) **…………………………………………………………………………………………………... 13**

* 1. Inter-VLAN Routing **………………………………….……………..………………………………….** **13**
  2. DHCP **………………………………………………………………………..…………………………. 13**
  3. RIP **…………………………………………………………….………………….…………………..… 13**
  4. NAT **………………………………………………………………………….……….………………… 13**
  5. ACL **………………………………….……………………………………………..………………....... 14**
  6. WAP for guest users **…………………………………………….……………………….…………...… 14**
  7. Firewall Rules **………………………………………………….……………………………….………. 14**

14. Conclusion **……………………………………………………………………………………………………. 14**

# **PHYSICAL NETWORK ARCHETICTURE**

## ****Introduction****

This project involves designing and implementing a secure enterprise-level network using Cisco Packet Tracer. It connects multiple departments IT, Sales, HR, and Guest, through VLANs and central networking devices, including routers, switches, and wireless access points. The topology is designed to allow structured internal communication, controlled inter-departmental access, and simulated internet connectivity. Each department is assigned a specific subnet for logical separation and easier network management:

* **IT Department:** 192.168.10.0/24
* **Sales Department:** 192.168.20.0/24
* **HR Department:** 192.168.30.0/24
* **Guest Network:** 192.168.40.0/24

All devices are connected through a central **multilayer switch**, with a **2911 router** providing internet access, and a **WRT300N wireless router** handling guest connections

## ****Problem Statement****

The organization requires a logically segmented and secure internal network for managing multiple departments while ensuring restricted communication between them. It must support internet access, dynamic IP addressing, departmental isolation using VLANs, and guest wireless access with limited privileges. The network should also be scalable, easy to manage, and demonstrate enterprise-grade practices such as NAT, ACLs, and dynamic routing.

## ****Problem Solution****

A departmental network was designed and implemented using Cisco Packet Tracer with the following features:

* **VLANs** were created for each department to ensure logical separation.
* **Inter-VLAN routing** was enabled via a multilayer switch.
* **ACLs** were applied to restrict inter-department access, such as blocking Sales from accessing IT resources.
* **DHCP** was used for automatic IP assignment across all VLANs.
* **NAT** and **RIP routing** were configured on the router to provide external connectivity via the simulated cloud.
* **Wireless Access Point** was added for Guest users to isolate them from internal departments.

This setup supports secure, segmented, and scalable communication in a virtual enterprise network.

## ****Related System Analysis****

Modern enterprises rely on logically segmented, scalable, and secure networks to ensure efficient communication across departments. The system developed in this project emulates a real-world organizational setup using Cisco Packet Tracer. It separates departments (IT, HR, Sales, and Guest) into individual VLANs to reduce broadcast domains and enforce access control policies. Each department operates within its IP subnet, which improves network manageability and enhances security. To enable necessary communication between departments, **inter-VLAN routing** is implemented using a **multilayer switch**. **Access Control Lists (ACLs)** are deployed to restrict unauthorized access, for instance, preventing the Sales department from accessing IT resources. To simplify IP management, a **DHCP server** is used for dynamic address allocation. The **RIP protocol** is applied between the internal router and ISP router to propagate routes dynamically. Additionally, **Network Address Translation (NAT)** allows internal hosts with private IP addresses to access simulated internet services via a single public IP address through the ISP router. The **Guest VLAN** is managed using a **wireless access point (WAP)**, keeping guest devices isolated from the internal network while still allowing internet access. This architecture models enterprise-level practices such as departmental segmentation, network policy enforcement, and secure connectivity, providing a realistic simulation of business network infrastructure.

## ****Vision Statement****

## To design and implement a secure, scalable, and logically segmented enterprise network that supports structured communication between departments, enforces access control policies, provides dynamic IP management, enables internet connectivity, and simulates real-world networking principles using Cisco Packet Tracer. The project aims to reflect best practices in enterprise networking by integrating VLANs, inter-VLAN routing, ACLs, DHCP, NAT, and RIP within a unified architecture, ensuring both functionality and security for all organizational units including guest users.

## ****Project Scope****

This project focuses on the simulation and configuration of a departmental enterprise network using Cisco Packet Tracer. The network includes logical segmentation through VLANs for four main entities: IT, HR, Sales, and Guest users. It implements:

* **VLANs** to ensure isolated broadcast domains and secure department-wise communication.
* **Inter-VLAN Routing** via a multilayer switch to allow controlled communication between departments.
* **Access Control Lists (ACLs)** to enforce security policies and restrict unauthorized access for example, blocking Sales from accessing IT.
* **Dynamic Host Configuration Protocol (DHCP)** to automate IP address assignment.
* **Routing Information Protocol (RIP)** for dynamic routing between internal and ISP routers.
* **Network Address Translation (NAT)** for enabling internet access to private IPs.
* **Wireless Access Point (WAP)** for Guest VLAN to allow external device connectivity with internal network isolation.

The project is limited to a simulation environment but is designed to reflect scalable and secure networking models used in real-world organizations.

1. **Network Structure Overview** 
   1. **Cloud:**

Acts as the simulated internet in Cisco Packet Tracer. It connects to the ISP router and represents external public connectivity for testing NAT and external access.

* 1. **ISP Router:**

Serves as the link between the internal organization and the simulated cloud. It has two interfaces: one facing the cloud (outside) and one facing the internal Router0 (inside). It is configured with RIP for route propagation and handles NAT for internet access by internal users.

* 1. **Main Router (Router0):**

This router connects to the ISP router for external access and to the core multilayer switch for internal communications. It is configured with sub-interfaces for each VLAN, acting as the default gateway for department devices. RIP routing and NAT are configured here to enable internet access and route advertisement.Core Switch or Layer 3 Switch (for internal network access).

* 1. **Core Switch (or Multilayer Switch):**

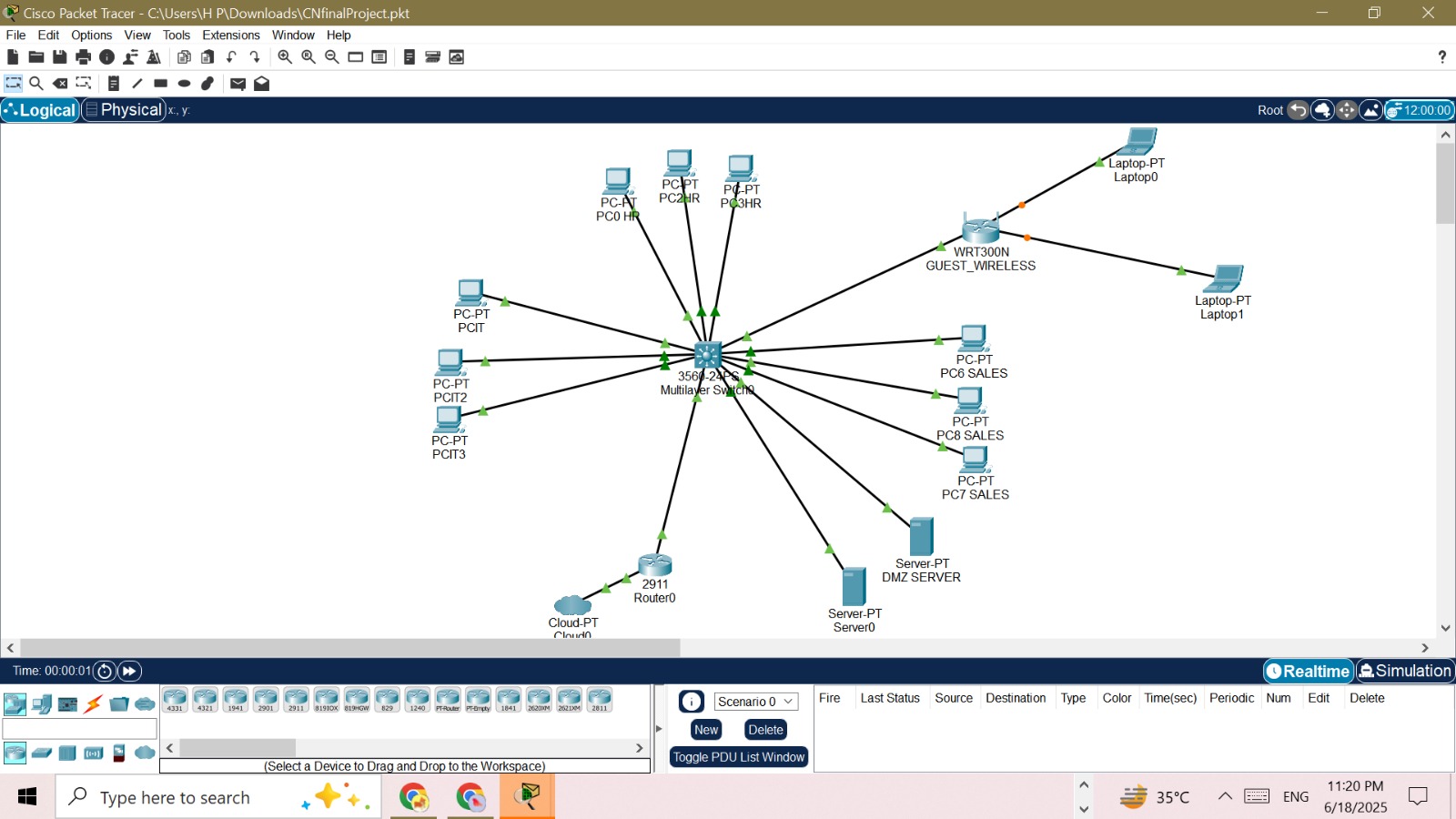
The central Layer 3 switch handles trunking with the router, access ports for PCs, and inter-VLAN routing functionality. It connects all departments (HR, IT, Sales) and internal services like servers and the WAP. It plays a critical role in handling segmented traffic efficiently.

* 1. **Wireless Access Point:**

Connected to the Guest VLAN, the WAP allows guest laptops to access the internet while being isolated from the internal LAN. It simulates real-world guest access, secured using ACLs.

* 1. **End Devices (PCs, Printers, etc.):**

Each department's devices are connected to access ports assigned to specific VLANs. IP addresses are assigned using DHCP. The Guest network uses wireless laptops, and servers are placed internally and in the DMZ for secured access.Communicate through the Main Router to reach other VLANs or the internet.



1. **System Limitations**

This network design was implemented within the Cisco Packet Tracer simulation environment, which introduces certain limitations that differentiate it from real-world deployment. Internet access is simulated using a cloud device and does not reflect true external connectivity, restricting accurate testing of public IP behavior. The use of **RIP** as a dynamic routing protocol limits scalability, as it supports only classful routing and is restricted to a maximum of 15 hops. Similarly, **Access Control Lists (ACLs)** are manually configured and lack dynamic policy adjustment, making them less practical for larger, evolving networks. **NAT** implementation in Packet Tracer is simplified and may not fully replicate real-world performance or behavior. Wireless capabilities are basic, offering limited SSID and security options. Additionally, there is no support for advanced security features like firewalls, intrusion detection systems (IDS), or real-time traffic monitoring. Furthermore, performance metrics such as bandwidth usage, latency, and packet loss cannot be effectively analyzed due to the constraints of the simulation. While the design demonstrates fundamental enterprise networking principles, its limitations must be acknowledged when considering practical deployment.

1. **Tools And Technologies**

| **Tools** | **Usage** |
| --- | --- |
| Cisco Packet Tracer | Used to design, configure, and simulate the entire network infrastructure. |
| Command Prompt | Used on end devices to verify connectivity using ping, ipconfig, etc. |

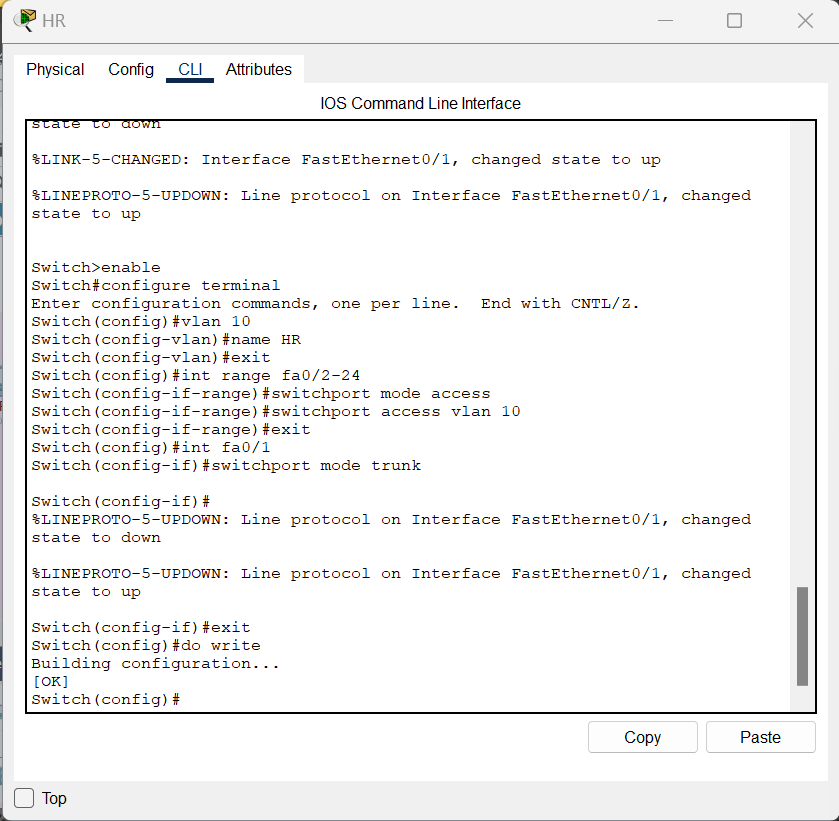
| **Technology** | **Usage** |
| --- | --- |
| VLAN | Logical separation of departments (IT, HR, Sales, Guest) to isolate traffic and reduce broadcast domains. |
| Inter-VLAN Routing | Enabled communication between different VLANs using a multilayer switch and sub-interfaces. |
| ACL (Access Control List) | Implemented to restrict unauthorized access, such as preventing Sales from accessing IT resources. |
| DHCP | Automatically assigned IP addresses to hosts in each VLAN, simplifying network management. |
| NAT | Allowed internal users with private IPs to access external networks via a single public IP. |
| RIP (Routing Protocol) | Used to dynamically propagate routes between the internal router and the ISP router. |
| Wireless Access Point (WAP) | Provided wireless access to guest users on a separate VLAN with restricted connectivity. |

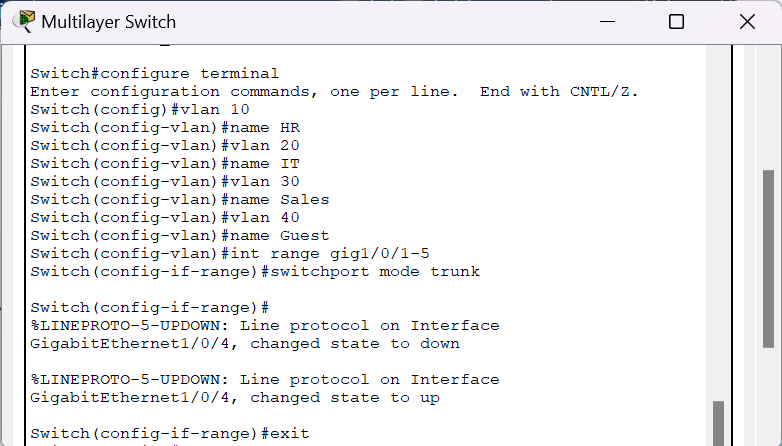
1. **Project Stakeholders**

|  |  |
| --- | --- |
| **Project Sponsor** | COMSATS University Islamabad, Islamabad Campus |
| **Stakeholder** | PRESENTED BY:   * Muhammad Ahmad (FA23-BDS-048) * Huzaima Imtiaz (FA23-BDS-017)   SUPERVISOR NAME:   * Dr.Marium Akbar |

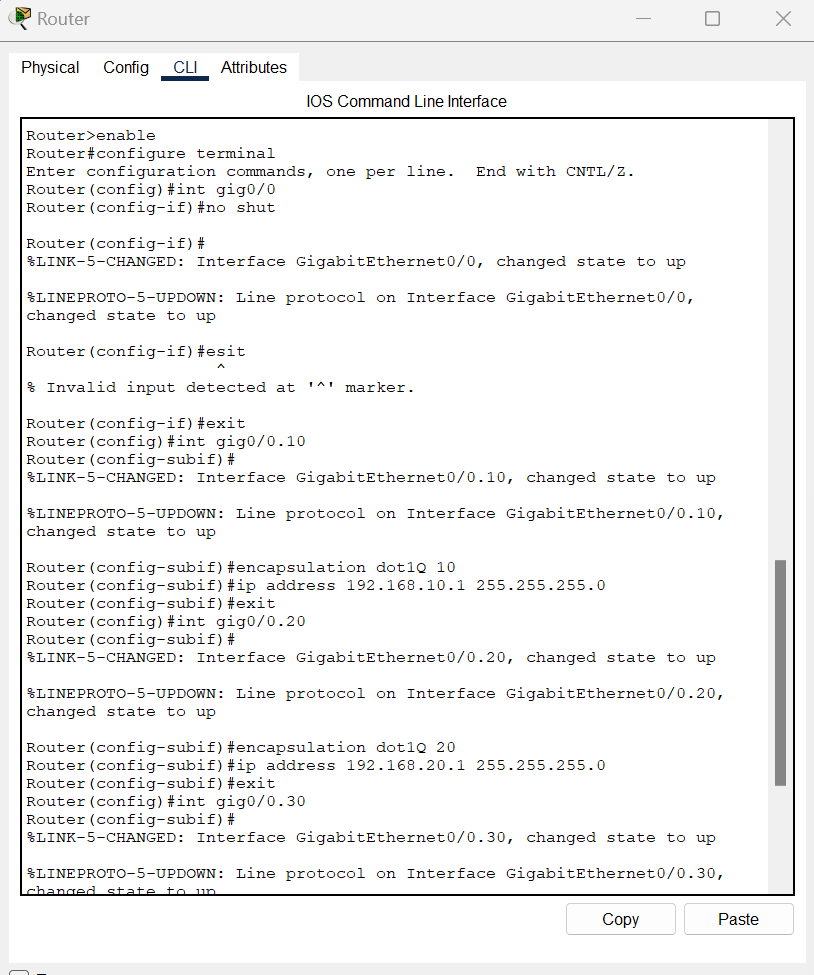
1. **Configurations With Snapshots**
   1. **Inter-VLAN Routing:**

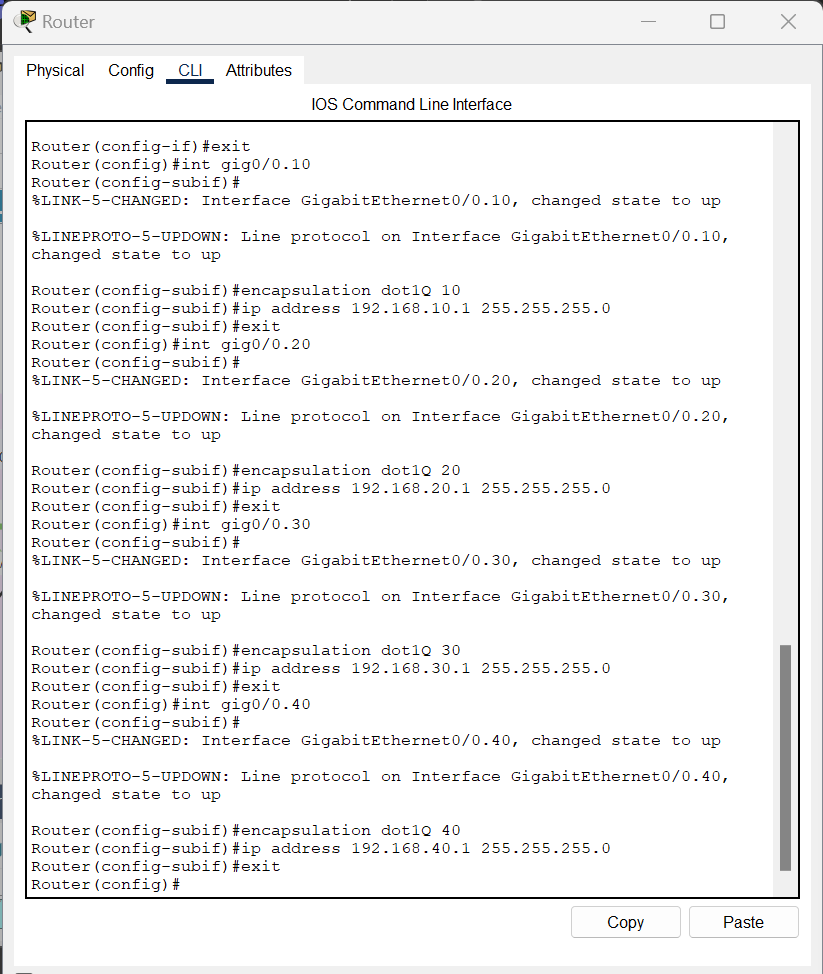
* Configured VLANs, named them, assigned ports and configured trunks between switches and to the router.



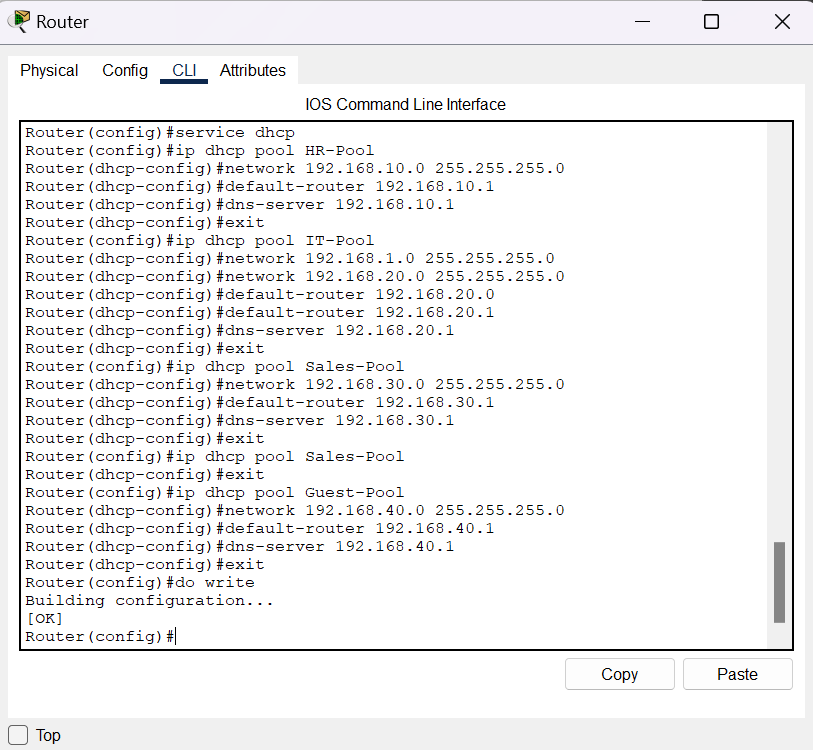


* Created sub-interfaces on the router, bind them to respective VLAN ID, and assigned the IP address

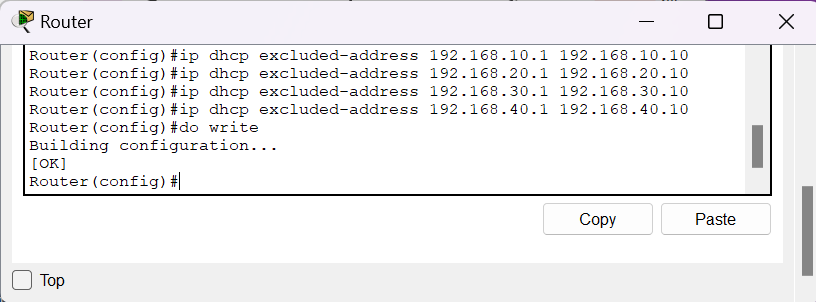




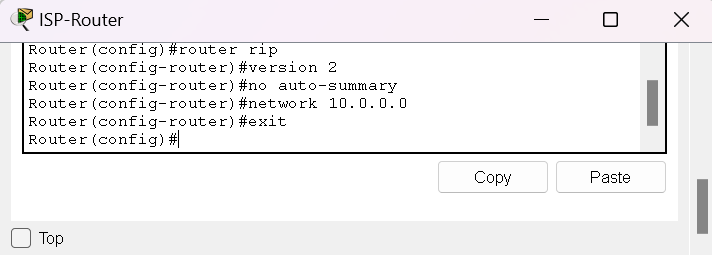
* 1. **DHCP Configuration:**
* Created DHCP pools and assigned network address, default gateway and DNS address.



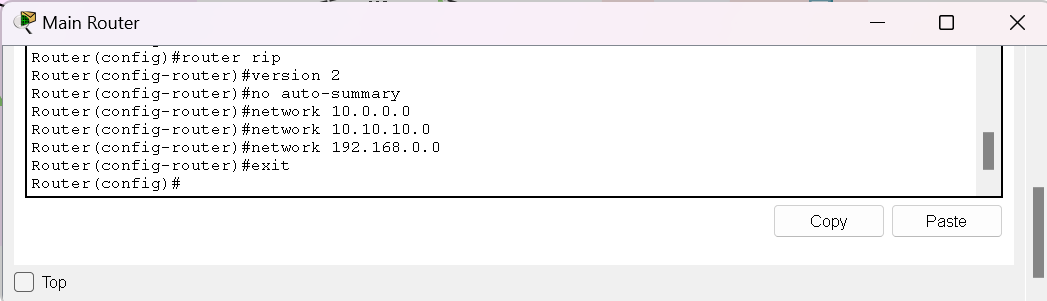
* Exclude ranges of IP address that should not be assigned dynamically.



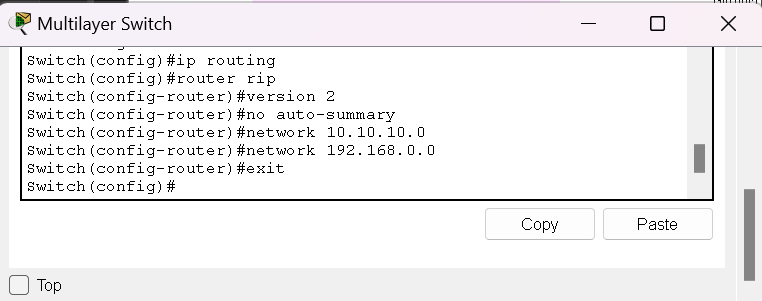
* Went to every PC and changed IP configuration from Static to DHCP.
  1. **Routing Information Protocol(RIP):**
* Configured RIP on ISP router



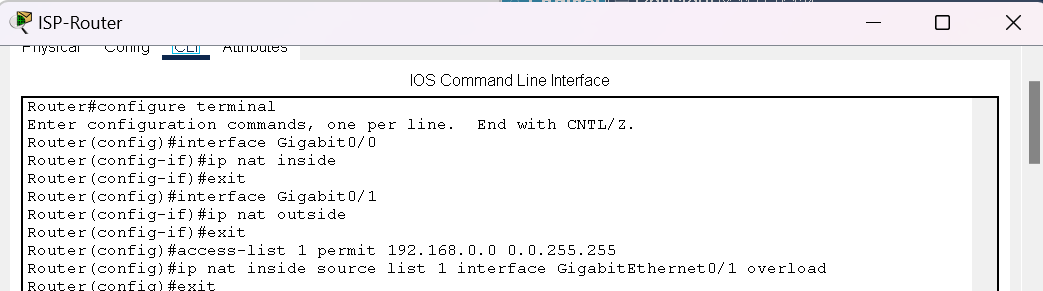
* Configured RIP on main router.



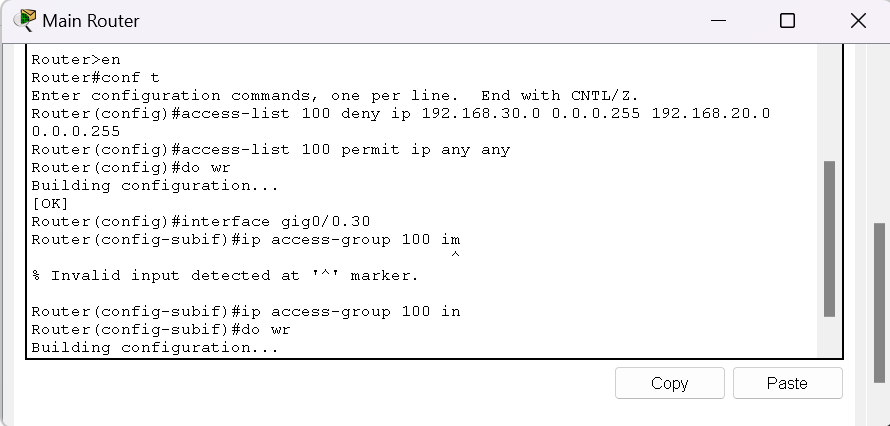
* Configured RIP on the multilayer switch.



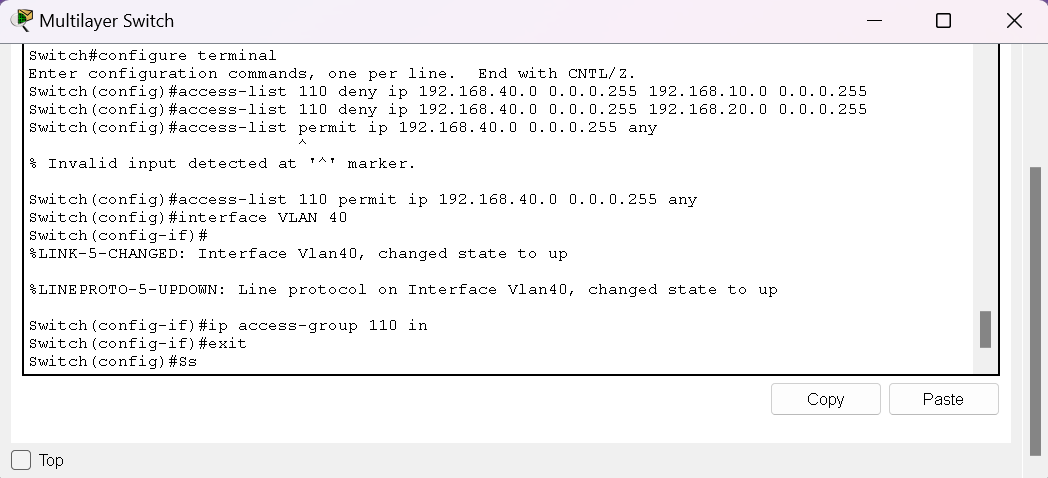
* 1. **NAT:**



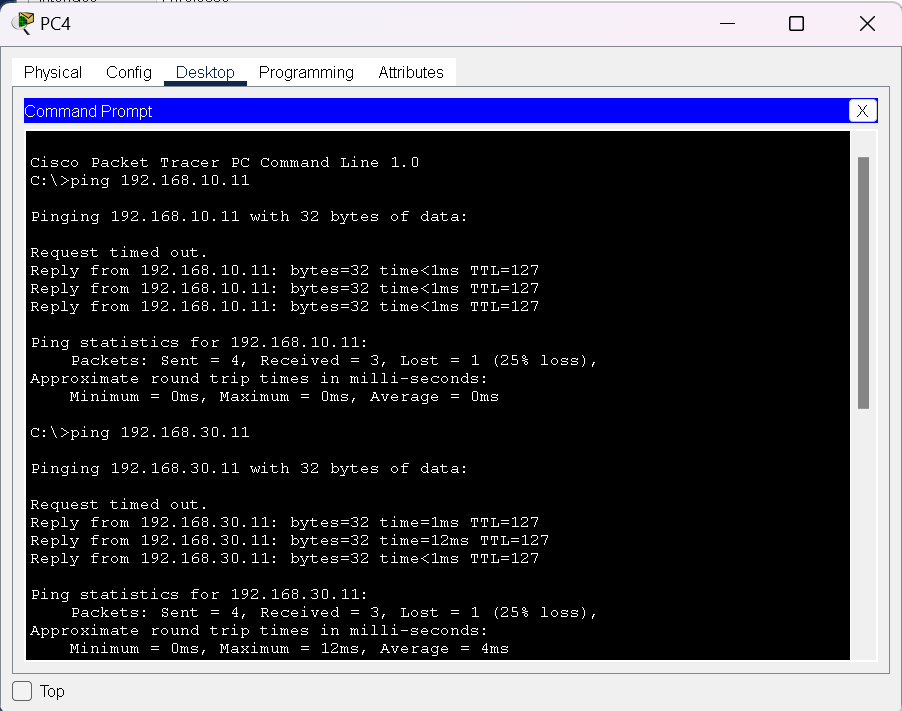
* 1. **ACL Configuration:**



* 1. **WAP for Guest User:**

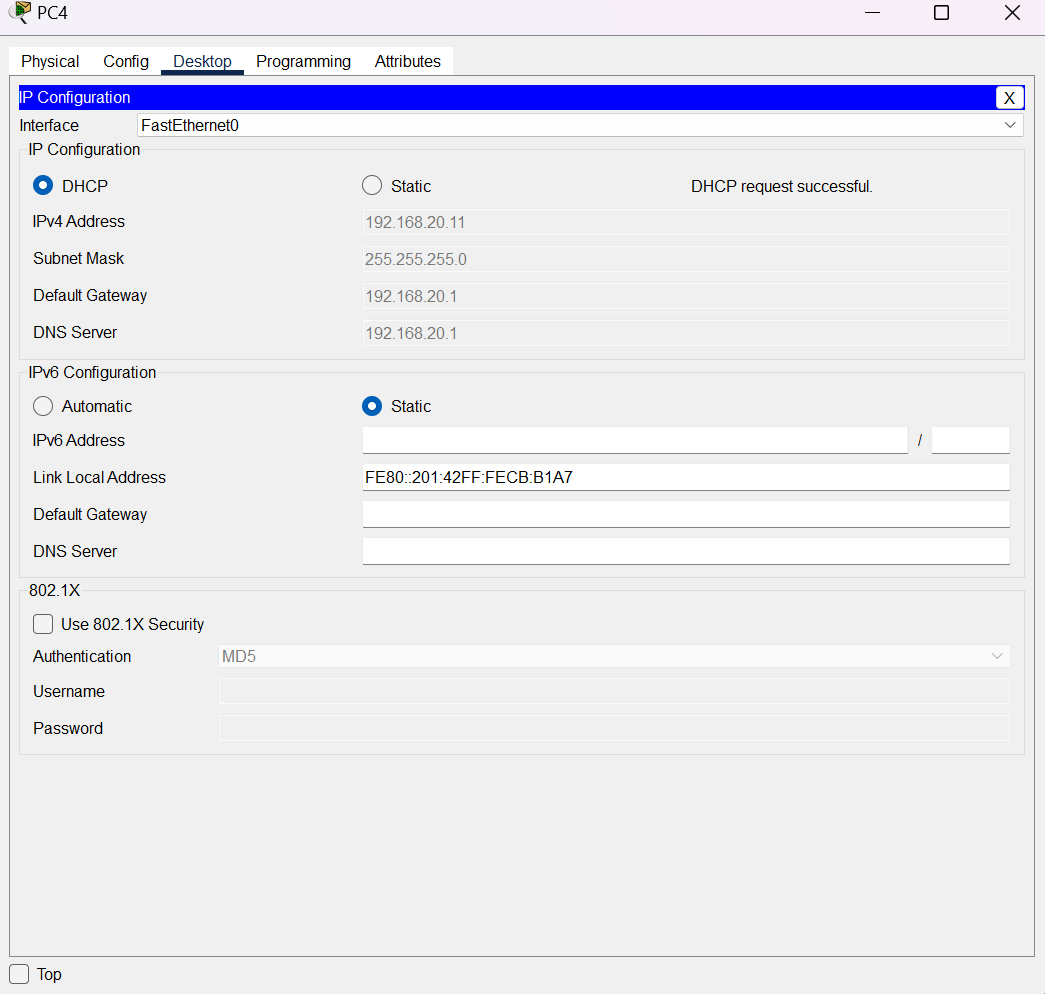


1. **Testing of all configurations:**
   1. **Inter VLAN Routing:**

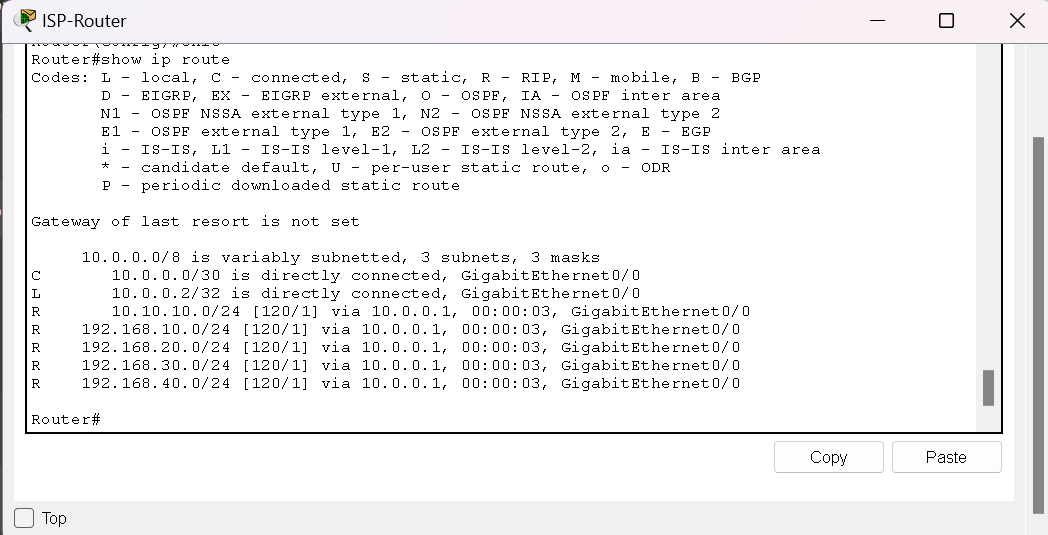


***^ Description: IT PC pinging Sales and HR PCs***

* 1. **DHCP:**

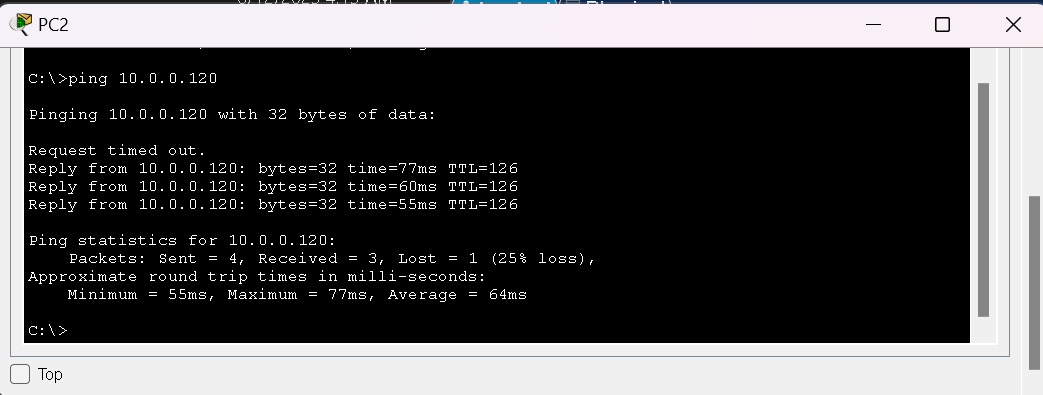


* 1. **RIP:**



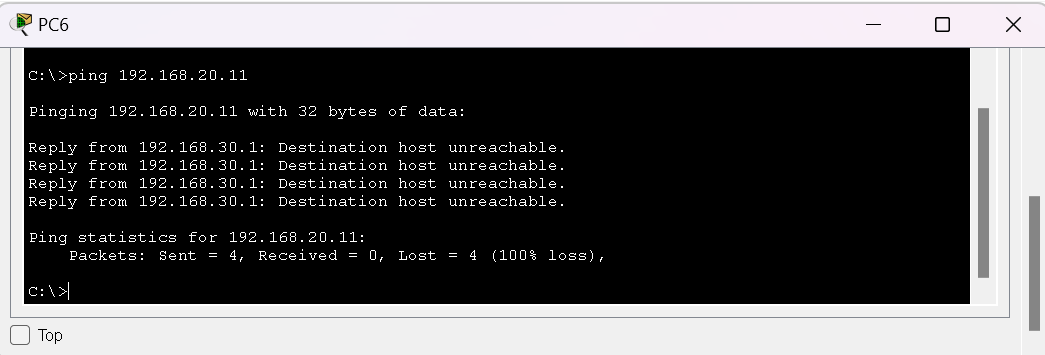
***^ Description: The paths starting with R are available due to RIP.***

* 1. **NAT:**



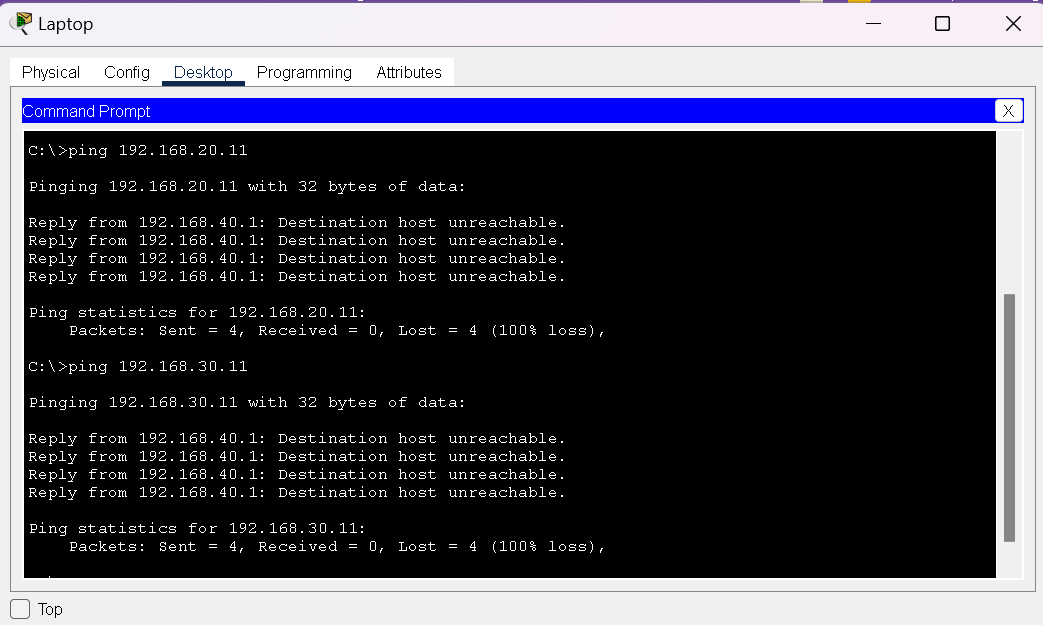
***^ Description: Pinging the Google Server from HR PC***

* 1. **ACL:**



***^ Description: Sales PC failed to get a response from IT PC***

* 1. **WAP for Guest user:**



1. **Justification of our choices:**
   1. **Inter-VLAN Routing:**

To ensure logical separation between departments while still allowing necessary communication, inter-VLAN routing was implemented using a multilayer switch. This allowed each VLAN (HR, IT, Sales, and Guest) to operate independently while enabling controlled interaction between them through routing interfaces.

* 1. **DHCP:**

The use of DHCP simplified network management by automatically assigning IP addresses to devices in each VLAN. This approach reduced manual configuration errors and made it easier to manage and scale the network, especially as the number of devices grows.

* 1. **RIP:**

RIP was chosen as the dynamic routing protocol due to its simplicity and ease of configuration within the Cisco Packet Tracer environment. It allowed automatic exchange of routing information between the main router and the ISP router, avoiding the need for static routing.

* 1. **NAT:**

NAT was configured on the ISP router to provide internet access to devices using private IP addresses. By using Port Address Translation (PAT), all internal users were able to share a single public IP (10.0.0.2), simulating real-world internet connectivity while conserving address space.

* 1. **ACL:**

ACLs were used to apply security policies between departments. For example, we blocked the Sales VLAN from accessing the IT VLAN. ACLs were also used to restrict the Guest VLAN from accessing any internal department, making the network more secure.

* 1. **WAP for guest users:**

The WAP was configured under the Guest VLAN to allow internet access for visiting users. ACLs were applied to ensure guests could not access sensitive resources in HR, IT, or Sales networks, providing both convenience and security.

* 1. **Firewall Rules:**

In place of a physical firewall, ACLs were used to simulate firewall functionality. These rules blocked unwanted traffic between departments and helped protect sensitive data and internal resources.

* 1. **Sub-netting Approach:**

We used /24 subnets for all VLANs like 192.168.10.0/24 for IT, 192.168.20.0/24 for Sales, and so on. This made IP management simple, avoided conflicts, and allowed room for future growth in each department.

1. **Conclusion:**

This project successfully demonstrates the complete implementation of a secure and well-structured departmental network using Cisco Packet Tracer. All required components and configurations were fully implemented according to the project requirements, including VLANs, Inter-VLAN Routing, DHCP, RIP, NAT, ACLs, and Wireless Access Point for guest users. Each department (IT, HR, Sales, and Guest) was assigned a unique VLAN and a separate /24 subnet to ensure proper network segmentation and address management. Inter-VLAN routing was configured using a multilayer switch to allow controlled communication between departments. DHCP was used to automatically assign IP addresses, minimizing manual errors and simplifying network management. RIP was implemented for dynamic routing between the main router and the ISP router. NAT was configured on the ISP router to enable internal devices with private IPs to access the internet through a single public IP. ACLs were applied to enforce access restrictions for example, blocking the Sales department from accessing IT resources and isolating guest users from internal VLANs. A wireless access point was set up for guest users under the Guest VLAN to provide internet access while maintaining internal network security. The subnetting strategy used /24 networks, making IP planning simple and scalable. In conclusion, all features were implemented successfully, and the entire network fulfills the project’s functional and technical requirements. The simulation provides a practical and complete representation of how modern enterprise networks are designed and secured.