Khulna University of Engineering and Technology

Department of Electronics and Communication Engineering

Project Title:
Design a campus network consisting of two or three departments and an admin office using CISCO packet tracer simulation software.

Course Title: Computer Network Laboratory
Course No: ECE 4110
Submission Date: 6 June, 2024

Prepared By:

Name: Tawsif Kaisar
Roll: 1909053
Department of Electronics & Communication Engineering
Khulna University of Engineering and Technology

Table of Contents

Abstract:
Using Cisco Packet Tracer, we designed and simulated a secure and scalable campus network. The network takes special care of two departments (e.g., ECE and CSE) and an Admin office. It includes dynamic routing for effective network communication, Access Control Lists (ACLs) to restrict access to administrative resources, password protection for network devices, DHCP for automatic IP address assignment, VLANs for departmental network segmentation, web and DNS servers for internal resource management, and dynamic routing for efficient network communication.

Introduction:

In today's educational landscape, technology plays a pivotal role in facilitating communication, resource accessibility, and administrative operations. A robust campus network serves as the backbone of this technological infrastructure, enabling effective collaboration among students, faculty, and administrative staff. This project focuses on designing a comprehensive campus network using CISCO Packet Tracer simulation software. Tailored to meet the needs of two or three departments and an administrative office, the network aims to address key requirements and challenges commonly encountered in educational institutions.
Key objectives include enhancing security through password protection mechanisms, simplifying network management with DHCP implementation, optimizing performance and security with VLAN segregation, strategically placing critical servers within the administrative office, implementing dynamic routing protocols for adaptability, and enforcing access control policies with ACLs.

Theory:

- Password Protection: Security is paramount in any network infrastructure. To safeguard against unauthorized access, all switches and routers within the network are configured with robust password protection mechanisms. This ensures that only authorized personnel can access and manage network devices, mitigating the risk of security breaches and unauthorized modifications.

- DHCP Implementation: Network management is streamlined through the implementation of the Dynamic Host Configuration Protocol (DHCP) in one of the departments. DHCP automates the assignment of IP addresses to devices within the network, eliminating the need for manual configuration. This not only reduces administrative overhead but also ensures efficient utilization of IP address space, facilitating scalability as the network grows.

- VLAN Segregation: To address the diverse user groups within the institution, a Virtual Local Area Network (VLAN) system is implemented in one of the departments. VLANs enable the segmentation of network traffic, separating student and faculty networks for enhanced security and performance. By isolating traffic between different user groups, VLANs minimize the risk of unauthorized access and optimize network bandwidth utilization.

- Server Placement: Critical servers, such as the web server and DNS server, are strategically placed within the administrative office. The web server hosts essential academic resources and services, while the DNS server facilitates efficient name resolution within the network. Centralizing these servers within the administrative office simplifies management and ensures consistent access to vital network services for all users.

- Dynamic Routing Protocol: Network flexibility is upgraded through the mix of a dynamic routing protocol. Dynamic routing protocols empower switches inside the network to trade routing data dynamically, considering ideal packet routing ways and proficient response to changes in network topology. This guarantees flexibility and versatility, empowering the network to adjust to advancing necessities and conditions.

- Access Control Lists (ACLs): Access to resources inside the administrative office is directed using Access Control Lists (ACLs) configured in routers. ACLs characterize granular principles overseeing which hosts or networks are allowed or denied access to explicit resources, like web servers or administrative systems. By upholding access control approaches, ACLs assist in safeguarding delicate information and guarantee consistency with security prerequisites.

By implementing these key objectives, this project aims to design a campus network that fosters a secure, efficient, and collaborative learning environment.

Required Software:

Cisco Packet Tracer [Version: 8.1.1.0022]

Network Design:

We implemented a departmentalized network utilizing two routers: one for the ECE department, another for the CSE department, and a third dedicated to the admin office.

For the ECE department, we configured a switch to connect four PCs. These PCs were further segmented into two VLANs, isolating two student PCs from two faculty PCs for enhanced security and network management.

Within the CSE department, we deployed four PCs and utilized the DHCP protocol to automatically assign unique IP addresses to each device on the network.

Finally, the admin network housed two servers and one PC. One server functioned as a DNS server, responsible for translating website addresses into corresponding IP addresses, while the other assumed the role of a web server, likely for hosting internal applications or resources.

All of these are illustrated in figure 1 below:

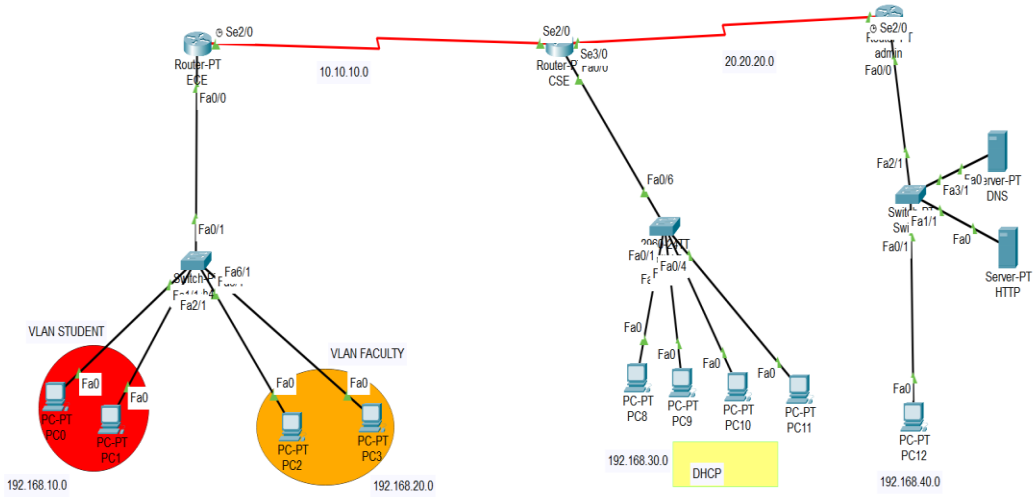


Figure 1: Network Architecture using Cisco Packet Tracer Simulation Software

Implementation:

1. For making all the switches and routers password protected, we have to configure passwords both on routers and switches using CLI command.

For example, on the ECE router, we wrote the following code for enabling password:

en
conf t
enable password 53
exit

Here, "53" is the password to login in the ECE router configuration.
For the switches, we applied the following code for enabling password:

en
conf t
line con 0
password ece
login
exit

Here, "ece" is the password to login in the switch configuration of ECE.

Similarly, we applied the same code with different passwords for all the routers and switches of the network.

2. We used DHCP protocol to assign IP addresses to all PCs of CSE department. For applying DHCP, we wrote the following code;

   ip dhcp exclude-address 192.168.30.2 192.168.30.10
   ip dhcp pool ece
   network 192.168.30.0 255.255.255.0
   default-router 192.168.30.1
   dns-server 192.168.40.4

   Here, We excluded the address from 192.168.30.2 to 192.168.30.10. We also declared the default router and the DNS server which we will use later.

3. We applied VLAN in ECE department to separate students and teachers network. For creating this VLAN, we applied the following code on the switch CLI terminal:

   en
   conf t
   vlan 10
   name student

vlan 20
name teacher
vlan 99
name management
exit
interface range fa1/1,fa2/1
switchport mode access
switchport access vlan 10
no shut
exit
interface range fa3/1,fa6/1
switchport mode access
switchport access vlan 20
no shut
exit

Then, we applied the following code on the ECE router:
interface range fa0/1
switchport mode trunk
switchport trunk native vlan 99
exit

Thus, we implemented VLAN system on ECE department to separate students and teachers network.

4. We setup two servers under the admin network. A HTTP web server where we hosted a website named “cc.com” and a DNS server from where we hosted our web server by applying DNS protocol.
   The server configuration settings are depicted below in figure 2 and figure 3:

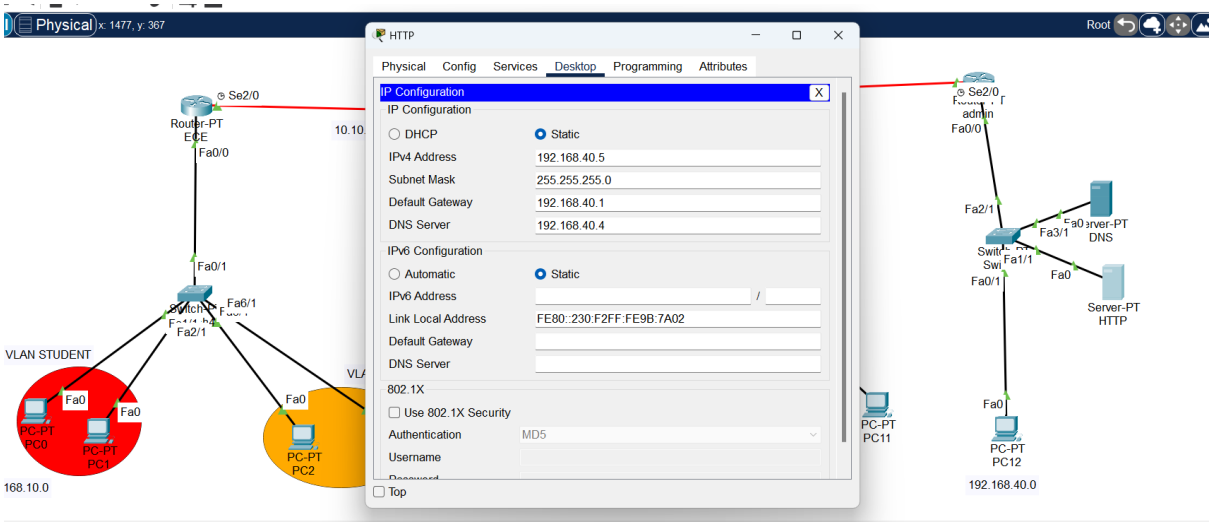


Figure 2: IP configuration of HTTP server

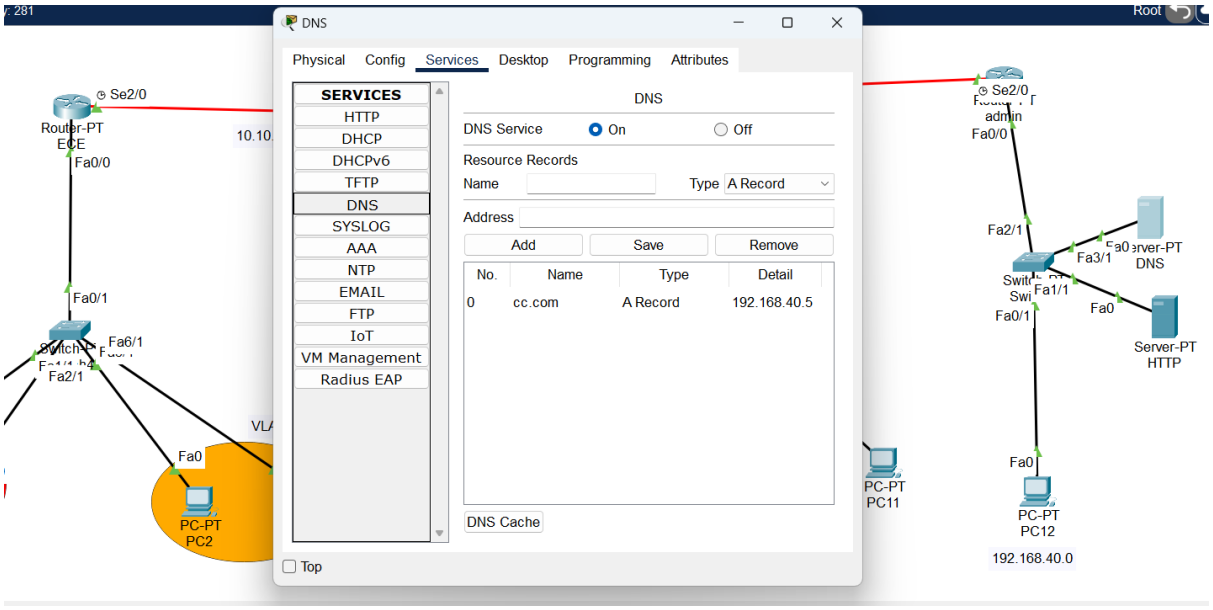


Figure 3: DNS configuration of DNS server

5. We used RIP for dynamic routing between the routers. For applying RIP on Admin router, we applied the following code on the CLI interface of the router:

en
conf t
router rip
network 20.20.20.0
network 192.168.40.0
passive-interface f0/0
no auto summary

exit

Similarly, for the ECE and CSE router we applied the same code with slight changes depending on the corresponding IP addresses of the router.

6. Finally, we applied ACL in routers to deny the PC8 and PC10 to access the web server and DNS server in the admin office. For applying ACL on PC8 and PC10, we input the following code on the CLI interface of CSE router:

   en
   conf t
   access-list 102 deny icmp host 192.168.30.14 host 192.168.40.4 echo
   access-list 102 deny tcp host 192.168.30.13 host 192.168.40.5 eq www
   access-list 102 permit ip any any
   int fa0/0
   ip access-group 102 in
   exit

Performance Analysis:

- All the switches and routers are password protected. No one without entering the password cannot configure the switches and routers. We applied enable password in the routers and console-line mode password in the switches which can be shown in the figure 4 and figure 5 below:

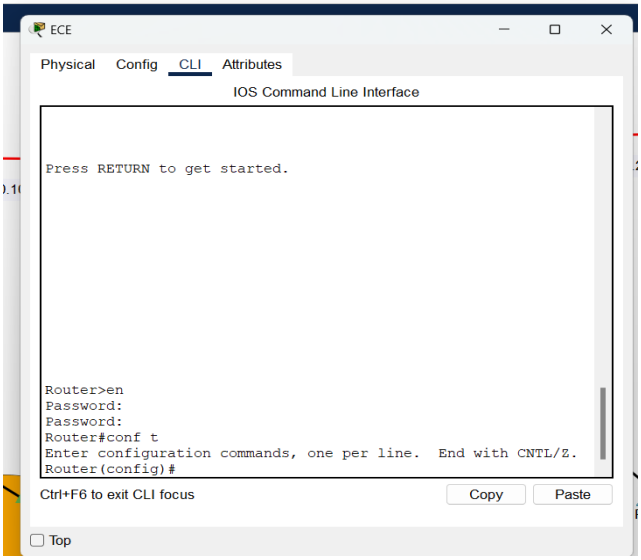


Figure 4: Password Protection on Router

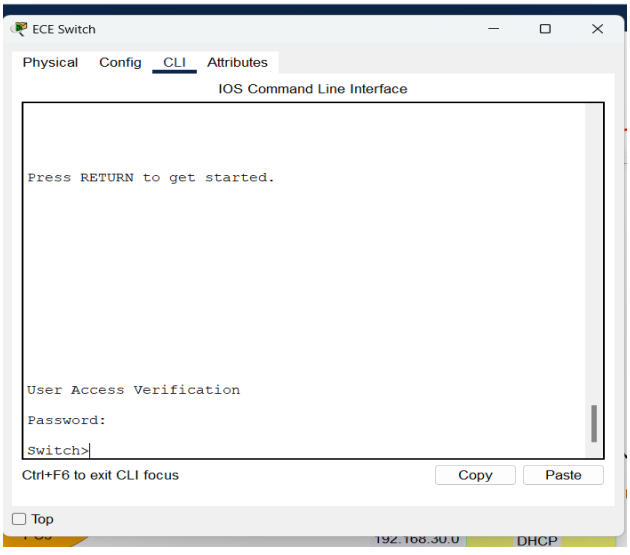


Figure 5: Password Protection on Switch

- We applied DHCP protocol on CSE department's PCs to assign the IP addresses automatically excluding a range of addresses. The router address was 192.168.30.1 so we excluded addresses from 192.168.30.2 to 192.168.30.10 . By applying DHCP we got the IP addresses of four PCs from 192.168.30.11 to 192.168.30.14 .

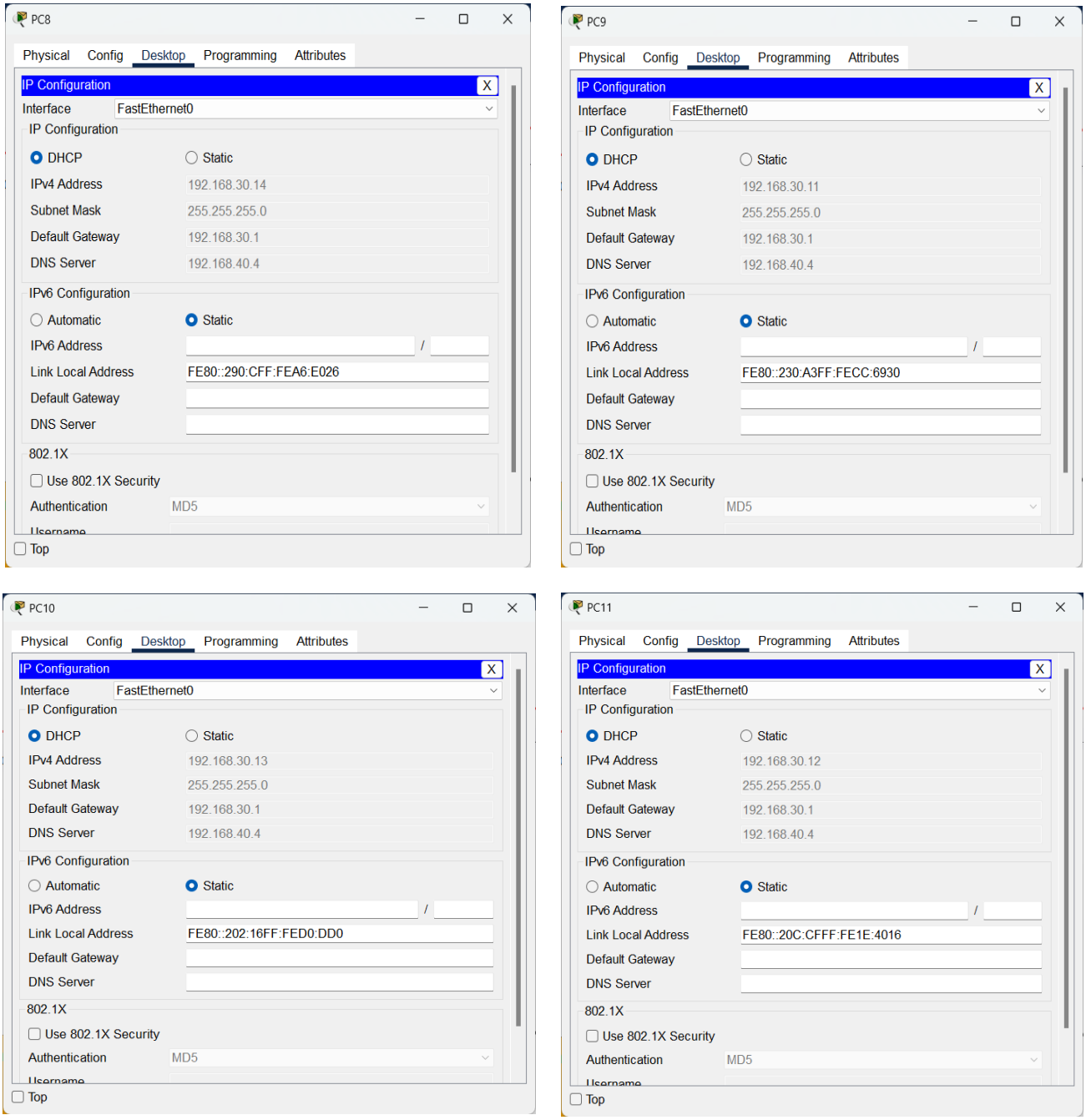


Figure 6: DHCP assigned IP addresses on the PCs of CSE Department

- We made two VLAN networks on ECE department named STUDENT and TEACHER to separate student and faculties networks. Figure 7 shows both the VLAN network of ECE department.

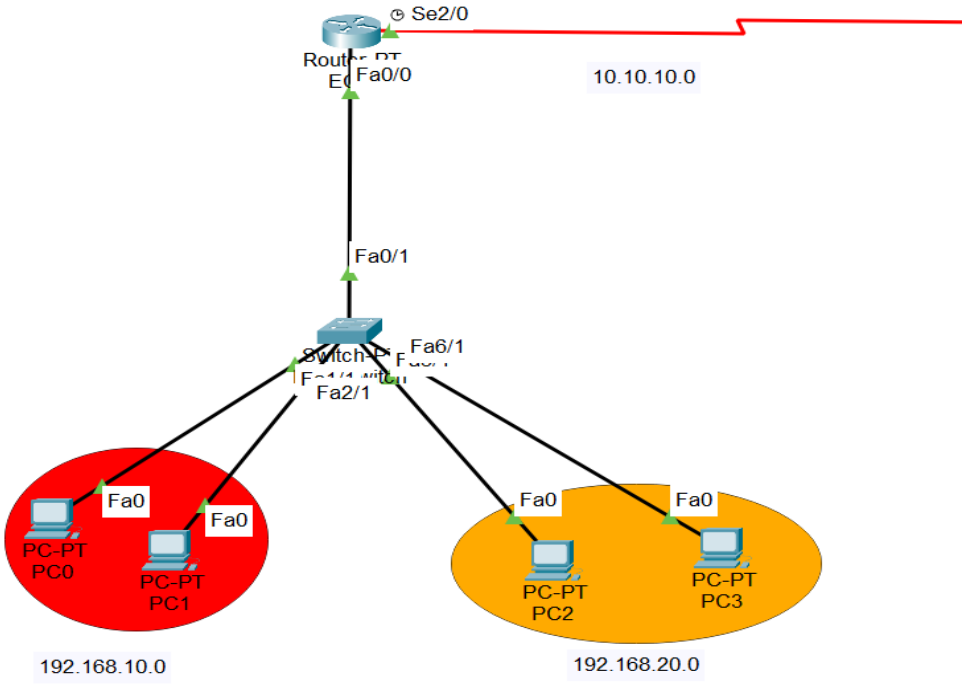


Figure 7: Red Colored PCs are in VLAN STUDENT and Yellow Colored PCs are in VLAN TEACHER

- We added two servers in Admin router where one acts as web server while the other acts as DNS server. We access these servers from any PC of the network until we apply any ACL on any PC or network.

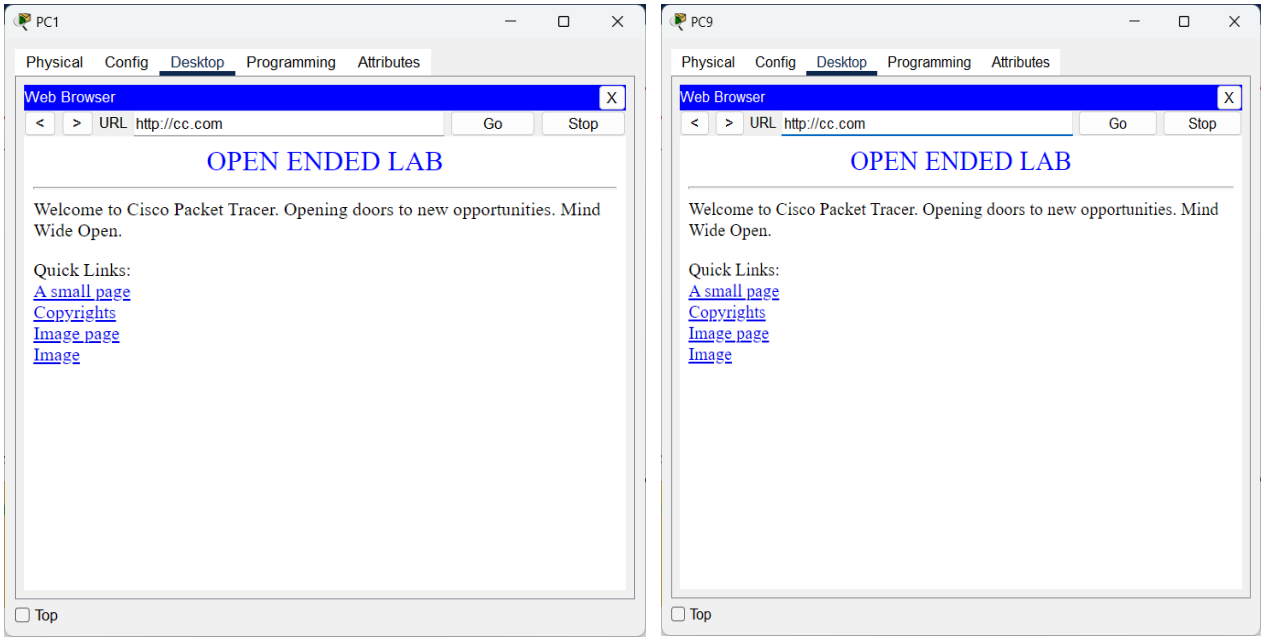
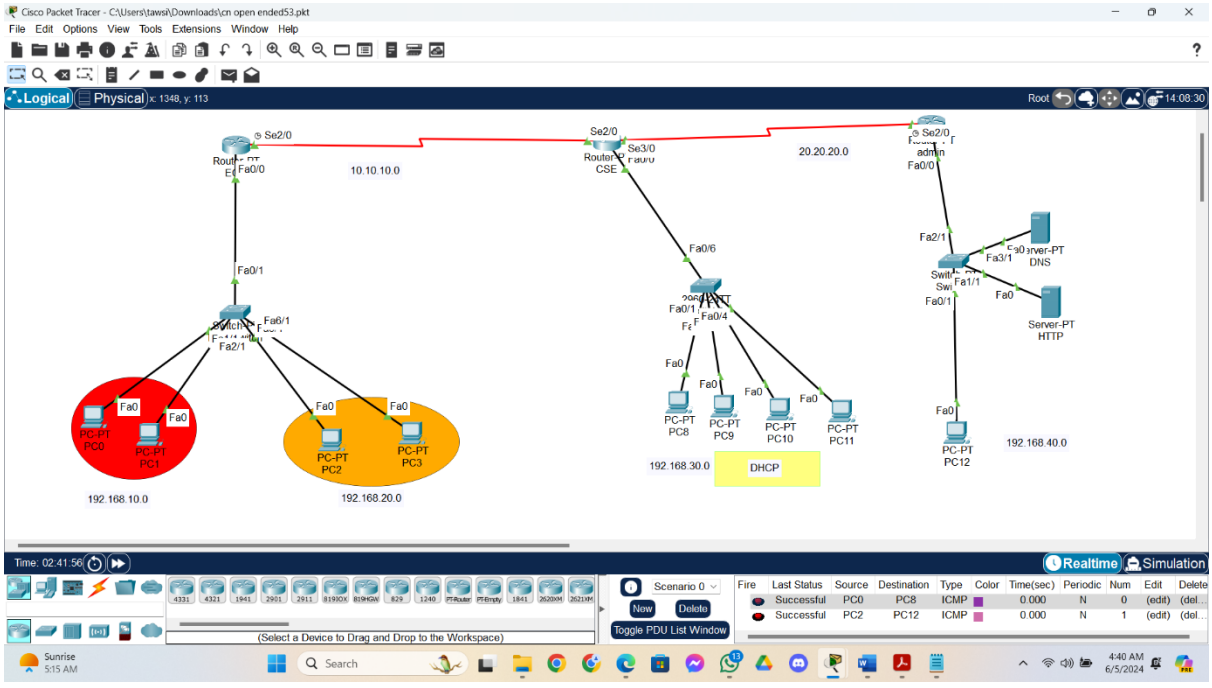
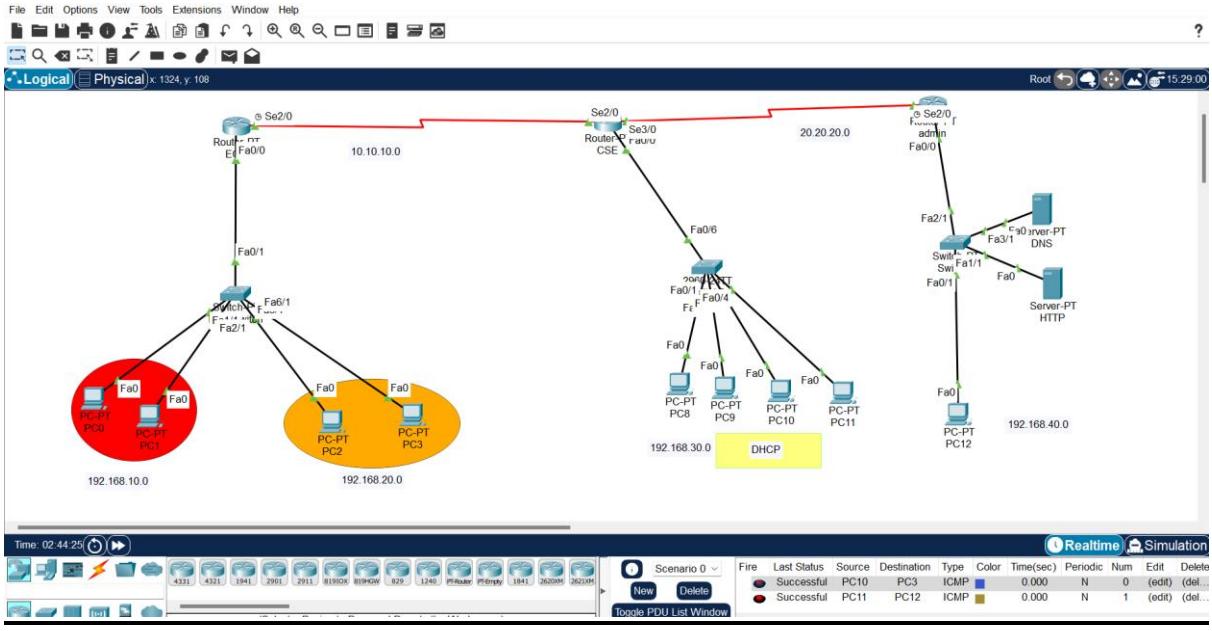


Figure 8: Accessing website from PCs of all other departments

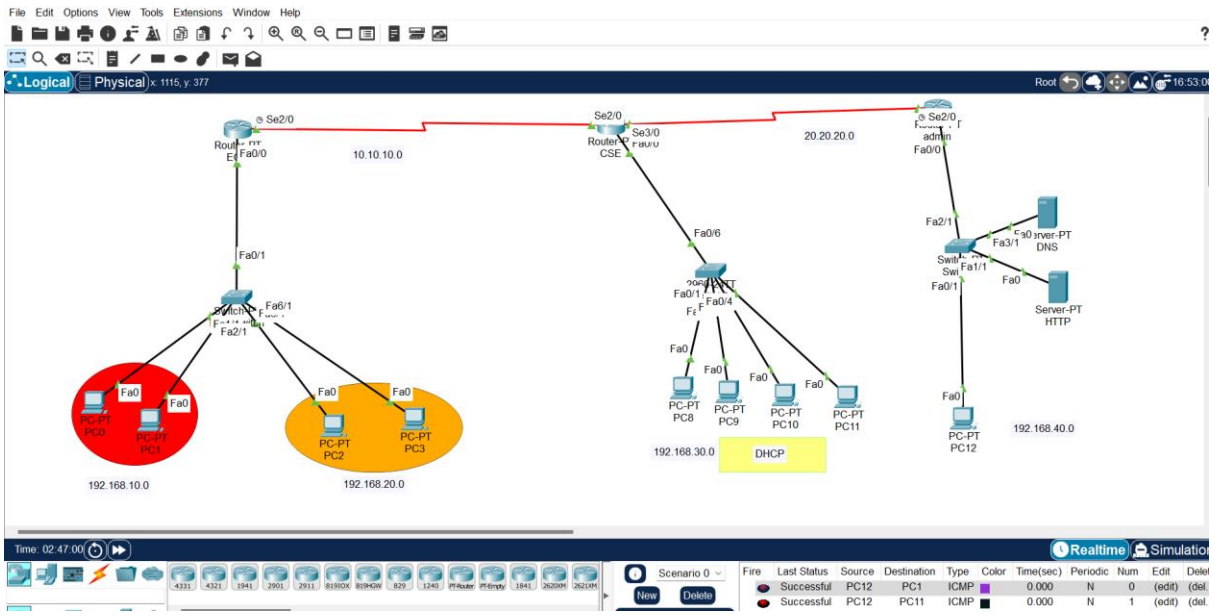
- For connecting and sharing data between all the departments, we have to do routing in all the routers. In this case, we used RIP Dynamic Routing Protocol in all the three routers of three departments. After establishing dynamic routing successfully, we can send packets from any hosts of any department to any other host of any other departments. In figure 9, we can see, we can send packets from any department PC to other department PC successfully because of successful routing.



(a)



(b)



(c)

Figure 9: (a) Successful packet transfer from ECE department's PCs to other department's PCs, (b) Successful packet transfer from CSE department's PCs to other department's PCs, (c) Successful packet transfer from Admin office's PCs to other department's PCs.

- We applied ACL in CSE router to deny access of PC8 to access the DNS server and to deny access of PC10 to access the web server in Admin office. After applying ACL on PC8, we can observe that we cannot ping the DNS server from PC8 which is shown in figure 10. After applying ACL on PC10, we observed that we cannot access the website from PC10 which presented in figure 11.ACL on PC10, we observed that we cannot access the website from PC10 which presented in figure 11.

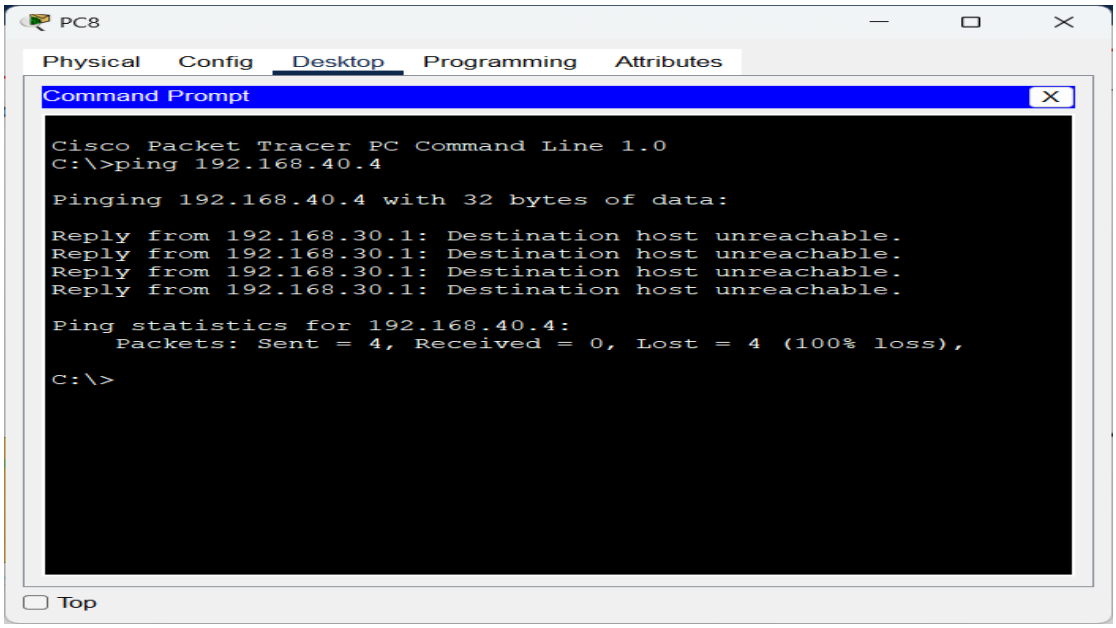


Figure 10: Unable to ping from PC8 to DNS Server Due to extended ACL

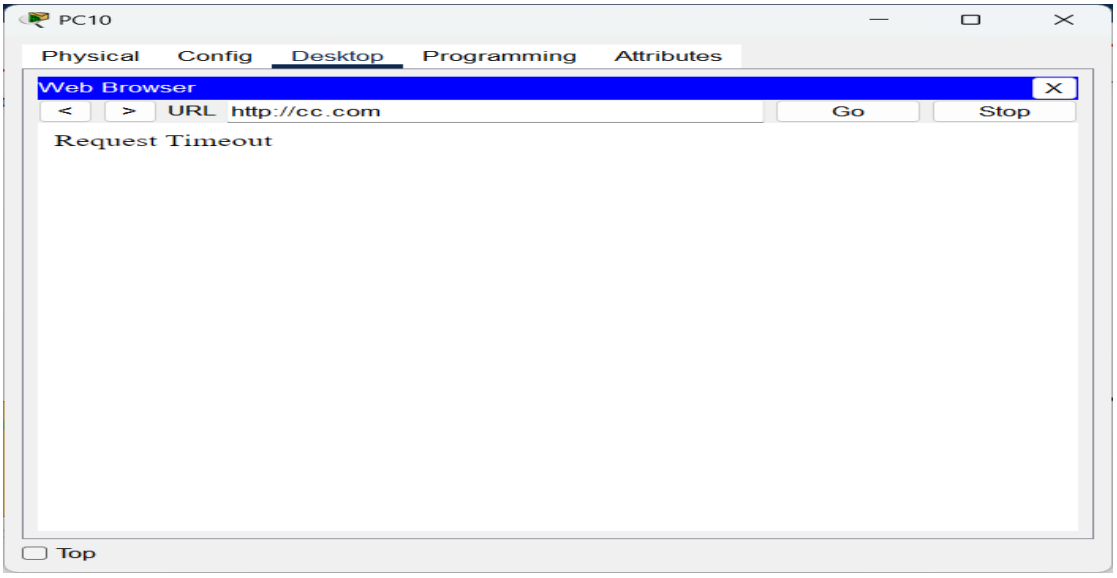


Figure 11: Unable to access web server from PC10 due to extended ACL

Conclusion:

The design and implementation of a campus network for two departments and an admin office using CISCO Packet Tracer successfully met all specified requirements, resulting in a robust, secure, and efficient network infrastructure. All switches and routers were password-protected to prevent unauthorized access, and Access Control Lists (ACLs) were applied on routers to regulate access to admin office resources, ensuring that only authorized personnel could access sensitive data.

The network efficiently utilized the DHCP protocol for CSE department network, automating IP address assignment and reducing administrative effort while ensuring efficient IP management. In ECE department, VLAN segmentation was implemented to separate student and faculty networks. This approach enhanced security and improved network performance by reducing broadcast domains.

The strategic placement of a web server and DNS server within the admin office supported various campus applications and facilitated seamless domain name resolution, ensuring uninterrupted network operations. A dynamic routing protocol such as RIP was also integrated into the network topology, optimizing routing paths and enhancing overall network performance and resilience.

In summary, the campus network designed with CISCO Packet Tracer not only meets but exceeds the project requirements. The integration of security measures, dynamic IP addressing, VLAN segmentation, server placement, and dynamic routing collectively contributes to a comprehensive and scalable network

framework, demonstrating practical networking concepts and providing a strong foundation for future network expansion.

References:

1. Lab Manuals
2. www.ipcisco.com
3. www.geeksforgeeks.com
4. www.netwrix.com