



**Khulna University of Engineering and Technology**  
**Department of Electronics and Communication Engineering**  
**Open Ended Project**

**Course No:** ECE 4110

**Course Title:** Computer Networks Laboratory

**Topic:** Design of a campus network using CISCO packet tracer

**Submitted by**

Name: Md. Saif Alvi.

Roll: 1909013

Semester: 4-1

Department of Electronics and Communication Engineering.

Khulna University of Engineering and Technology, Khulna.

**Submitted to**

MD Foysal

Assistant Professor

Department of Electronics and Communication Engineering.

Khulna University of Engineering and Technology, Khulna.

Shah Muhammad Azmat Ullah

Lecturer

Department of Electronics and Communication Engineering.

Khulna University of Engineering and Technology, Khulna.

## Open Ended Project

Design a campus network consisting of two or three departments and an admin office using CISCO packet tracer simulation software. The network topology must meet the following requirements:

1. All switches and routers should be password protected.
2. One of the departments would use the DHCP protocol to assign the IP addresses to all hosts of that network.
3. One of the departments would contain a VLAN system to separate students and faculties networks.
4. A web server and a DNS server should be placed under the admin office.
4. Any of your known dynamic routing protocols should be applied in the designed topology.
5. Apply your desired ACL in routers to access the resources of the admin office. (For example, permit/deny any host/network to access the web server or any host in the admin office)

# **Introduction**

This report describes the building and installation of a campus network for two departments and an admin office using Cisco Packet Tracer simulation software. In order to satisfy the demands of a contemporary campus setting, the network has been designed with security, scalability, and efficiency in mind. It does this by combining a variety of networking protocols and capabilities.

## **Network Design Features**

### **1. Security**

All network devices, including switches and routers, are password protected to prevent unauthorized access. This ensures that only authorized personnel can modify the network configurations, enhancing the security and integrity of the network.

### **2. Dynamic Host Configuration Protocol (DHCP)**

One of the departments employs the DHCP protocol to automatically assign IP addresses to all network hosts. This minimizes manual configuration efforts and reduces the risk of IP address conflicts, ensuring efficient and streamlined network management.

### **3. Virtual Local Area Network (VLAN)**

One department utilizes VLAN technology to segregate the network into student and faculty segments. VLANs enhance security and improve network performance by isolating traffic and preventing unauthorized access between different user groups.

### **4. Network Servers**

The admin office houses a web server and a DNS server. The web server hosts the admin website and other online resources, while the DNS server resolves domain names to IP addresses, facilitating smooth network navigation and access to resources.

### **5. Routing Information Protocol (RIP)**

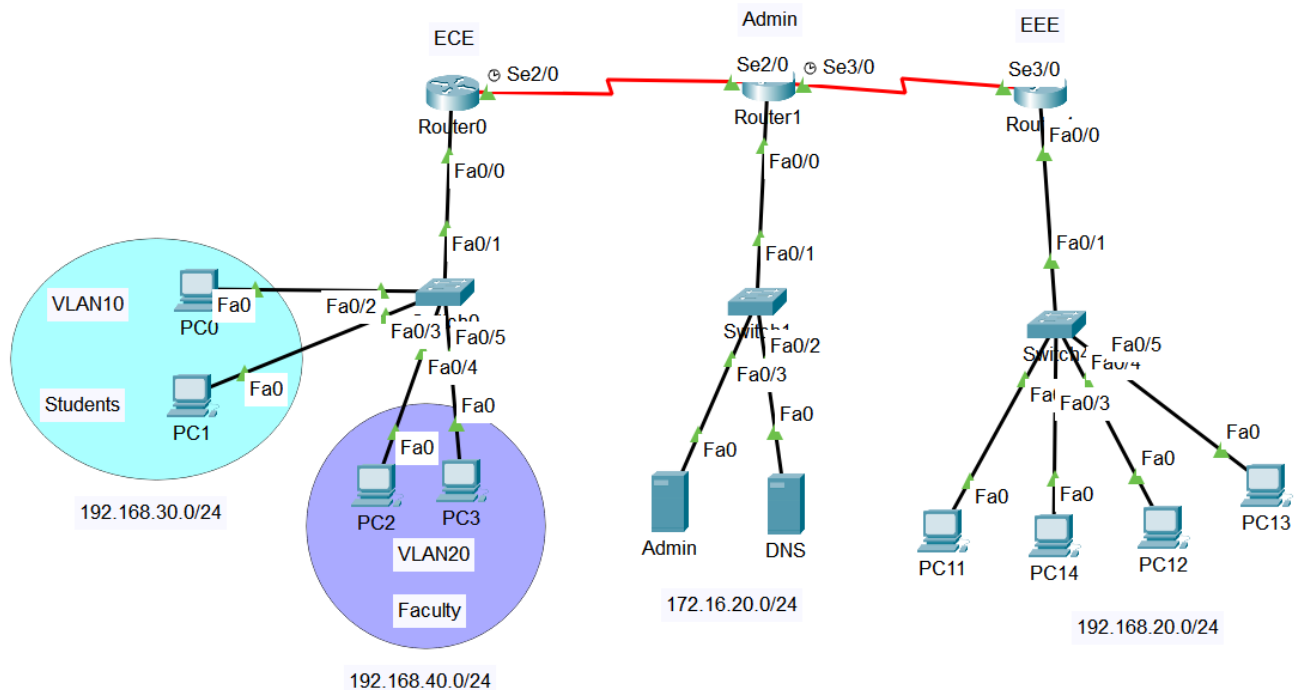
The network employs the RIP dynamic routing protocol, which allows routers to dynamically learn and propagate routes. This enhances network resilience and ensures optimal path selection for data transmission across the network.

### **6. Access Control Lists (ACL)**

Extended Access Control Lists (ACL) are implemented on routers to control access to the resources in the admin office. ACLs permit or deny traffic based on specified

criteria, such as IP address or network, thus enforcing security policies and regulating access to sensitive resources.

## Network Topology



**Figure 1.1:** Network topology as described in the problem

## Network Devices and Connections

### 1. Routers:

- Router0: Connects ECE department and the Admin Office.
- Router1: Connects ECE department, EEE department and the Admin Office.
- Router2: Connects EEE department and the Admin Office.

### 2. Switches:

- Switch0: ECE department
- Switch2: EEE department
- Switch1: Admin Office

### 3. Servers:

- Web Server
- DNS Server

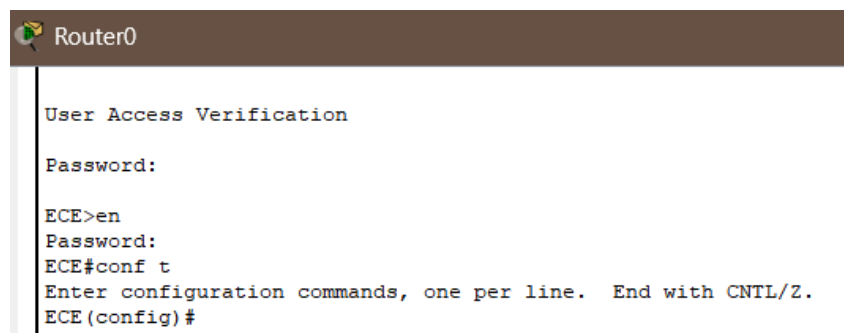
### 4. PCs:

- Multiple PCs in each department.

## Configuration Details

### 1. Router and Switch Password Protection

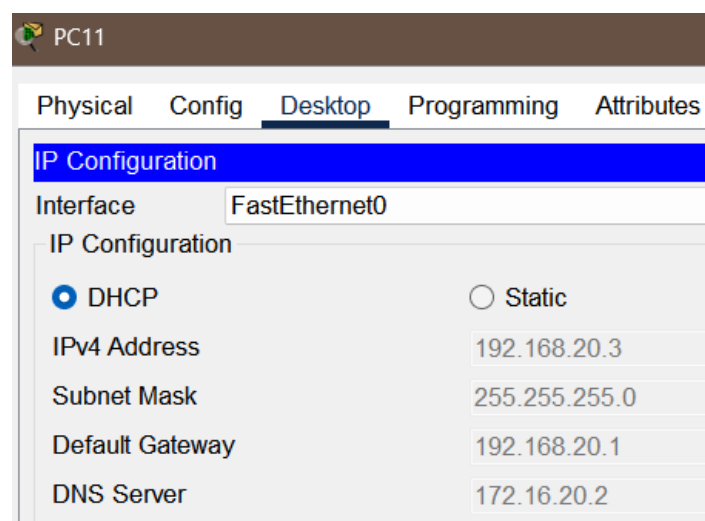
All routers and switches are configured with passwords to enhance security.



**Figure 1.2:** Password protection in Router0

### 2. DHCP Configuration on Router2 (EEE department)

Router2 is configured to provide DHCP services for EEE department.



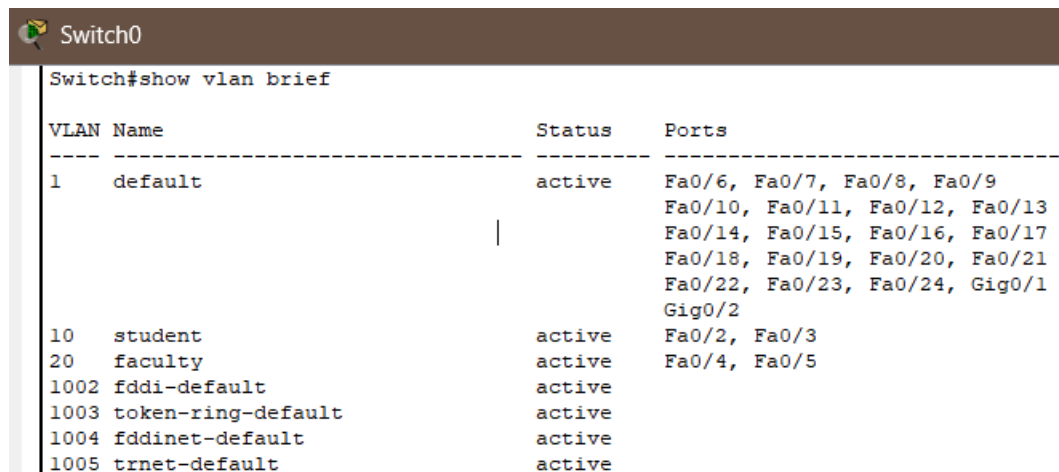
**Figure 1.3:** DHCP service in a pc under Router2

### 3. Static IP configuration for pcs and servers in Router0 and Router1

- Router0: 192.168.10.1
- Router1: 172.16.20.1
- PC0: 192.168.30.2 (VLAN10)
- PC1: 192.168.30.3 (VLAN10)
- PC2: 192.168.40.2 (VLAN20)
- PC3: 192.168.40.3 (VLAN20)
- Admin Server: 172.16.20.3
- DNS Server: 172.16.20.2

### 4. VLAN Configuration on Switch0 (ECE department)

Switch0 is configured to create VLANs for students and faculty networks.



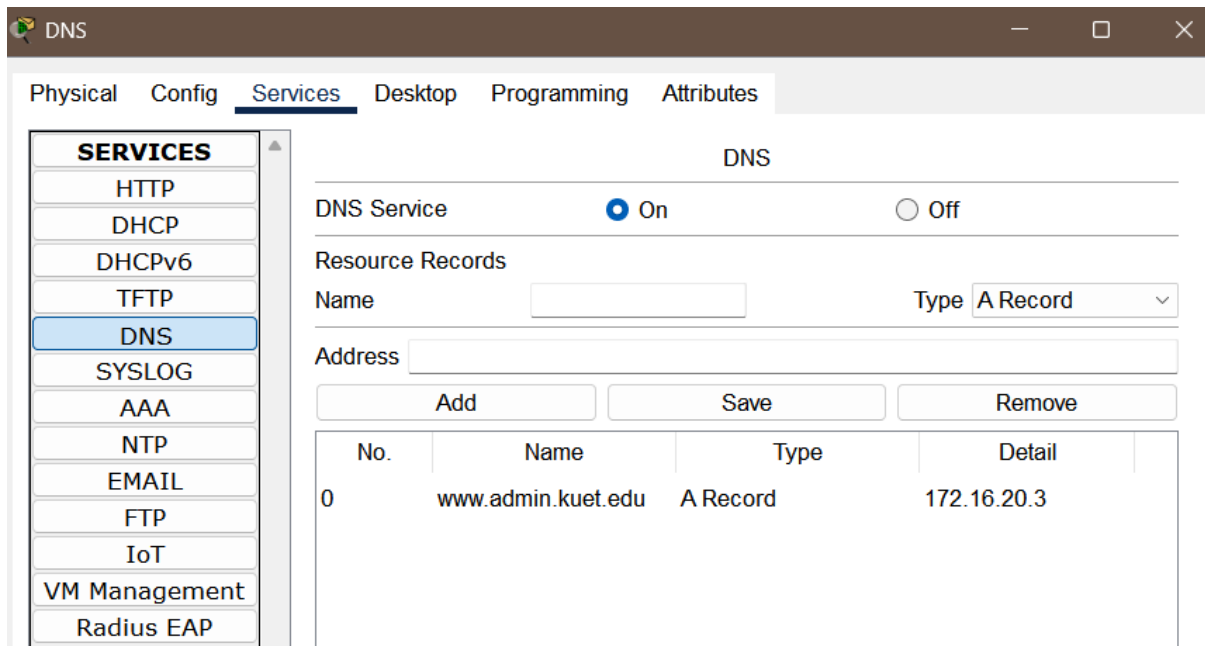
VLAN	Name	Status	Ports
1	default	active	Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Gig0/1 Gig0/2
10	student	active	Fa0/2, Fa0/3
20	faculty	active	Fa0/4, Fa0/5
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

**Figure 1.4:** VLAN configuration in Switch0

From Figure 1.4 we can observe that VLAN 10 is assigned to students and VLAN 20 is assigned to Faculty.

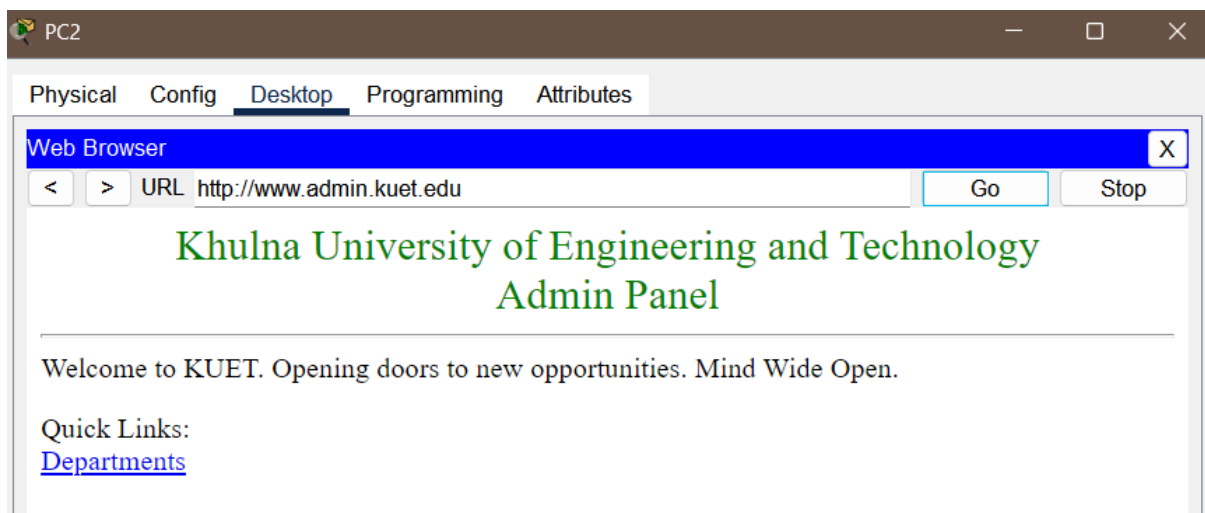
### 5. Web Server and DNS Server configuration on Router1 (Admin)

Admin server (172.16.20.3) is hosting a website called [www.admin.kuet.edu](http://www.admin.kuet.edu). Now this Admin server address 172.16.20.3 is stored in DNS server (172.16.20.2) which is mapped to the domain name [www.admin.kuet.edu](http://www.admin.kuet.edu).



**Figure 1.5:** DNS service in DNS server

Now setting the DNS server *172.16.20.2* in pcs IP configuration in the network and then we can browse the website [www.admin.kuet.edu](http://www.admin.kuet.edu) from any pcs in the network.



**Figure 1.6:** Browsing using the domain name

## 6. Access Control Lists (ACLs) Configuration

Extended ACLs are configured to control access to the web server in the admin office. The students' pcs in ECE department which is under VLAN 10 (*192.168.30.0*) should not have access to the Admin Server. On the other hand, the faculty pcs in ECE

department which is under VLAN 20 (192.168.40.0) have the access to the Admin Server.

```

Router0

User Access Verification









Password:

ECE>en
Password:
ECE#show access
ECE#show access-lists
Extended IP access list 100
 10 deny ip 192.168.30.0 0.0.0.255 host 172.16.20.3
 20 permit ip any any

```

**Figure 1.7:** Extended ACL configuration to control access in the Admin Server

PC0 and PC1 of VLAN 10 are denied access to the admin server. On the contrary, PC2 and PC3 of VLAN 20 have the permit to access the admin server.

PDU List Window								
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Failed	PC0	Admin	ICMP		0.000	N	0
	Failed	PC1	Admin	ICMP		0.000	N	1
	Successful	PC2	Admin	ICMP		0.000	N	2
	Successful	PC3	Admin	ICMP		0.000	N	3

**Figure 1.8:** Access control lists test

## Result Analysis and Simulation

### Connectivity

- **Ping Test:** Verified connectivity between PCs and servers.
- **VLANs:** Ensured VLAN separation between student and faculty networks.

### DHCP

- **IP Assignment:** Verified that PCs in EEE department received IP addresses via DHCP.



## **RIP Routing**

- **Routing Table:** Checked the routing table to ensure RIP routes are correctly propagated.

## **ACLs**

- **Access Restrictions:** Tested access restrictions to ensure ACLs are working as expected.

## **Conclusion**

The designed network meets all specified requirements, including password protection for all devices, DHCP for ECE department, VLAN separation for EEE department, hosting web and DNS servers in the admin office, implementing RIP for dynamic routing, and configuring ACLs for access control. This ensures a secure, efficient, and well-organized campus network. Finally, we can say that the open ended project is done successfully.