

KHULNA UNIVERSITY OF ENGINEERING AND TECHNOLOGY

DEPT OF ELECTRONICS AND COMMUNICATION ENGINEERING

Course Title: Computer Networks Laboratory

Course Code: ECE 4110

Open Ended Project Report

Software: Cisco Packet Tracer

|  |  |
| --- | --- |
| Submitted by  H.M.Fahad  Roll: 1909049  Year: 4th  Dept: ECE | Submitted to  Md Foysal  Assistant Professor  Dept of ECE, KUET  Shah Muhammad Azmat Ullah  Lecturer  Dept of ECE, KUET |

**Project Requirements**

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.

5. Any of your known dynamic routing protocols should be applied in the designed topology.

6. 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)

After completing the above task, you must prepare a well-organized report that reflects the description and clarification of your whole work.

**Introduction:**

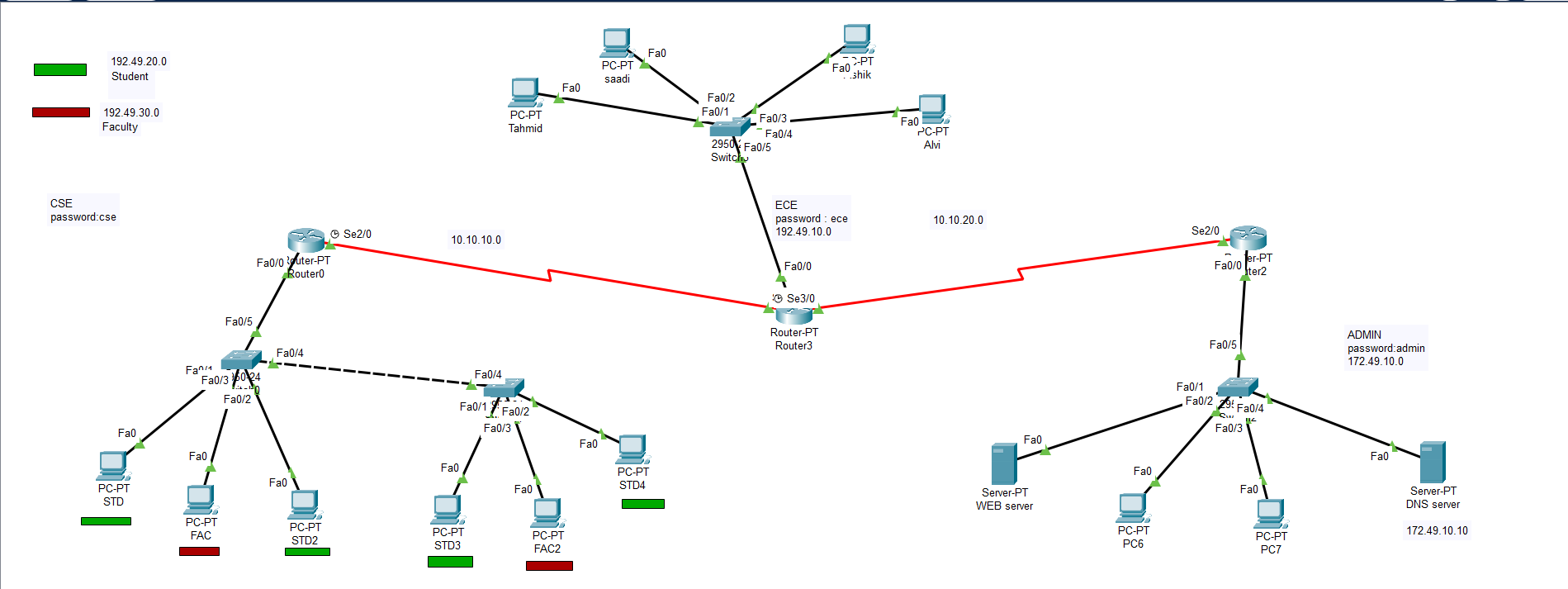
Strong and effective campus networks are necessary in today's educational institutions to guarantee resource sharing and seamless connectivity throughout departments. This article describes how a campus network was designed and put into operation using the Cisco Packet Tracer simulation program. The network is divided into two departments: one uses Virtual Local Area Networks (VLANs) to divide the networks belonging to the teachers and students, and the other uses Dynamic Host Configuration Protocol (DHCP) to assign IP addresses. The management office also houses a DNS server and a web server, and dynamic routing protocols help network segments communicate with one other. In order to maintain security and manage access to essential services, the network design also incorporates Access Control Lists (ACLs) on routers to regulate access to administrative resources.

**Theory:**

#### **Network Design and Components**

1. **Password Protection for Network Devices:** Password protection on all switches and routers is a fundamental security measure. It prevents unauthorized access and potential network breaches, ensuring that only authorized personnel can configure or alter network settings.
2. **Dynamic Host Configuration Protocol (DHCP):** DHCP automates the assignment of IP addresses to devices within a network. In one department, DHCP is implemented to manage IP address allocation dynamically. This reduces the administrative burden of manually assigning IP addresses and helps avoid IP conflicts.
3. **Virtual Local Area Networks (VLANs):** VLANs are used in the second department to create separate network segments for students and faculty. By segregating the network, VLANs enhance security and reduce broadcast traffic. This ensures that sensitive faculty communications remain isolated from student networks.
4. **Web Server and DNS Server:** The administration office hosts a web server and a DNS server. The web server provides essential services and resources accessible over the network, while the DNS server translates domain names into IP addresses, facilitating easier access to network resources.
5. **Dynamic Routing Protocols:** Dynamic routing protocols, such as OSPF (Open Shortest Path First) or EIGRP (Enhanced Interior Gateway Routing Protocol), are implemented to ensure efficient routing of data packets between different network segments. These protocols automatically adjust to network changes, optimizing the routing paths and enhancing overall network performance.
6. **Access Control Lists (ACLs):** ACLs are employed on routers to control access to the resources within the admin office. By defining rules that permit or deny traffic based on IP addresses or network segments, ACLs enhance network security. For instance, access to the web server can be restricted to specific hosts or networks, preventing unauthorized access.

**The Constructed Topology:**

Figure 1.1: Network Topology

**Topology Description:**

Three departments on campus—ECE, CSE, and an administration office—are intended to operate under the network topology that is given. The topology is described in full below:

**CSE Department:**

* **Router 1** is connected to the central switch.
* The department uses VLANs to separate networks:
  + **VLAN 10 (192.49.20.0/24)** for students.
  + **VLAN 20 (192.49.30.0/24)** for faculty.
* Several PCs are connected to the switch via VLANs:
  + PCs in VLAN 10: STD, STD, STD2, STD3, STD4.
  + PCs in VLAN 20: FAC, FAC2.

**ECE Department:**

* **Router 2** connects to the central switch through a switch.
* The department uses the network **192.49.10.0/24**.
* Four PCs (Tahmid , saadi , Ashik and Alvi) are connected to this network.

**Administration Office:**

* The administration office hosts critical servers:
  + **Web Server** (HTTP Server) with the IP address **172.49.10.5**.
  + **DNS Server** with the IP address **172.49.10.10**.
* PCs in the admin network use the IP range **172.49.10.0/24**.
* The admin network includes PCs such as PC6 and PC7.

**Interconnectivity and Routing:**

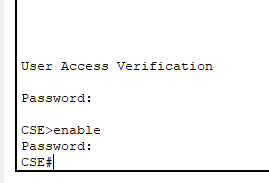
* + Router 1 (CSE) serial interface **Se2/0** connects to Router 2 (ECE) **Se2/0**.
  + Router 2(ECE) serial interface **Se3/0** connects to Router 3(Admin) **Se2/0**.

Table 1.1: IP Addresses:

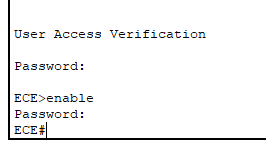
|  |  |  |
| --- | --- | --- |
| Router | IP Address | Network |
| R1 | 192.49.20.1  192.49.30.1  10.10.10.1 | 192.49.20.0  192.49.30.0  10.10.10.0 |
| R2 | 192.49.10.1  10.10.10.2  10.10.20.1 | 192.49.10.0  10.10.10.0  10.10.20.0 |
| R3 | 172.49.10.1  10.10.20.2 | 172.49.10.0  10.10.20.0 |
| DNS Server | 172.49.10.10 | 172.49.10.0 |
| HTTP Server | 172.49.10.5 | 172.49.10.5 |

**Result Analysis:**

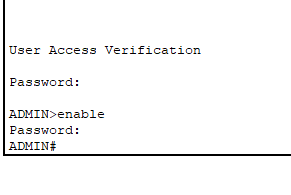
**Objective 1: All switches and routers should be password protected**

****

(a)

****

(b)

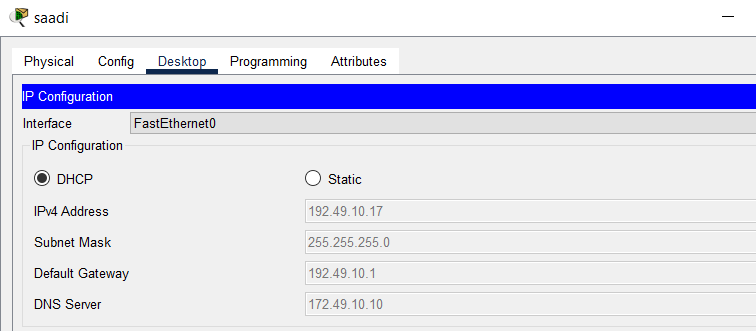
****

(c)

Figure 1.2: Password Protection Verification of Routers and Switches

**Objective 2: One of the departments would use the DHCP protocol to assign the IP addresses to all hosts of that network.**

The ECE Dept used DHCP protocol.

Figure 1.3: DHCP configuration of History department

**Objective 3: One of the departments would contain a VLAN system to separate students and faculties networks**

The CSE Dept was contains a VLAN system called VLAN10 and VLAN20

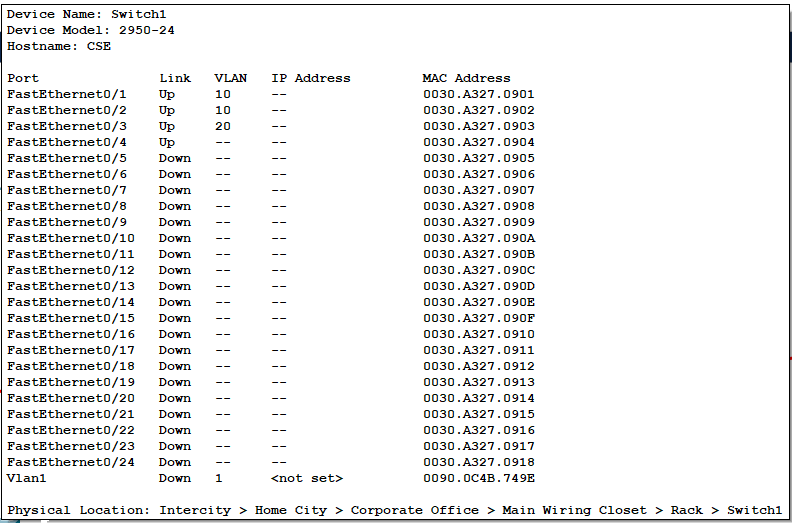


Figure 1.4: Vlan configuration for Switch 2 of Router 1

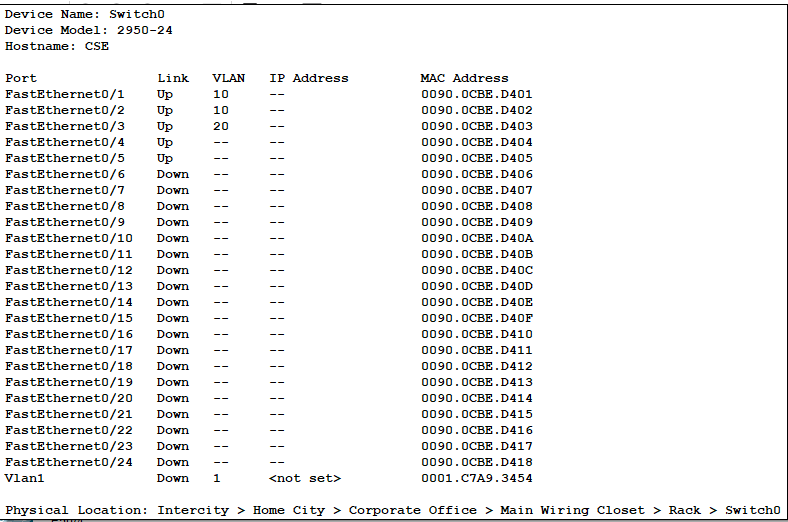


Figure 1.5: Vlan configuration for Switch 1 of Router 1

**Objective 4: A web server and a DNS server should be placed under the admin office:**

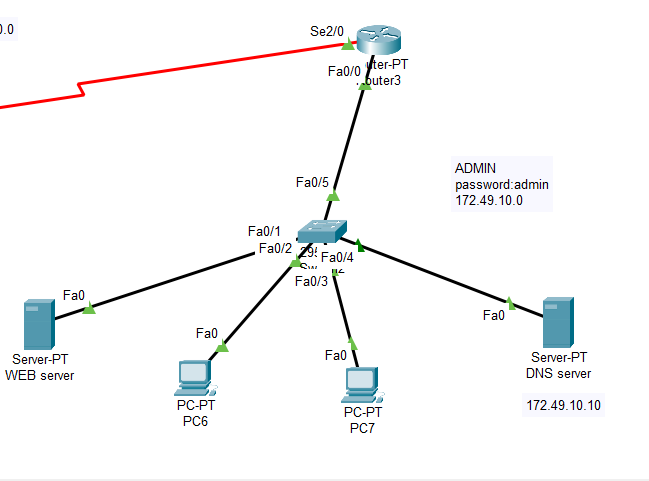
****

Figure 1.6: HTTP and DNS Server under Admin office

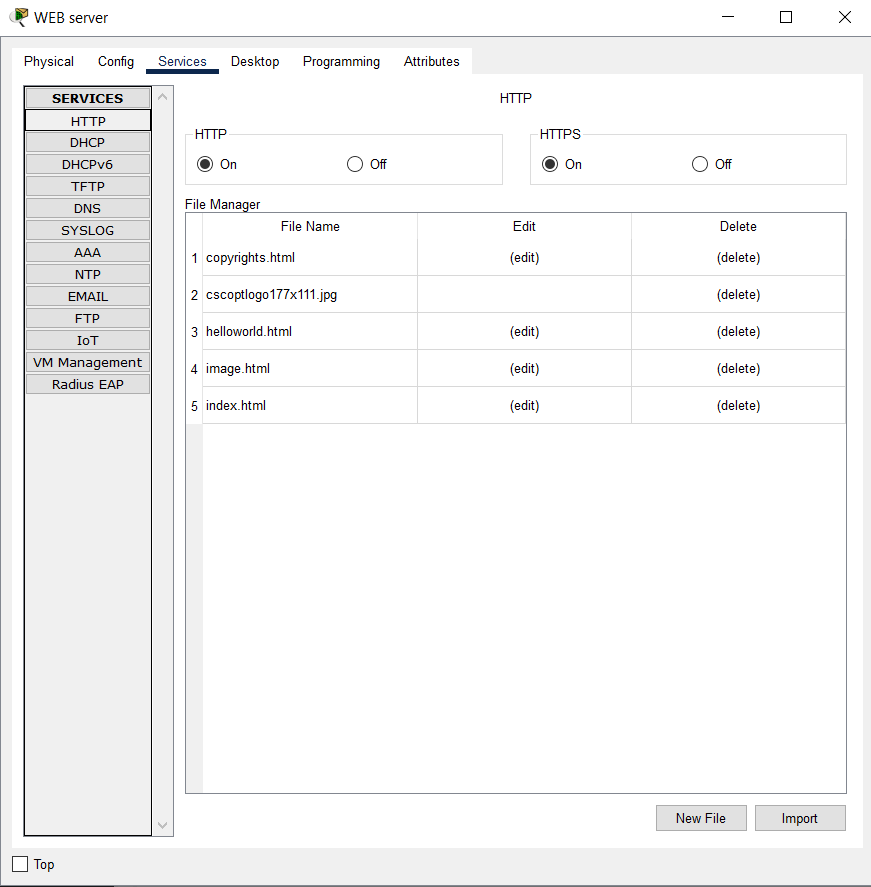


Figure 1.7: HTTP Server HTTP interface

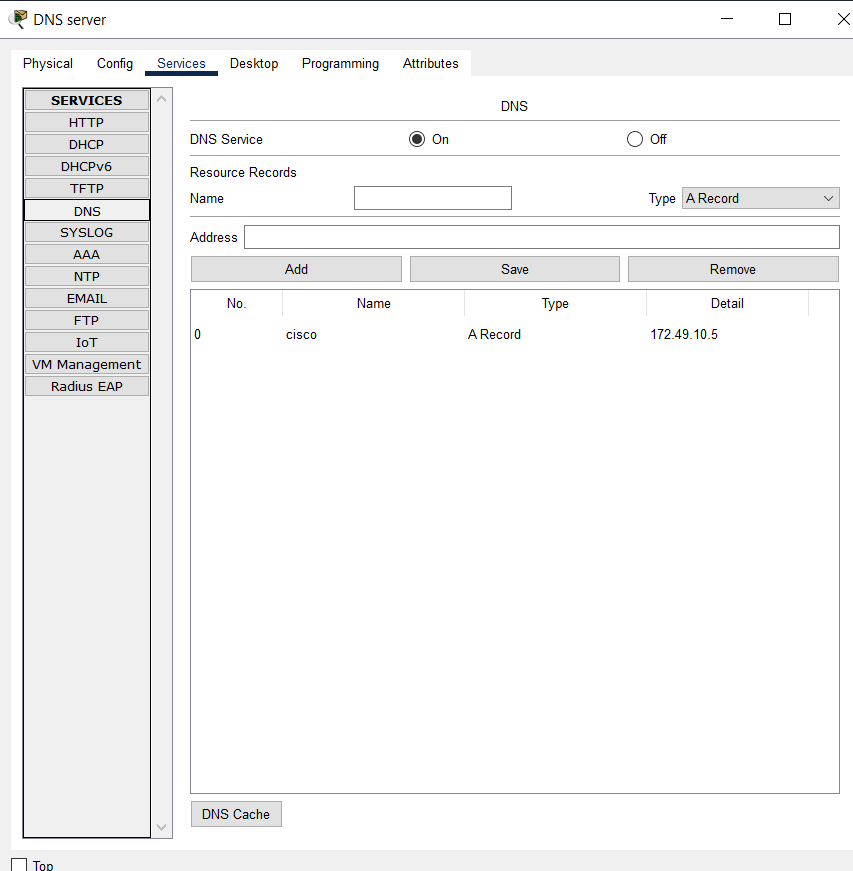


Figure 1.8: DNS interface of DNS Server

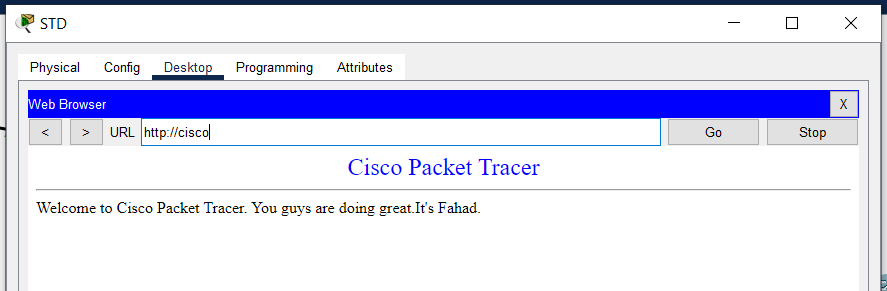


Figure 1.9: Web search result for Admin office’s website

**Objective 5: Any of dynamic routing protocols should be applied in the designed topology:**

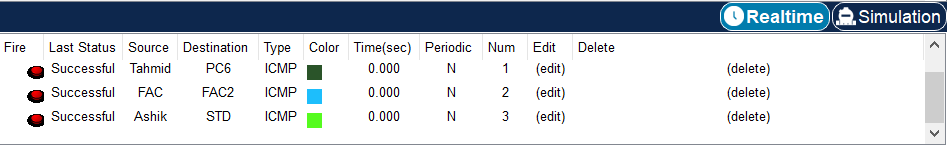
Applied protocol: OSPF

Tahmid, Ashik is under R2

PC6 is under R3

FAC, FAC2 is under R1

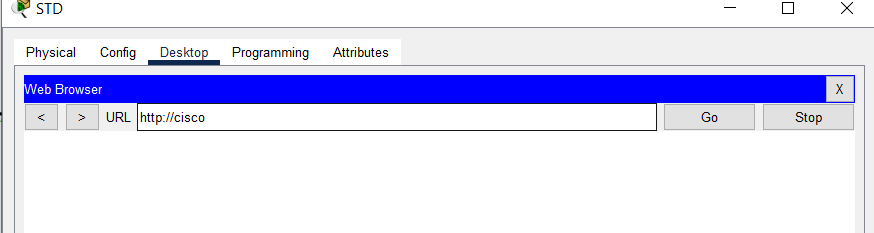
The packet transfer between these networks were successful.

Figure 1.10: Packet Transfer among R1, R2 and R3

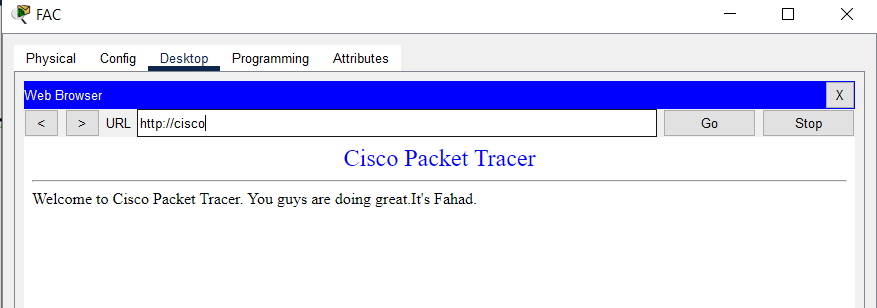
**Objective 6: Apply your desired ACL in routers to access the resources of the admin office:**

ACL was applied in VLAN 10 (Students) in Router 1.

STD is denied access to the admin page which is under Students:

Figure 1.11: Access denial of students

FAC is allowed access to the admin page which is under Faculty:

Figure 1.12: Access granted to Faculty

**Conclusion:**

By dividing the campus network into discrete departments, this network structure ensures efficient management and security. A comprehensive method to managing a large-scale network with varying security and performance needs is demonstrated by the use of VLANs, DHCP, dynamic routing protocols, and ACLs. The central administrative office houses vital servers that supply necessary services around the university and guarantee restricted access to these assets.