

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  Rifah Tasnia Joita  Roll: 1909005  Year: 4th  Dept: ECE | Submitted to  Md Foysal  Assistant Professor  Dept of ECE, KUET  Shah Muhammad Azmat Ullah  Lecturer  Dept of ECE, KUET |

**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.

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:

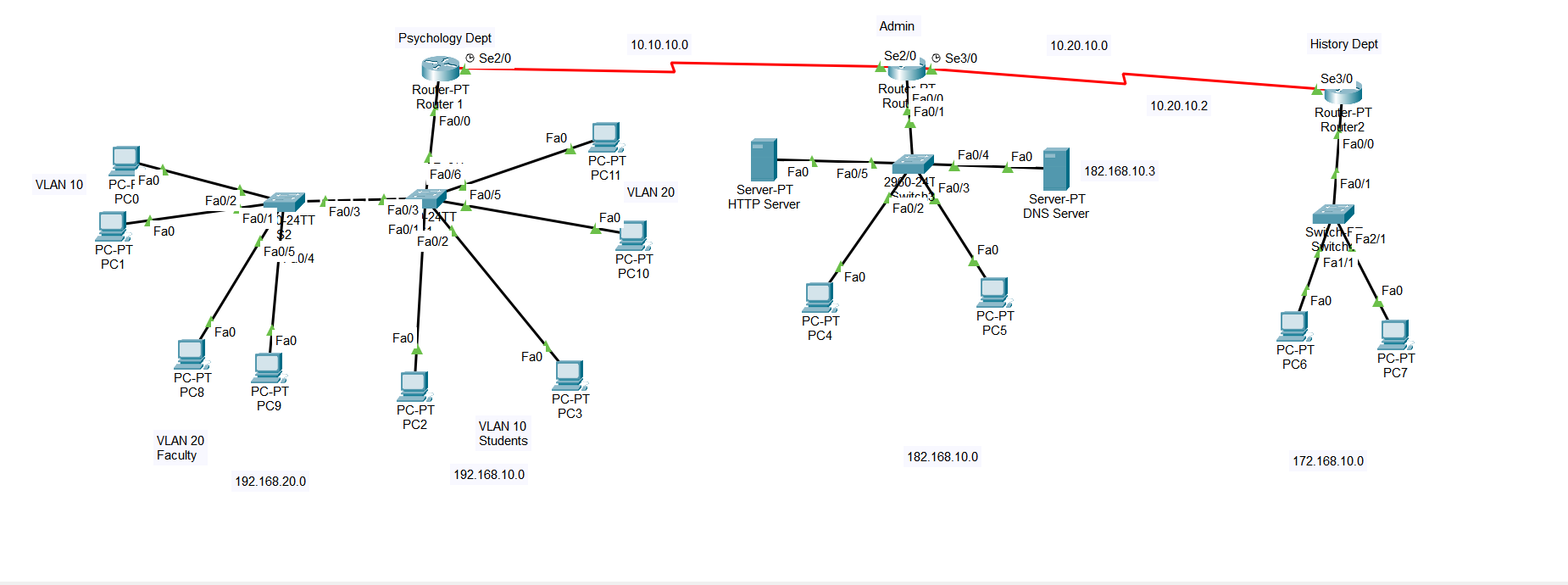
In today's educational institutions, robust and efficient campus networks are essential for ensuring seamless connectivity and resource sharing across various departments. This report presents the design and implementation of a campus network using Cisco Packet Tracer simulation software. The network comprises two departments—one employing Dynamic Host Configuration Protocol (DHCP) for IP address allocation and the other incorporating Virtual Local Area Networks (VLANs) to segregate student and faculty networks. Additionally, the administration office hosts a web server and a DNS server, with dynamic routing protocols facilitating communication between network segments. The network design also includes Access Control Lists (ACLs) on routers to control access to administrative resources, ensuring security and controlled access to critical services.

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:**

The provided network topology is designed for a campus environment consisting of three departments—Psychology, History, and an Administration Office. Here is a detailed description of the topology:

**Psychology Department:**

* **Router 1** is connected to the central switch.
* The department uses VLANs to separate networks:
  + **VLAN 10 (192.168.10.0/24)** for students.
  + **VLAN 20 (192.168.20.0/24)** for faculty.
* Several PCs are connected to the switch via VLANs:
  + PCs in VLAN 10: PC0, PC1, PC2, PC3, PC8, PC9.
  + PCs in VLAN 20: PC10, PC11.

**History Department:**

* **Router 2** connects to the central switch through a switch.
* The department uses the network **172.168.10.0/24**.
* Two PCs (PC6 and PC7) are connected to this network.

**Administration Office:**

* The administration office hosts critical servers:
  + **Web Server** (HTTP Server) with the IP address **182.168.10.2**.
  + **DNS Server** with the IP address **182.168.10.3**.
* PCs in the admin network use the IP range **182.168.10.0/24**.
* **Router Admin** connects to the main switch and provides routing capabilities for the administration network.
* The admin network includes PCs such as PC4 and PC5.

**Interconnectivity and Routing:**

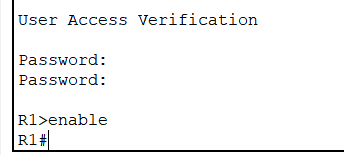
* + Router 1 (Psychology) serial interface **Se2/0** connects to Router Admin **Se2/0**.
  + Router Admin serial interface **Se3/0** connects to Router 2 (History) **Se3/0**.

Table 1.1: IP Addresses:

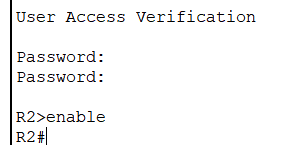
|  |  |  |
| --- | --- | --- |
| Router | IP Address | Network |
| R1 | 192.168.10.1  192.168.20.1 | 192.168.20.0 |
| R2 | 182.168.10.1 | 182.168.10.0 |
| R3 | 172.168.10.1 | 172.168.10.0 |
| DNS Server | 182.168.10.3 | 182.168.10.0 |
| HTTP Server | 182.168.10.2 | 182.168.10.0 |

**Result Analysis:**

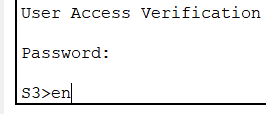
**Objective 1: All switches and routers should be password protected**



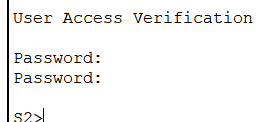
(a)



(b)



(c)

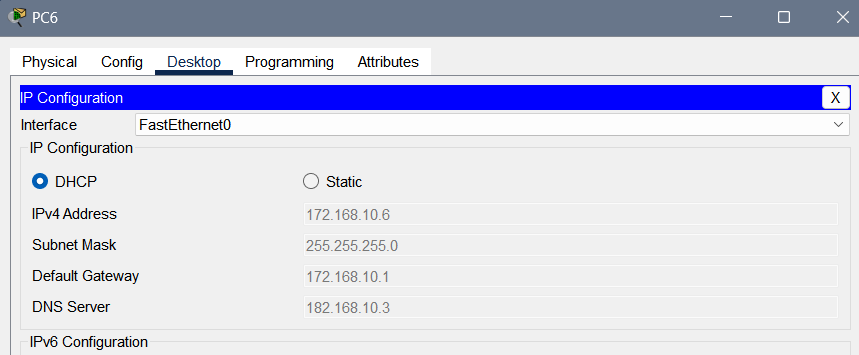


(d)

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 History 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 Psychology Dept was contains a VLAN system called VLAN10 and VLAN20

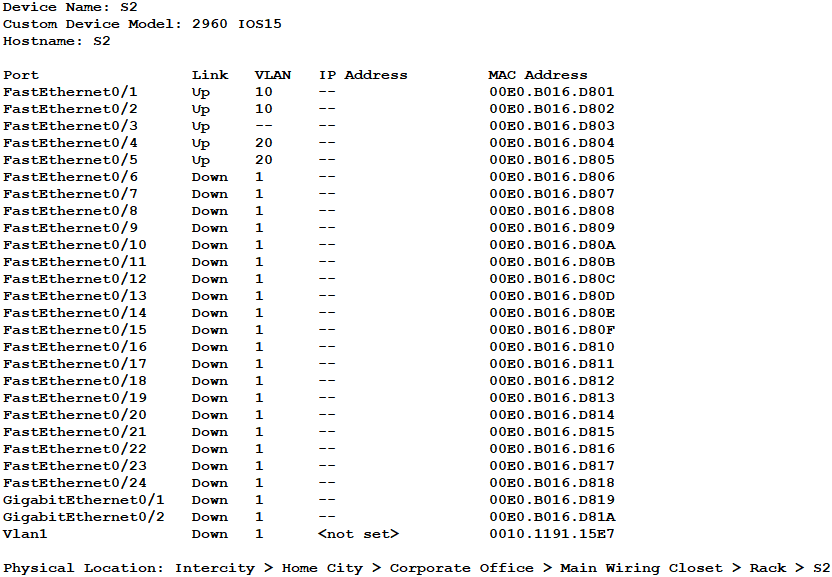


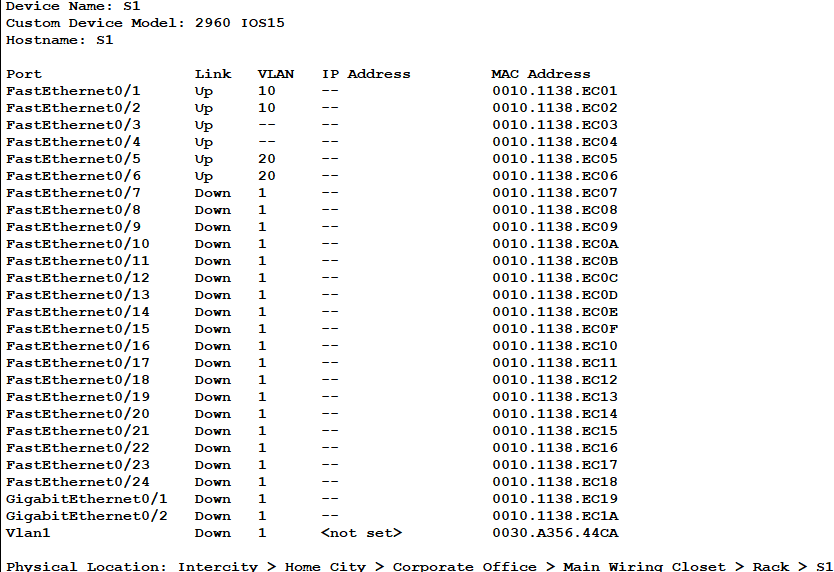
Figure 1.4: Vlan configuration for Switch 2 of Router 1

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:**

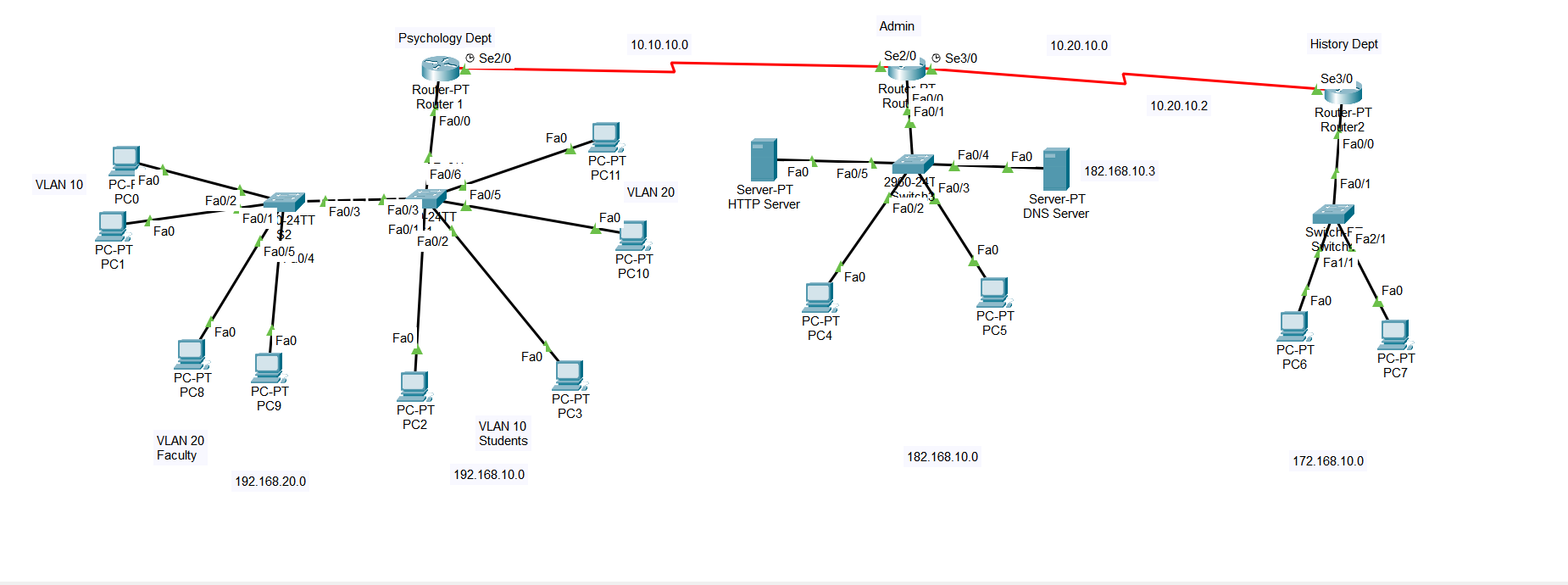


Figure 1.6: HTTP and DNS Server under Admin office

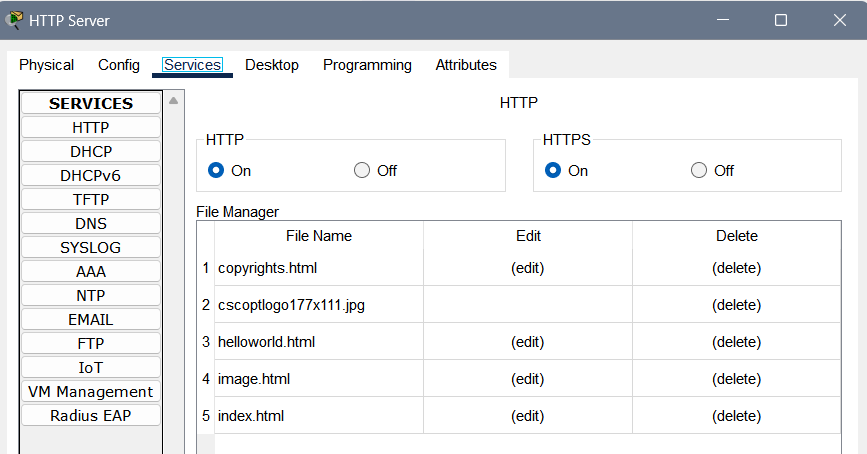


Figure 1.7: HTTP Server HTTP interface

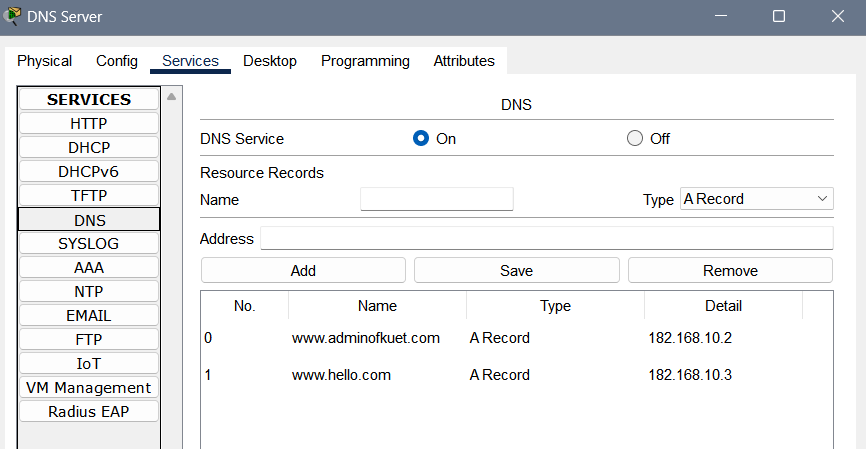
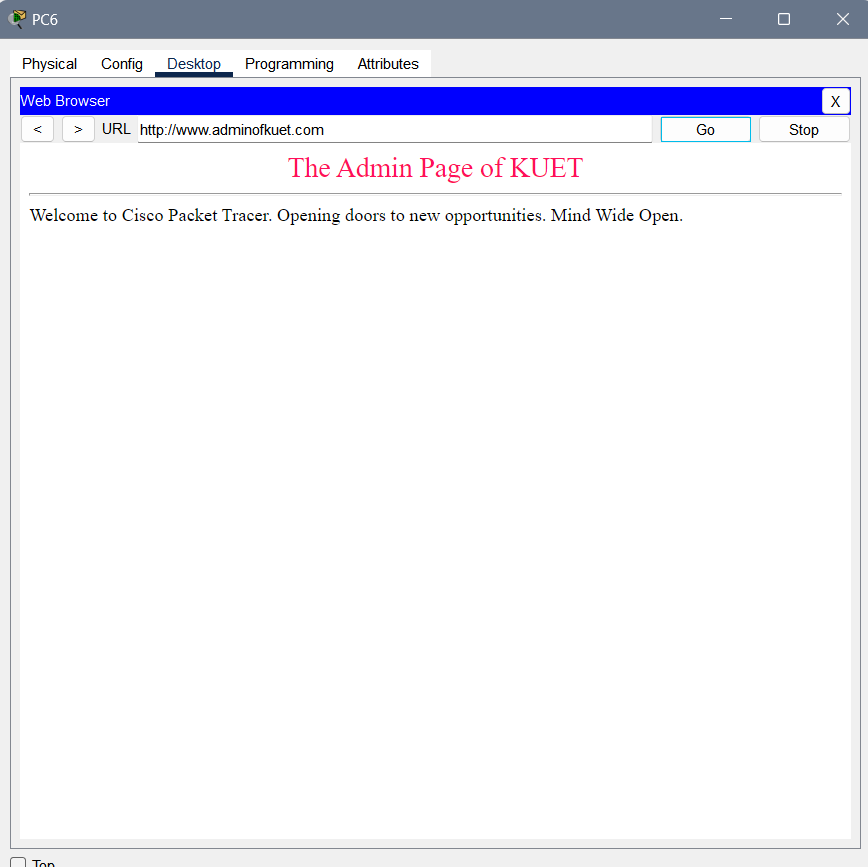


Figure 1.8: DNS interface of DNS Server

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:**

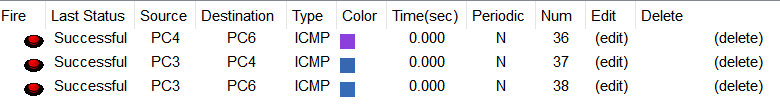
Applied protocol: RIP

PC4 is under R2

PC6 is under R3

PC3 is under R1

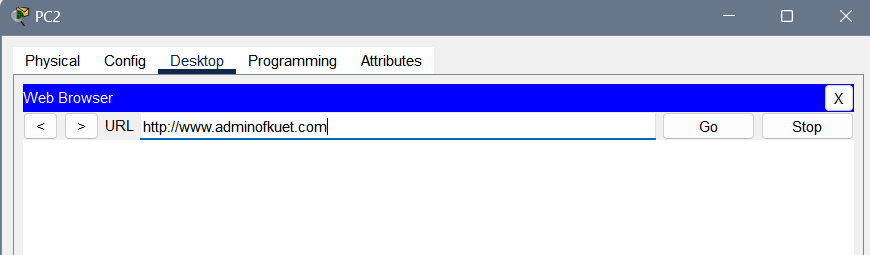
The packet transfer between these networks were successful.

Figure 1.10: Packet Transfer among R1, R2 and R3

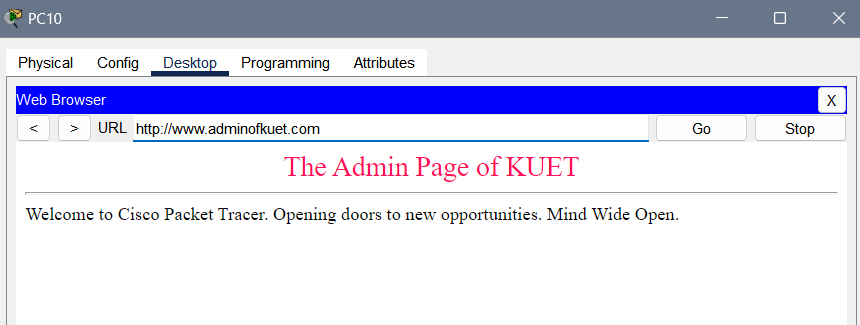
**Objective 6: Apply your desired ACL in routers to access the resources of the admin office:**

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

PC2 is denied access to the admin page which is under Students:

Figure 1.11: Access denial of students

PC 10 is allowed access to the admin page which is under Faculty:

Figure 1.12: Access granted to faculty

**Conclusion:**

This network topology effectively segments the campus network into distinct departments, ensuring security and efficient management. The use of VLANs, DHCP, dynamic routing protocols, and ACLs demonstrates a comprehensive approach to managing a large-scale network with various security and performance requirements. The central administration office hosts critical servers, providing essential services across the campus, while ensuring controlled access to these resources.