EE 8203 DESIGN AND MANAGEMENT OF DATA NETWORKS

ASSIGNMENT 01

NAME : THAKSHMILA M.D.

REG NO : EG/2018/3472

SEMESTER : 08

DATE : 15/09/2023

Topology

The star topology was chosen for the network design because it is easy to troubleshoot and manage, making it a good choice for a small network. In a star topology, each device is connected to a central switch. This makes it easy to add or remove devices from the network, and it also helps to isolate problems to individual devices.

Another advantage of the star topology is that it is a reliable topology. If one device fails, the other devices on the network will still be able to communicate. This is because each device is only connected to the central switch, and the failure of one device does not affect the other devices.

In the network design, the computers and other devices are connected to a central switch in each area. This central switch is then connected to the core switch, which is a layer 3 multilayer switch. The core switch provides routing and switching services for the entire network.

Here are some of the key benefits of using a star topology for a small network:

- Easy to troubleshoot and manage
- Reliable
- Scalable
- Secure
- Inexpensive

Network Media Design

Twisted-pair cable was chosen as the main network media because it is a popular choice for LANs. It is cost-effective and easy to install, and it is also resistant to interference.

Here are some of the advantages of using twisted-pair cable for LANs:

- Low cost: Twisted-pair cable is one of the most affordable types of network media.
- Easy to install: Twisted-pair cable is relatively easy to install, even for non-technical users.
- Interference resistant: Twisted-pair cable is resistant to electromagnetic interference, which can be a problem in noisy environments.
- Flexible: Twisted-pair cable is flexible and can be easily routed around obstacles.
- Available in different categories: Twisted-pair cable is available in different categories, which offer different data transfer rates and distances.

Cable Implementation:

Table 1: Cable information summary

Location	Cable Type	Speed/Model
PC to Switch	Copper (Twisted Pair) Straight	Fast Ethernet
Switches – Switches	Copper (Twisted Pair) Cross	Fast Ethernet
Switches – Layer 3 Switches	Copper (Twisted Pair) - Cross	Fast Ethernet
Layer 3 Switch - Router	Copper (Twisted Pair) - Cross	Fast Ethernet

Network connecting devices, links and redundancies

Network connecting devices:

Switches and routers were chosen as the network devices because they are the most common types of devices used to connect devices on a network. Switches are used to connect the computers and other devices to the network, while routers are used to connect the network to the internet. They are also relatively inexpensive and easy to manage.

In the network design, the following devices will be used:

- Core router: This is the main router in the network. It is responsible for routing traffic between the different parts of the network.
- Layer 3 (MLS) switch at core: This is a switch that can also route traffic. It is used to connect the different parts of the network and to the internet.
- Layer 2 switches in wiring closets on each floor: These switches are used to connect the computers and other devices on each floor to the network.
- Wireless access points for Wi-Fi coverage: These devices are used to provide wireless connectivity to the network.

Here are some of the advantages of using switches and routers for connecting devices on a network:

- Scalability: Switches and routers can be easily scaled to accommodate the growth of the network.
- Reliability: Switches and routers are relatively reliable devices.
- Security: Switches and routers can be configured to provide security for the network.
- Cost-effectiveness: Switches and routers are relatively inexpensive devices.

Redundancy:

In the network design, dual links will be used between the access layer, distribution layer, and core layer switches. This will ensure that the network is still accessible even if one link fails.

Here are some of the benefits of using dual links between switches:

- Increased reliability: If one link fails, the other link can still be used to keep the network up and running.
- Improved performance: Dual links can help to improve the performance of the network by providing more bandwidth.
- Reduced downtime: Dual links can help to reduce the amount of downtime caused by link failures.
- Increased security: Dual links can help to improve the security of the network by making it more difficult for attackers to disrupt traffic.

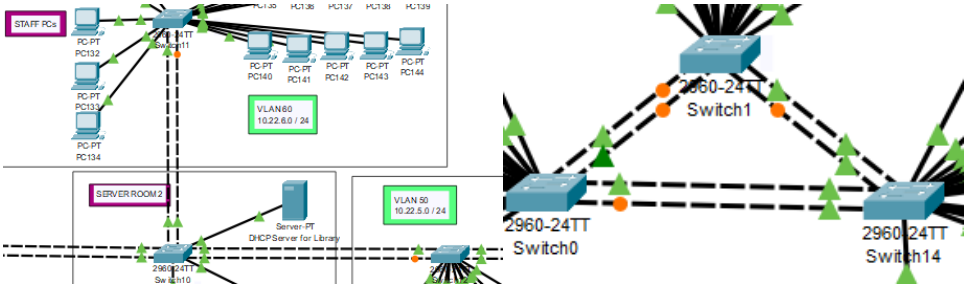

Figure 1: Dual links between switches

Physical layout of computers on the floor plan.

Floor Plan:

As shown in below Figures floor plan was designed for two floor building.

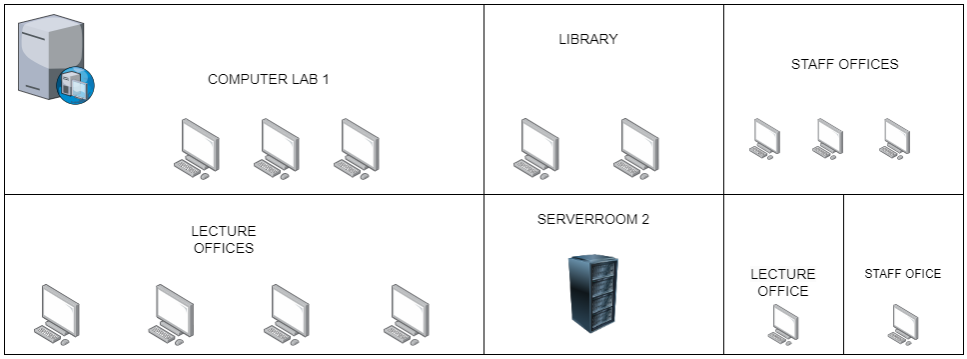

Figure 2: Floor plan for the second floor

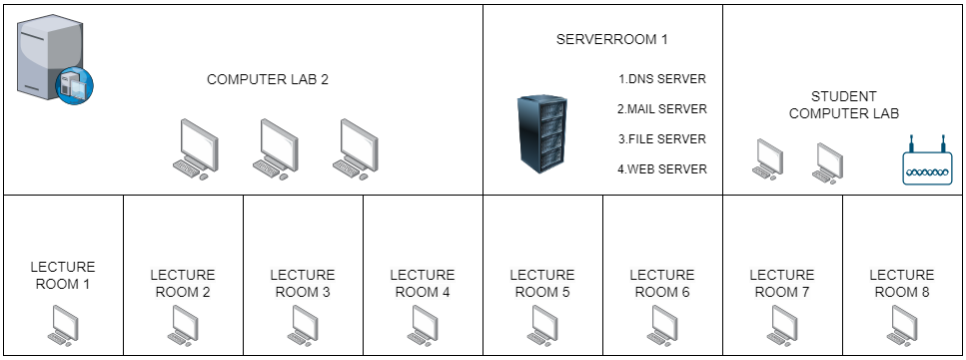

Figure 3: Floor plan for the first floor

The physical layout of the computers on the floor plan is as follows:

First Floor:

- Computer lab (51 computers): The computers in the computer lab will be connected to a 24-port 3 switches.
- Student computer lab (25 computers and Wireless devices): The computers in the student computer lab will be connected to a 24-port switch and wireless devices are connected to an access point.
- 8 lecture rooms (1 computer each): The computers in the lecture rooms will be connected to a 24-port switch.
- Server room: The server room will have one 24-port layer 2 switch, 24-port multilayer switch, four servers (Mail server, DNS server, File server and Web server) and a router.

Second floor:

- Computer lab (51 computers): The computers in the computer lab will be connected to a 24-port 3 switches.
- Library (15 computers): The 10 student computers and 5 staff computers in the library will be connected to a 24-port switch.
- Office rooms (25 computers): The 15 lecture computers and 10 staff computers in the office rooms will be connected to the same 24-port switch as the first floor.
- Server room: The server room will have one 24-port switch and a two DHCP severs.

IP plan and Addressing scheme:

IP plan of each network can be shown as following Table 2. This plan is developed considering minimizing of IP wastage. In order to minimize the IP wastage:

- Variable-length subnet masking (VLSM) allows to use different subnet masks for different parts of the network. This can help to minimize IP wastage by ensuring that the subnets are only as large as they need to be. For example, if we have a network with 100 devices, we could use a subnet mask of /24 for the entire network. However, this would mean that 254 IP addresses would be wasted. By using VLSM, we could create smaller subnets for the different parts of the network, such as the /28 subnet for the wiring closets. This would ensure that all of the IP addresses are used.
- Dynamic Host Configuration Protocol (DHCP) reservations allow to assign specific IP addresses to specific devices. This can help to minimize IP wastage by ensuring that the IP addresses are not used by devices that are not connected to the network. For example, we could create a DHCP reservation for the IP address of the server. This would ensure that the server always has the same IP address, even if the DHCP server is restarted.

Table 2: IP addressing scheme for each VLAN

Group	**Current Capacity**	**VLAN**	**Network**	**Subnet Mask**
Computer Lab 01 (Students)	51	10	10.22.1.0	255.255.255.0
Computer Lab 02 (Students)	51	10	10.22.1.0	255.255.255.0
Student's Computer Lab	25	20	10.22.2.0	255.255.255.192
Wireless AP at Students Lab	Not Limited	30	10.22.3.0	255.255.255.0
Sever Farm 01	4	40	10.22.4.0	255.255.255.0
Staff at Library	5	50	10.22.5.0	255.255.255.0
Office Area	25	50	10.22.5.0	255.255.255.0
Lecture Rooms	8	50	10.22.5.0	255.255.255.0
Students at Library	10	60	10.22.6.0	255.255.255.192

Network Design

Figure 4 shows the overall computer network design for the two storied building representing each floor and each sector.

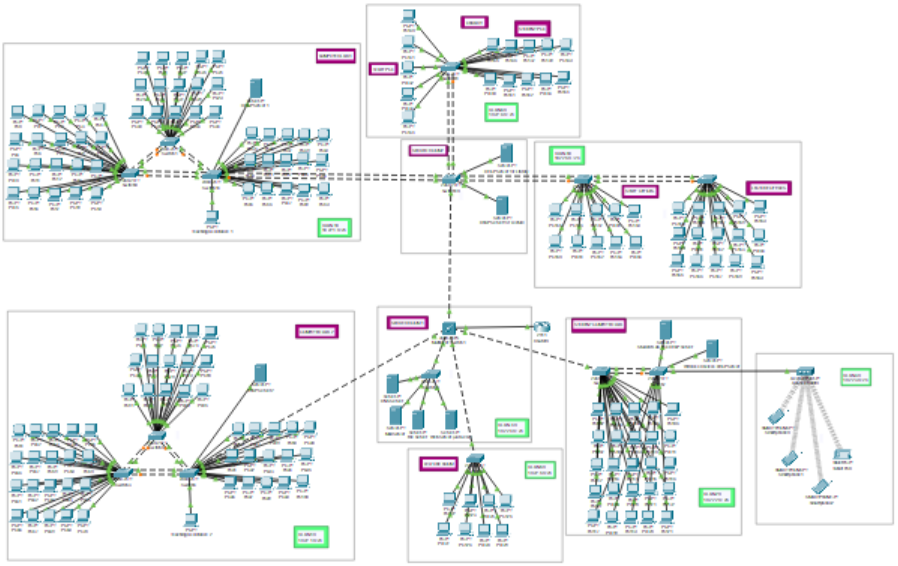

Figure 4: Overall network design of the building

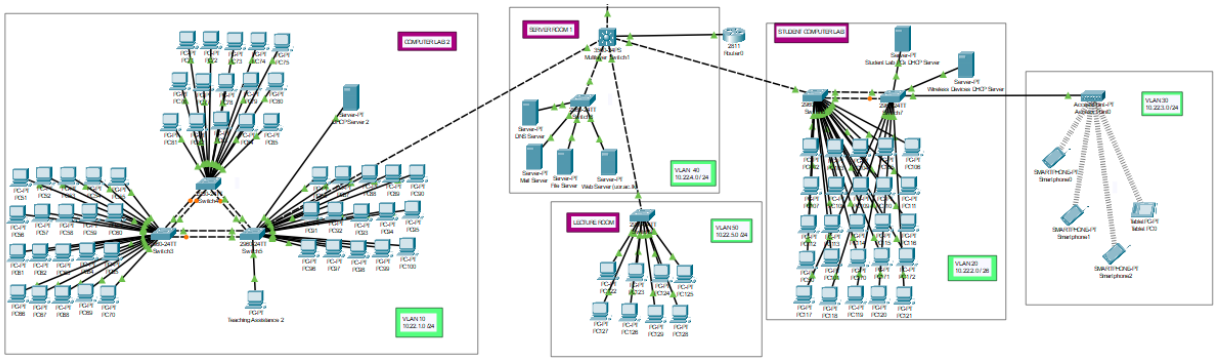

Figure 5: Network design of the First floor

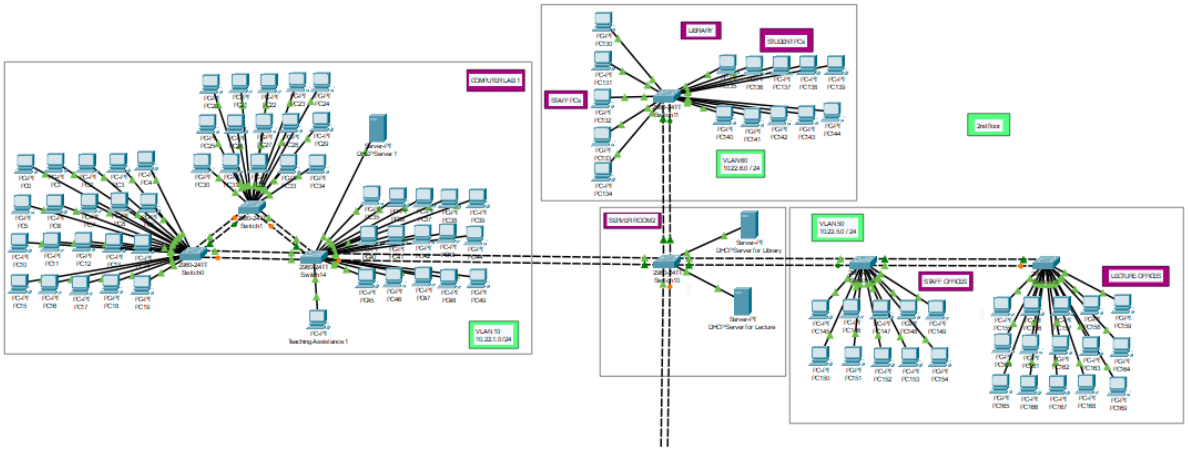

Figure 6: Network design of the Second floor

1. Computer Lab (1 and 2) network configurations

The computer network for the computer labs, which consists of 50 student PCs and 1 assistance PC, is shown in Figure 1. Both computer labs are assigned to the same VLAN, VLAN 10. DHCP is enabled on a server in this network to assign IP addresses to the PCs.

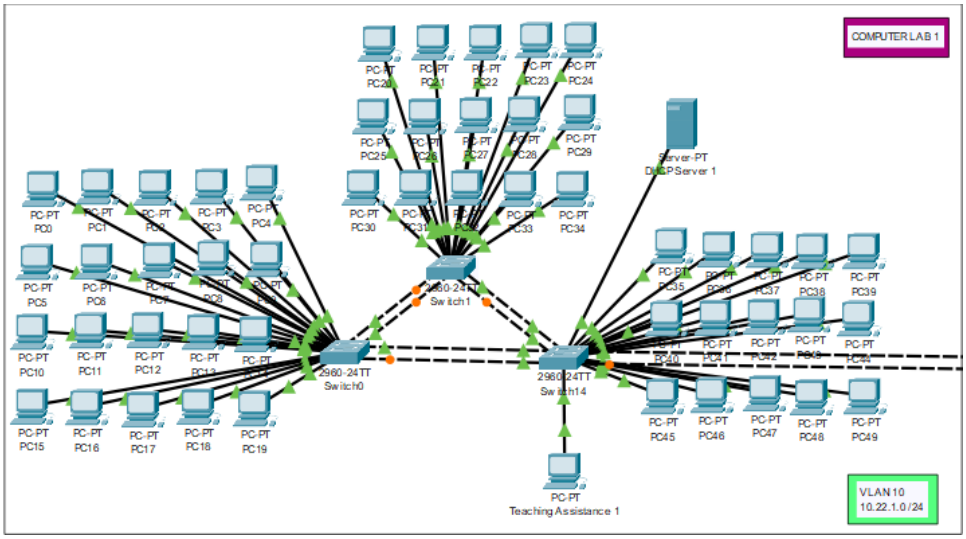

Figure 7: Network design for Computer lab 1

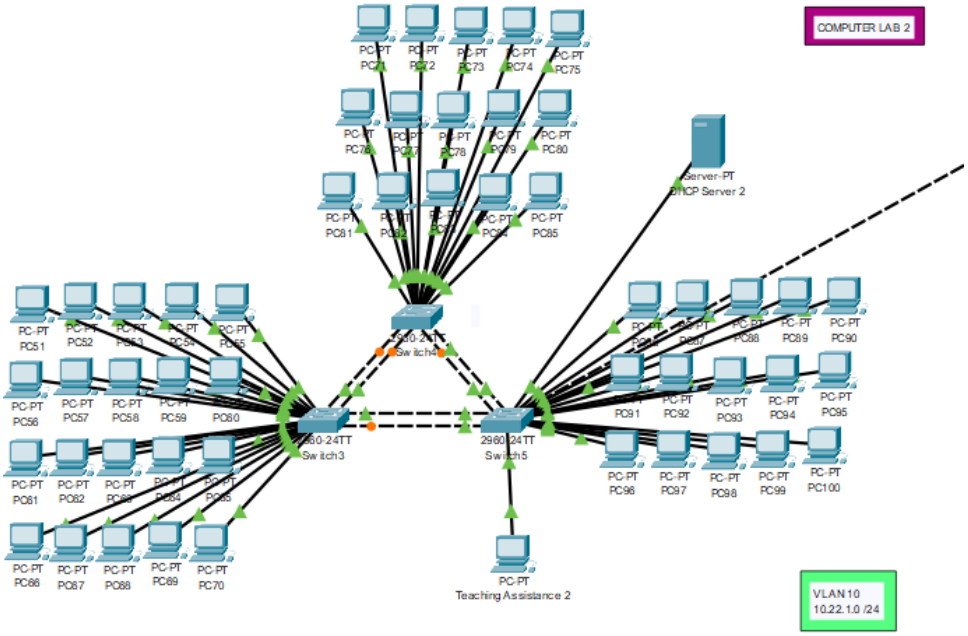

Figure 8: Network design for Computer lab 2

Dynamic Host Configuration Protocol (DHCP) allows each computer to obtain its IP address automatically from a pool of addresses managed by a DHCP server. The network configuration for each computer lab is as follows:

- The DHCP server is configured to assign IP addresses to the PCs within the respective computer labs.
- The configurations of the DHCP server are shown in Figure 9.
- The IP addresses obtained from the DHCP servers are shown in Figure 10.

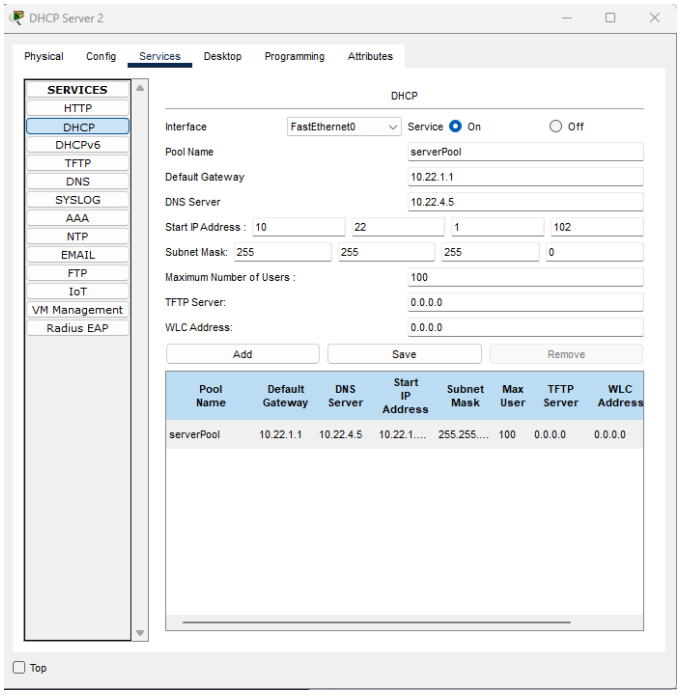

Figure 9: DHCP configuration for the server Computer lab 1

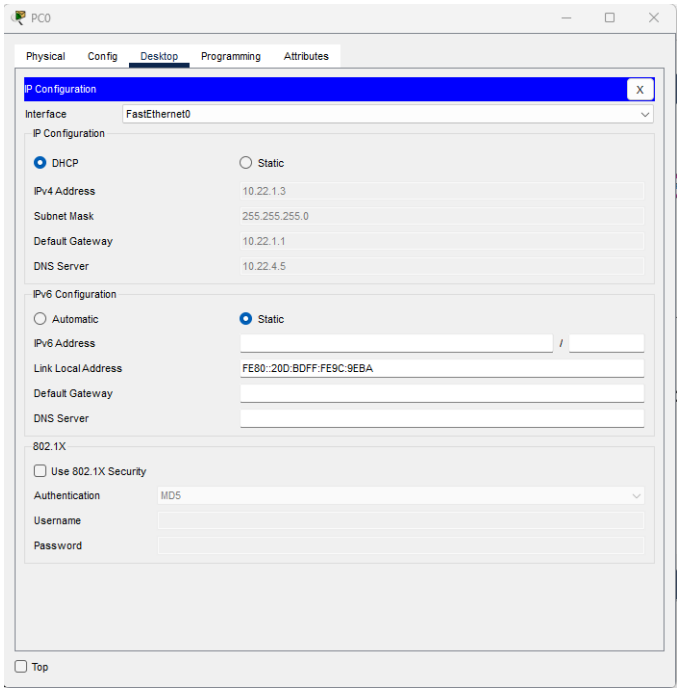

Figure 10: IP configuration for PC of Computer lab 1

2. Student computer Lab network configurations

The student computer lab has a separate DHCP server to assign IP addresses to the PCs. The lab is assigned to VLAN 20. The Wi-Fi network area has an access point (AP) that is assigned to a different VLAN, VLAN 30.

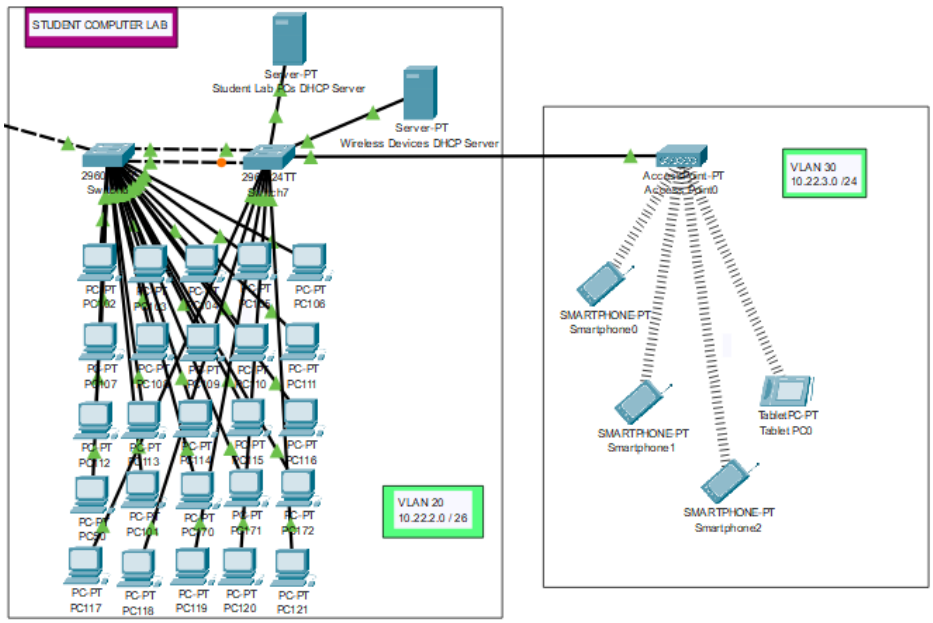

Figure 11: Network design for Student lab

Figure 12 shows the wireless AP configurations for the Wi-Fi network.

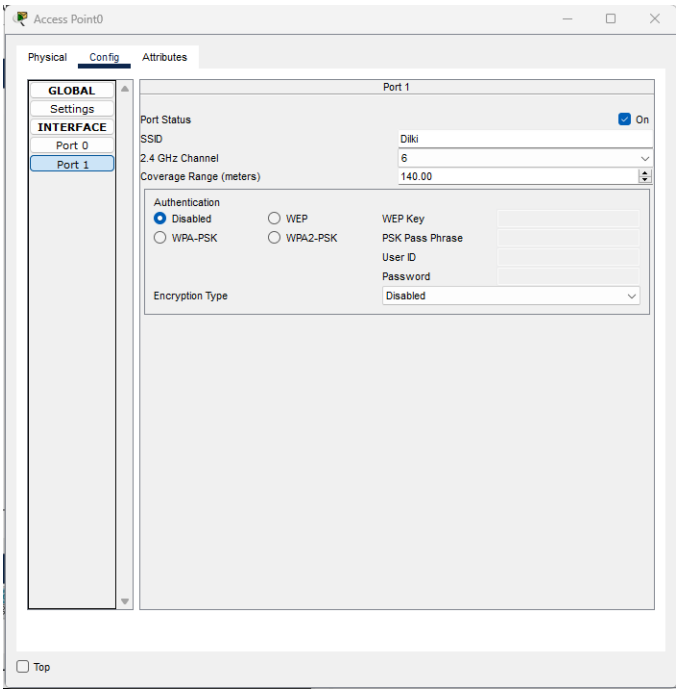

Figure 12: Configuration for the wireless access point

The configurations of the DHCP servers of both Student lab and wireless network. The no. of users of the wireless network is limited with max. no. of users of the DHCP server.

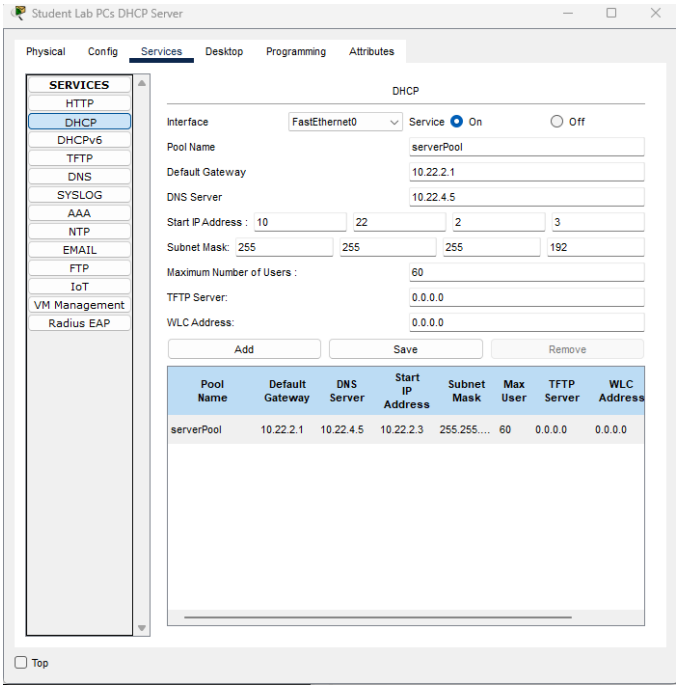

Figure 13: DHCP configuration for the server Student lab

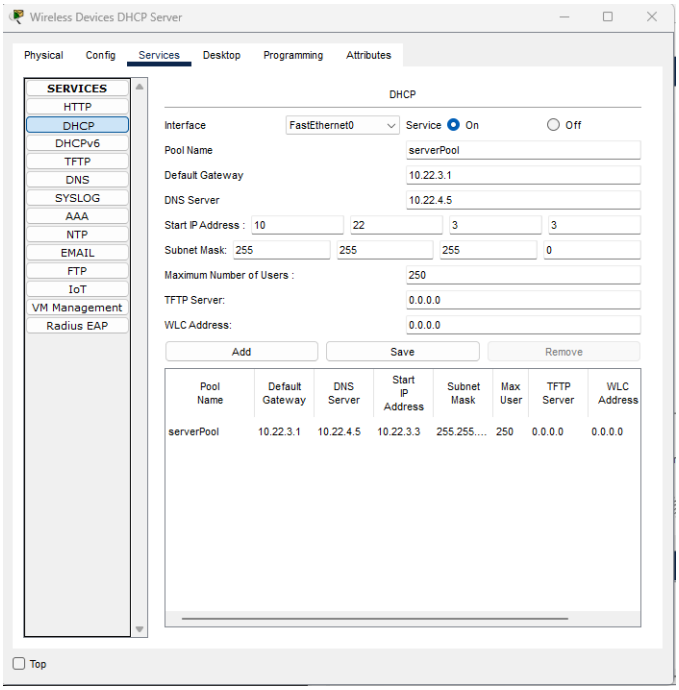

Figure 14: DHCP configuration for the wireless network

3. Lecture Room network configurations

There are 8 lecture halls and separate PC s for each

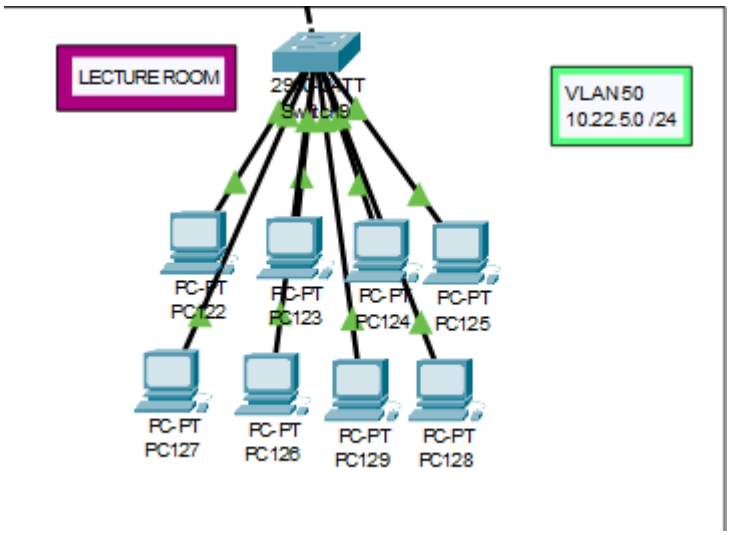

Figure 15: Network design for Lecturer rooms

4. Office network configurations

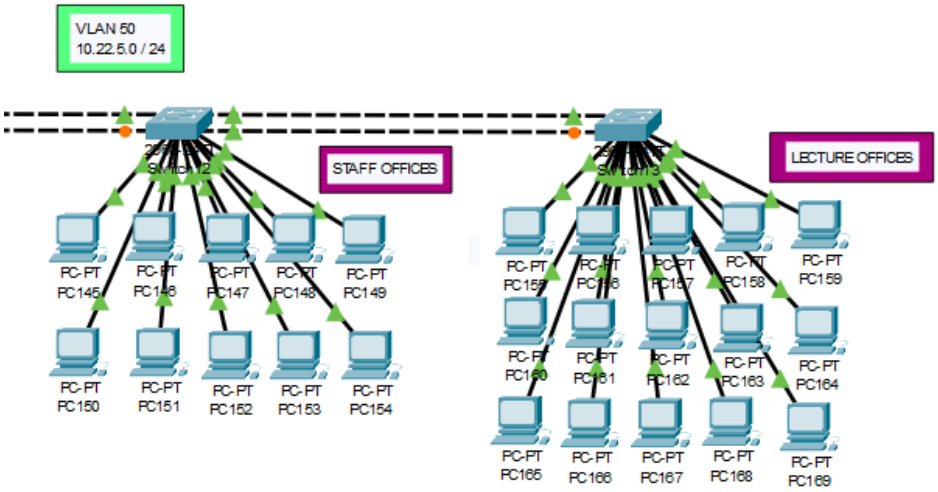

Figure 16: Network design for Office area

5. Library network configurations

The library has two VLANs: VLAN 60 for library students and VLAN staff (VLAN 50) for library staff PCs.

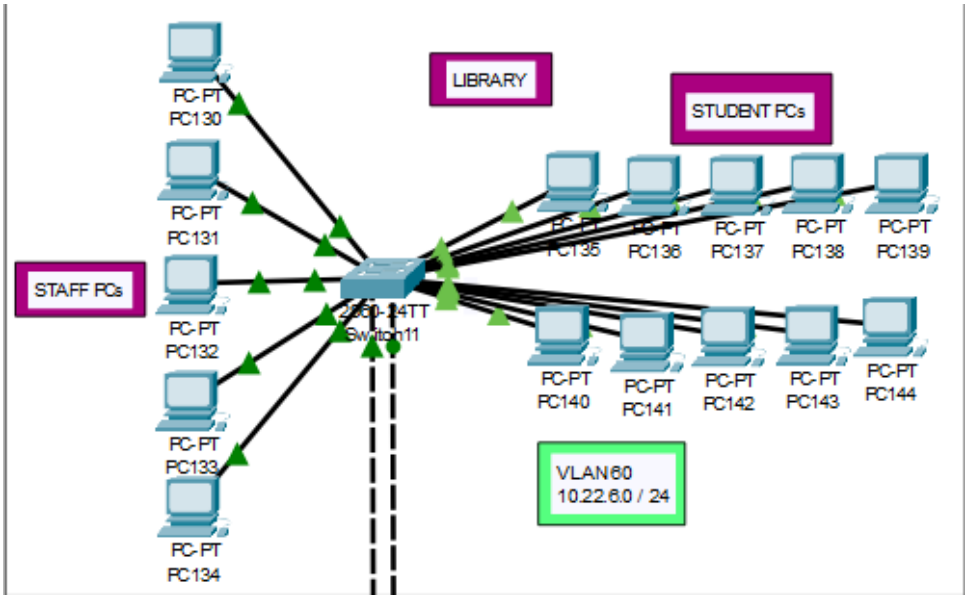

Figure 17: Network design for library network

6. Server Farms

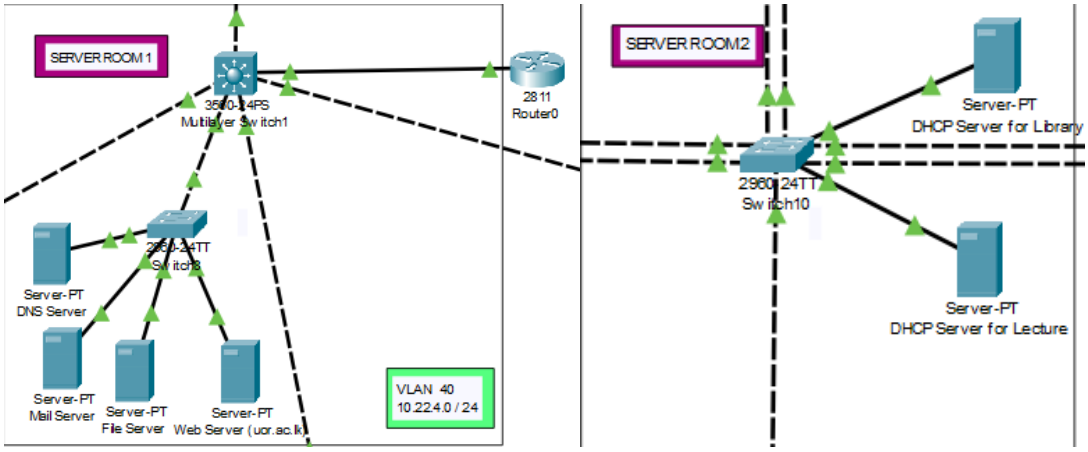

Figure 18: Server farm

Each floor has a separate server room. The main server room is located on the first floor, and the internet connection is patched to this server room.

1. DNS server:

A DNS server is a network service that translates domain names into IP addresses. The DNS server located in the server farm IP – 10.22.4.5 allocated a different DNS name for each server.

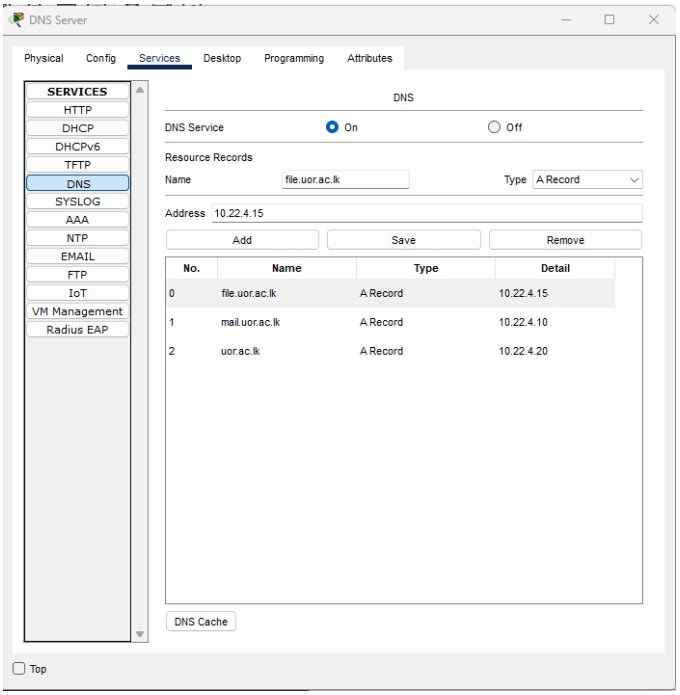

Figure 19: Configuration for DNS server

The following additional servers and network devices will be needed to implement the network in the main server room:

- A file server to store files for students and staff.
- A web server to host the faculty website.
- An email server to handle faculty email.

2. Mail server:

The mail server, which has the IP address 10.22.4.10, handles faculty email. The figure shows the configuration for the web server, which is accessed from the student PC.

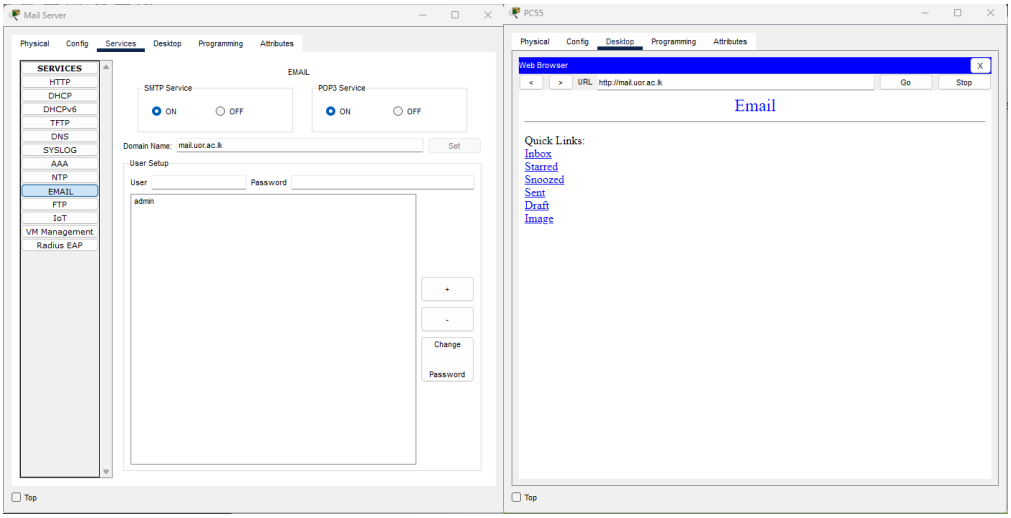

Figure 20: Configuration for mail server and the Mail server accessed from student PC

3. File server:

A file server with the IP address 10.22.4.15 allows students to access course materials from home. The figure shows the configuration for the web server, which is accessed from the student PC.

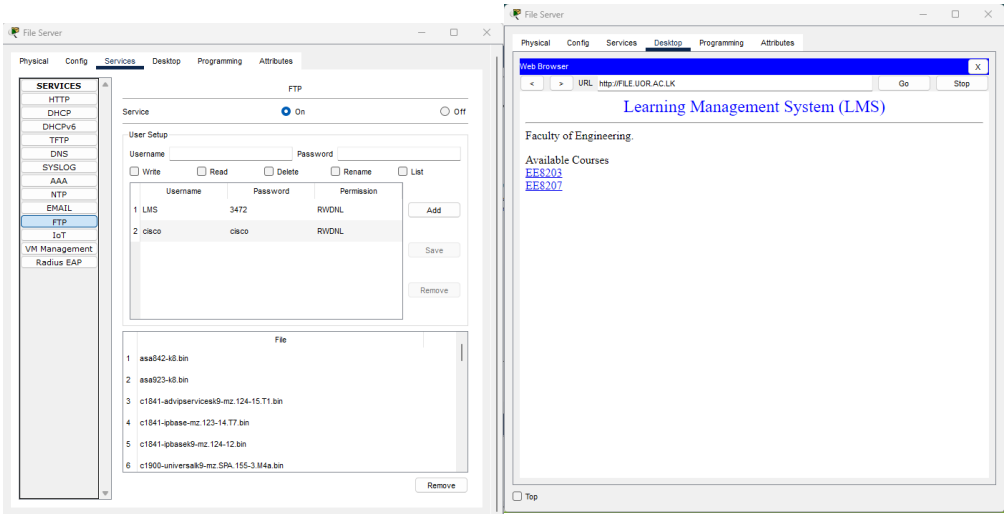

Figure 21: Configuration for file server and the file server accessed from student PC

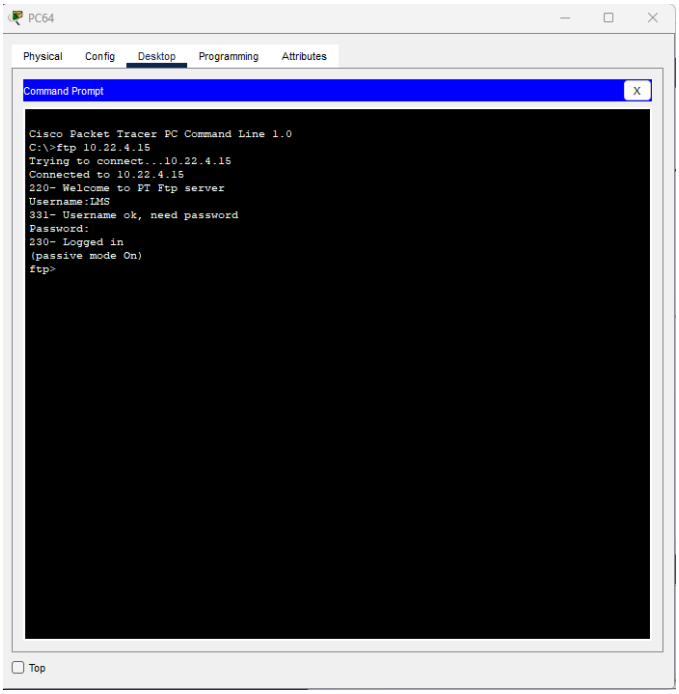

Figure 22: Check the ftp services by student computer

4. Web server:

A web server with the IP address 10.22.4.20 hosts the faculty website. The figure shows the configuration for the web server, which is accessed from the student PC.

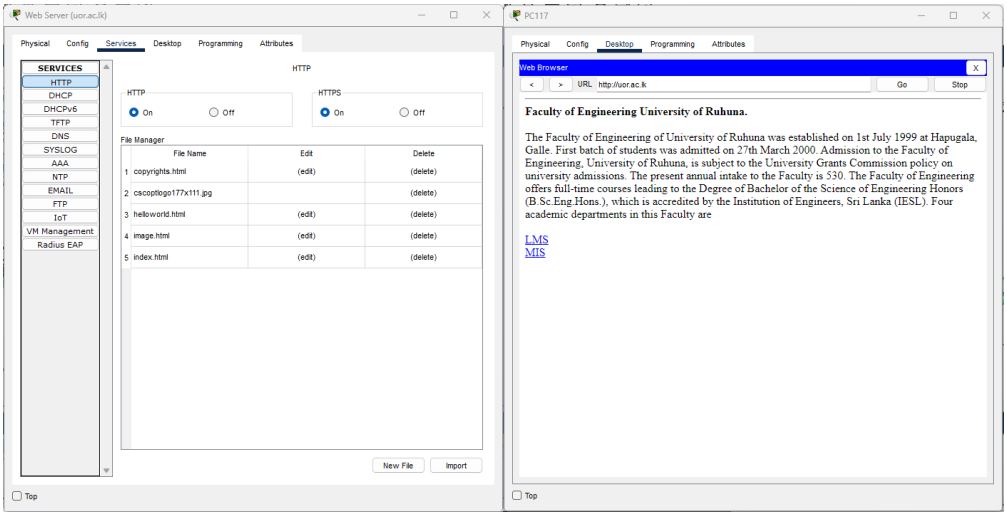

Figure 23: Configuration for web server and the web server accessed from student PC

Network Constraints:

The following constraints of the network design were implemented.

1. To prevent devices connected to the wireless AP from accessing the internet, an ACL (access control list) was implemented to block internet access from the wireless network. This is shown in Figure 24.

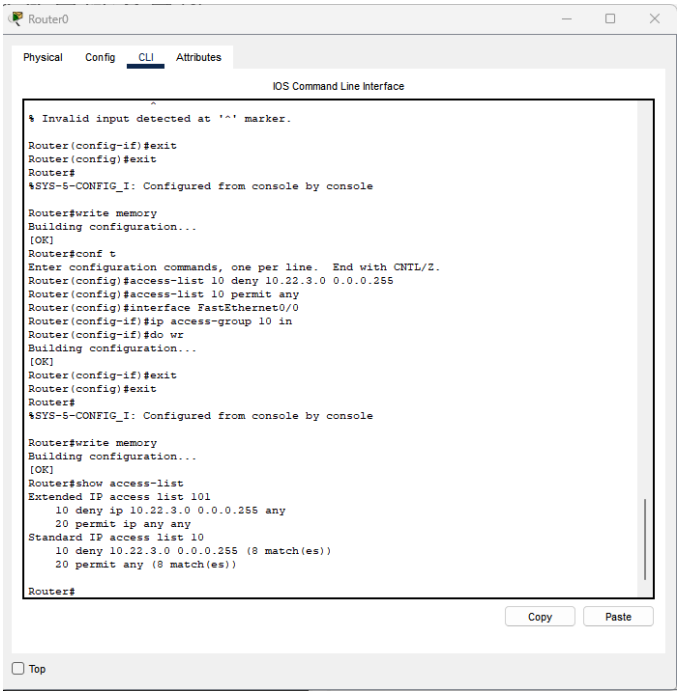

Figure 24: ACL for blocking internet access of wireless network

Following figure 25 shows that for the device in wireless network is unreachable to the internet and ACL is successfully initiated.

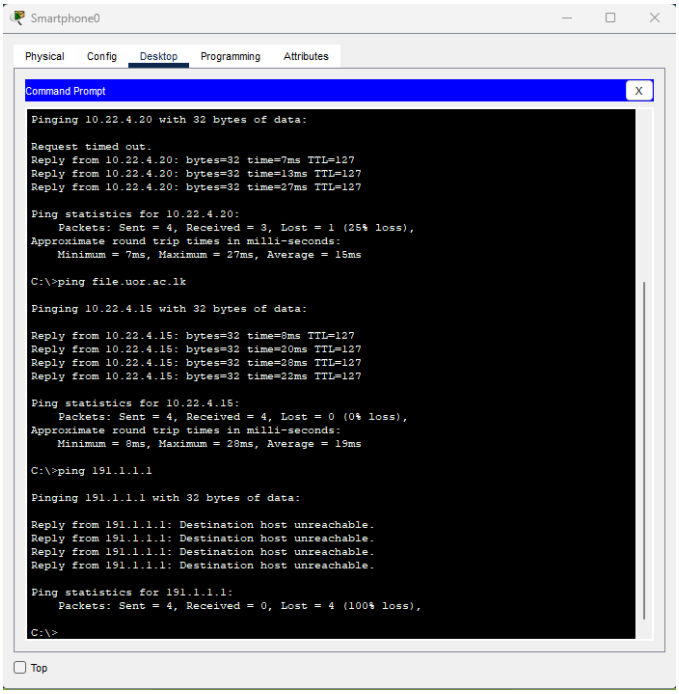

Figure 25: Wireless network is unreachable internet access

1. Students should be able to access the file server (file.uor.ac.lk), the faculty website (uor.ac.lk) and the mail server (mail.uor.ac.lk) successfully as in the Figure.

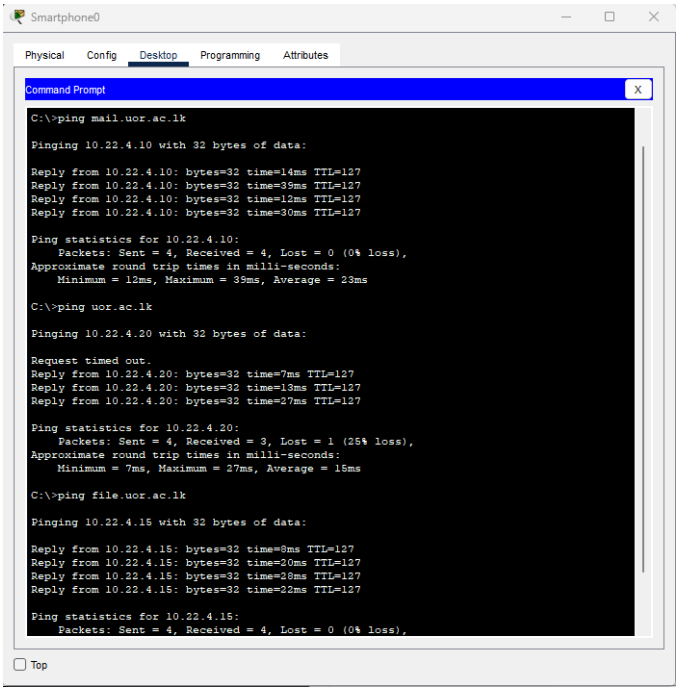

Figure 26: Student access the mail, web and file servers

2. To restrict student access to staff computers, the student-accessed computers are placed on a separate VLAN, VLAN 50. An ACL is then used to block student access to the staff computers. This is shown in Figure 27.

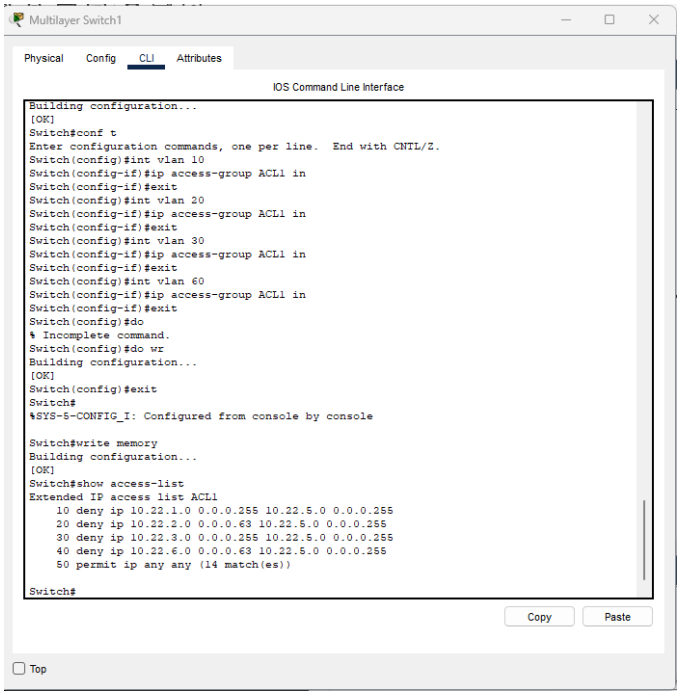

Figure 27: ACL for blocking student access to staff network

Figure 28 shows, a student PC is the computer lab 2 try to access the PC of the Teaching assistant and it is unreachable.

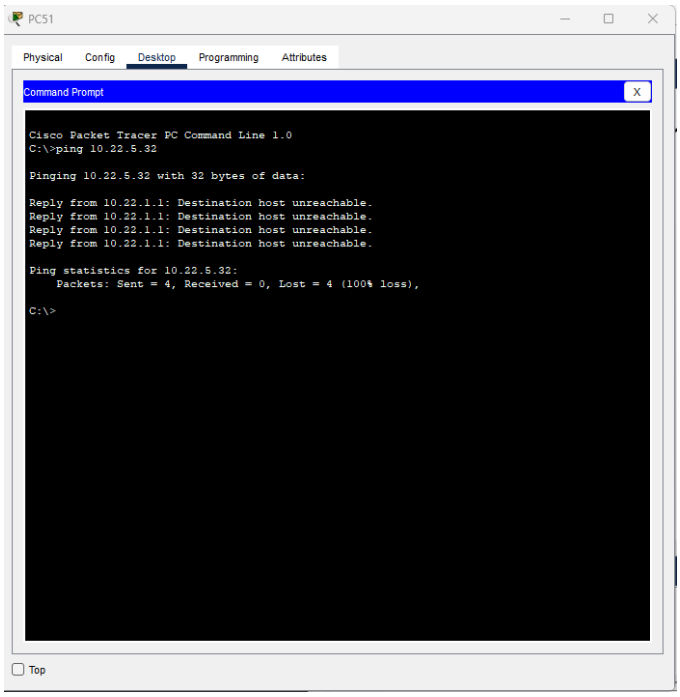

Figure 28: Staff PC is unreachable to student pc when pinging

NAT configurations:

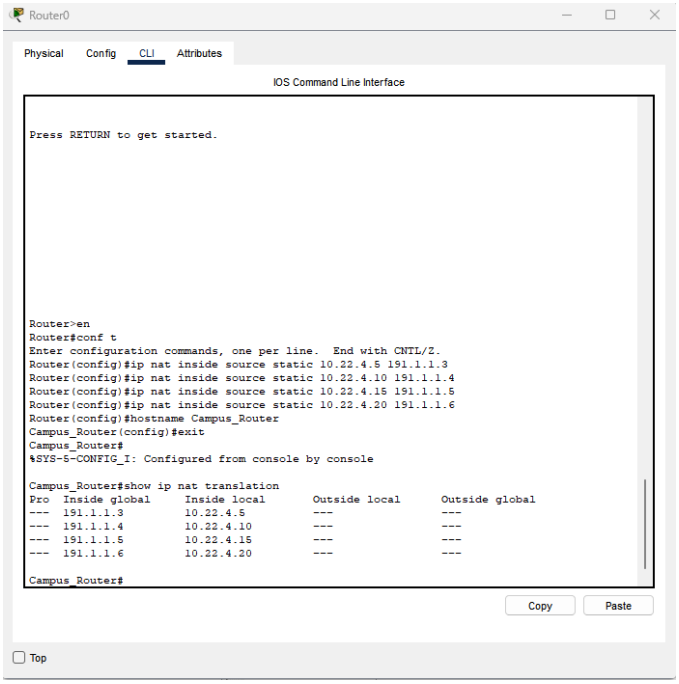

Figure 29: NAT configurations of the Core router

Routing configurations:

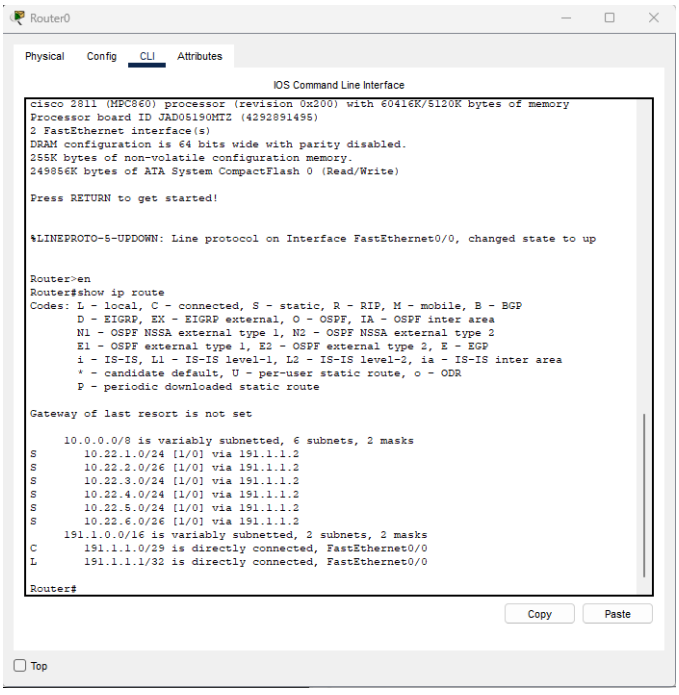

Figure 30: Routing Configuration for core router

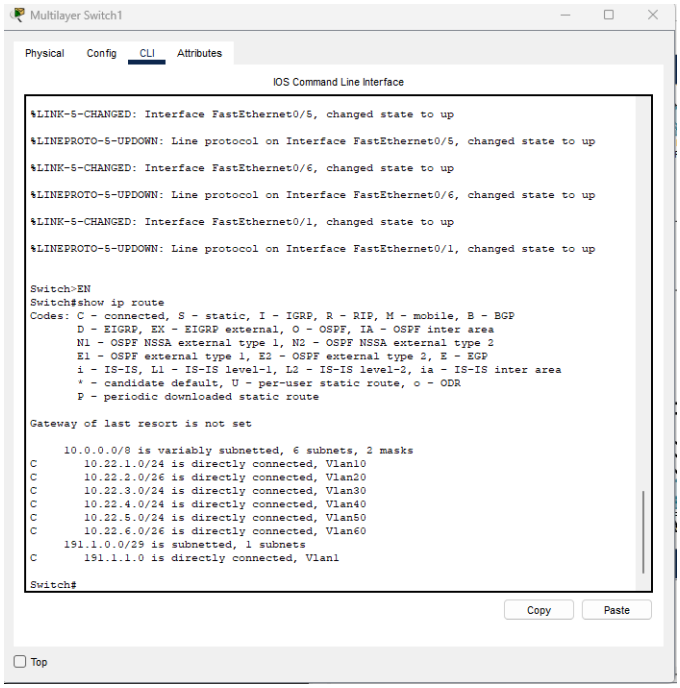

Figure 31: Routing Configuration for MLS