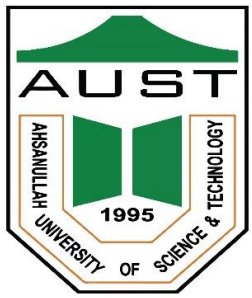


Ahsanullah University of Science and Technology

Department of Electrical and Electronic Engineering

Assignment

Course No: CSE 4295
Course Title: Multimedia Communication

Submitted By:

Group NO: 04

Group Members	Student ID
Md. Minhazur Rashid Adnan	190105017
Farhan Muhib Efty	190105022
Md. Esfaque Ahmed	190105041
Tahera Shormila Toma	190105049
A.K.M. Aktaruzzaman Shuvo	190105050

Solutions of Question NO: 1

▪ Network Planning and Requirements Gathering:

Zone	Total PC	Software Required	Network Service Required	Comment
DSP Lab [4B01]	30	Matlab/Octave Pspice/LTspice etc.	1. Roaming user profile 2. File/ Task submission to teacher etc	Internet Connectivity in selected PC's ONLY
VLSI Lab [4B03]	20	Linux Server, Cadence, Quartues Prime, Modelsim, AutoCAD	All PC's are Broadband Connected	Network Service setup to meet its specific needs and goals.
Microprocessor and Digital Lab [4B08]	20	Arduino IDE, AutoCAD, Proteus, Quartus, Matlab	Task/File Submission to teacher	Internet Connectivity in selected PC's ONLY
Simulation Lab [4B02]	30	Pspice, Orcade Codeblock, Matlab	Task/File Submission to teacher	Internet Connectivity in selected PC's ONLY

The goals and objectives of a network deployment project can vary depending on the expectations and requirements of the organization. However, some common goals and objectives associated with such programs are as follows:

Purposes:

Enhanced Connectivity: Establish a strong and dependable network infrastructure to improve the organization's overall connectivity and communication capabilities.

Scalability: Develop the network to allow future expansion and increased bandwidth, user, and device requirements.

Enhanced Performance: Ensure that the network performs smoothly and consistently with fewer delays and interruptions.

Implement stringent security procedures for protecting sensitive data, restrict illegal access, and defend against any cyber threats.

Optimize network configuration to achieve a mix of performance and cost-effectiveness, taking into account both the original investment and continuous maintenance.

Strengthening Security: Putting strong safety measures in place to safeguard sensitive data, prevent illegal entry, and reduce potential cybersecurity concerns.

Expense Efficiency: Analyzing and bringing about cost-effective network solutions that are in line with the organization's cost and economic objectives

Enhanced Productivity: Improving productivity and user experience by streamlining network operations, decreasing downtime, and enhancing network performance.

Efficient Administration: Create a network topology that is convenient to administer, set up, and monitor, decreasing network management complexity. Create a network framework to enable emerging technologies and applications that will improve the organization's operations.

Network Design: Develop the entire network according to the organization's performance, scalability, and security requirements.

Hardware and Software Implementation: Acquire and install the necessary networking hardware, such as routers, switches, and access points, as well as software components such as firewalls and intrusion detection systems, in accordance with the network plan.

Configuration: Configure network devices and components to ensure smooth connectivity and peak performance. This includes configuring IP addresses, routing protocols, and VLANs as necessary.

Compliance and Regulatory Adherence: Assure that the network infrastructure adheres to industry-specific regulations and standards.

Enhanced User Experience: Improving network quality, dependability, and responsiveness in order to increase user happiness and productivity. To protect sensitive information, security techniques such as firewalls, encryption, access controls, and intrusion detection systems are used. evaluating and quality assurance entails thoroughly evaluating the network infrastructure before to deployment in order to discover and resolve any connectivity, performance, or security concerns.

Paperwork: For future reference and troubleshooting, create detailed documentation outlining the network architecture, configuration settings, and procedures. The specific network services required may vary based on the needs of an organization or individual, but some frequent ones to consider are:

Internet Access: Internet access is an essential requirement for the majority of networks, allowing for web surfing, interaction with external networks, and different business operations such as email and file sharing.

File Sharing: Network users can exchange files, improving collaboration and resource sharing through simple and efficient file sharing and collaboration.

Printing: Network printing allows users to print documents from any connected device, minimizing the requirement for multiple printers and simplifying the printing procedure.

Email: Users are able to access their email accounts from any network-connected device, enabling electronic connection with coworkers, clients, and associates via email messages.

Distant connectivity: Remote access capabilities allow users to establish a connection to the network from remote locations, allowing them to function remotely and access network resources from any part of the entire world.

Audio and visual communication: Users can engage in live voice and video interactions through services like instant messaging and video conferencing, facilitating real-time connections

Web conferencing: Web conferencing enables users to have real-time, face-to-face conversations over the Internet, which aids in cooperation and training.

Security: Network security is crucial for safeguarding the network against unauthorized entry, malware, and various risks. This entails employing security measures like firewalls, intrusion detection systems, and antivirus software.

Management: Management of network-specific services, which includes tasks such as configuration, user management, and problem resolution, may vary based on the specific needs of the organization. This ensures that users experience smooth operations while utilizing the network.

In general, the network services required will be contingent upon the unique requirements of the organization or individual. However, the aforementioned services are some of the most commonly sought-after in modern networks.

It is essential, when establishing a network, to thoroughly evaluate all intended services and select the appropriate technology to support them. Additionally, the network should be secure, reliable, and capable of expansion. By building the network correctly, the organization can ensure that it meets its future goals and expectations.

Solutions of Question NO: 2

▪ Network Design and Topology:

Topology Used(Mesh):

Mesh Topology is a network topology in which every device in the network is connected to every other device, resulting in a full or partial mesh structure. In a full-mesh topology, every device has a direct link to every other device, whereas only certain devices have direct links to others in a partial-mesh topology. In your scenario, a mesh topology would connect each student, faculty, and staff member's device (PCs, printers, etc.) to every other device in the network, generating a complicated web of connections.

Advantages of Selecting Mesh Topology for the EEE Department's Network:

- **Availability and Redundancy:**

  Mesh topology provides a high level of redundancy. There are alternate channels for data transfer if one link fails. This ensures that the network is always available and reliable. This redundancy is a key advantage in a vital environment like an educational institution, where uninterrupted connectivity is critical.

- **Scalability:**

  Mesh topology can readily support an increasing number of devices. The network's functionality will not be jeopardized as the department grows. This is especially important in an academic atmosphere where the number of devices and users can grow over time.

- **High performance:**

  Because devices have dedicated connections to one another, data traffic on shared channels is not overloaded. This results in efficient data transport and low latency. High network performance is advantageous in an educational setting where huge files may be shared and real-time communication is required.

- **Privacy and security:**

  The dedicated connections of each device provide a level of isolation from the rest of the network. This can improve security by reducing the effect of security breaches or malware spread.

❑ **Customised Layout:**

In a partial-mesh setup, you can strategically pick which devices require direct connections, optimising the network layout to meet the specific needs of the department.

While mesh topology has numerous advantages, it also has some disadvantages, such as higher costs due to the increased number of necessary connections and added complexity in controlling and maintaining the network.

In summary, because of its redundancy, scalability, high performance, security, and adaptability, the mesh topology fits the needs of the EEE department. It's a good choice for situations when connectivity, collaboration, and dependability are essential.

Logical Layout of the infrastructure consisting placement of routers, switches, access points via Mesh Topology

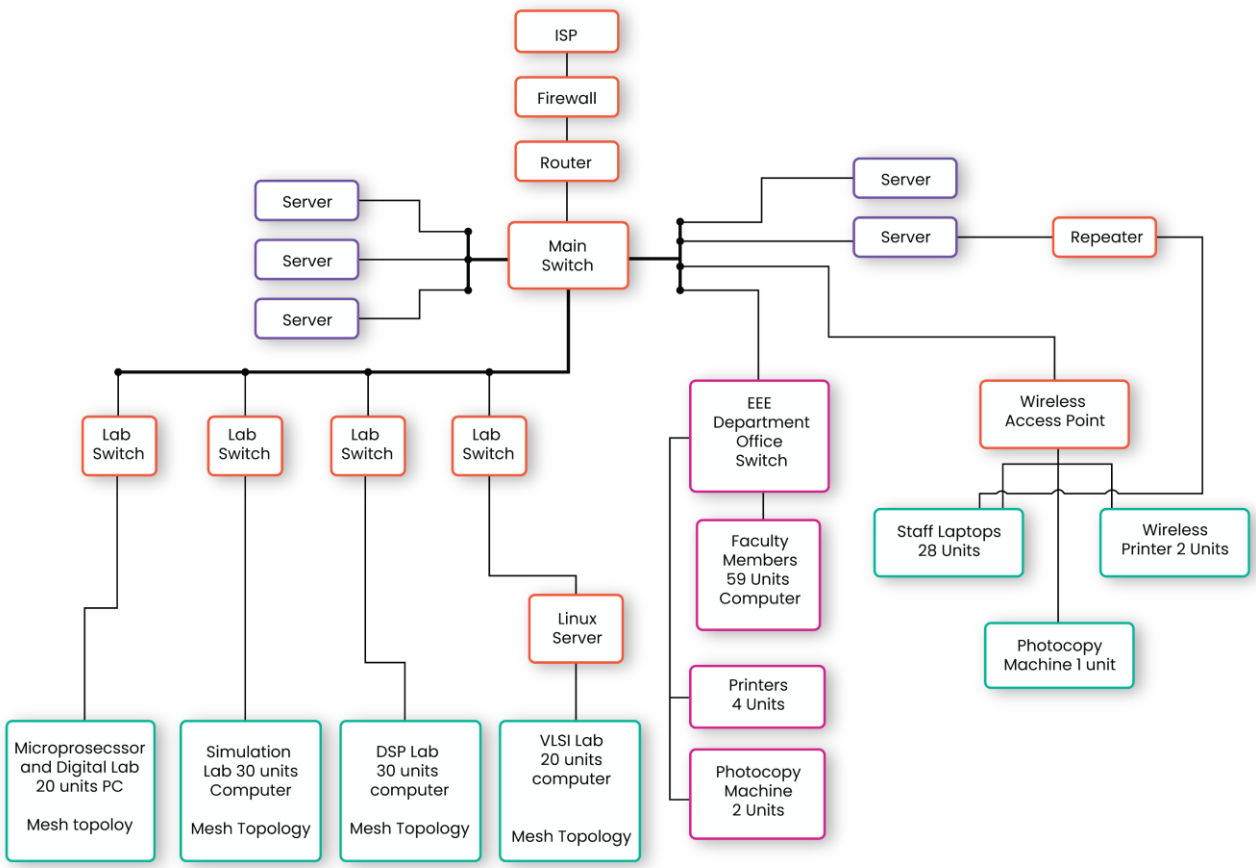
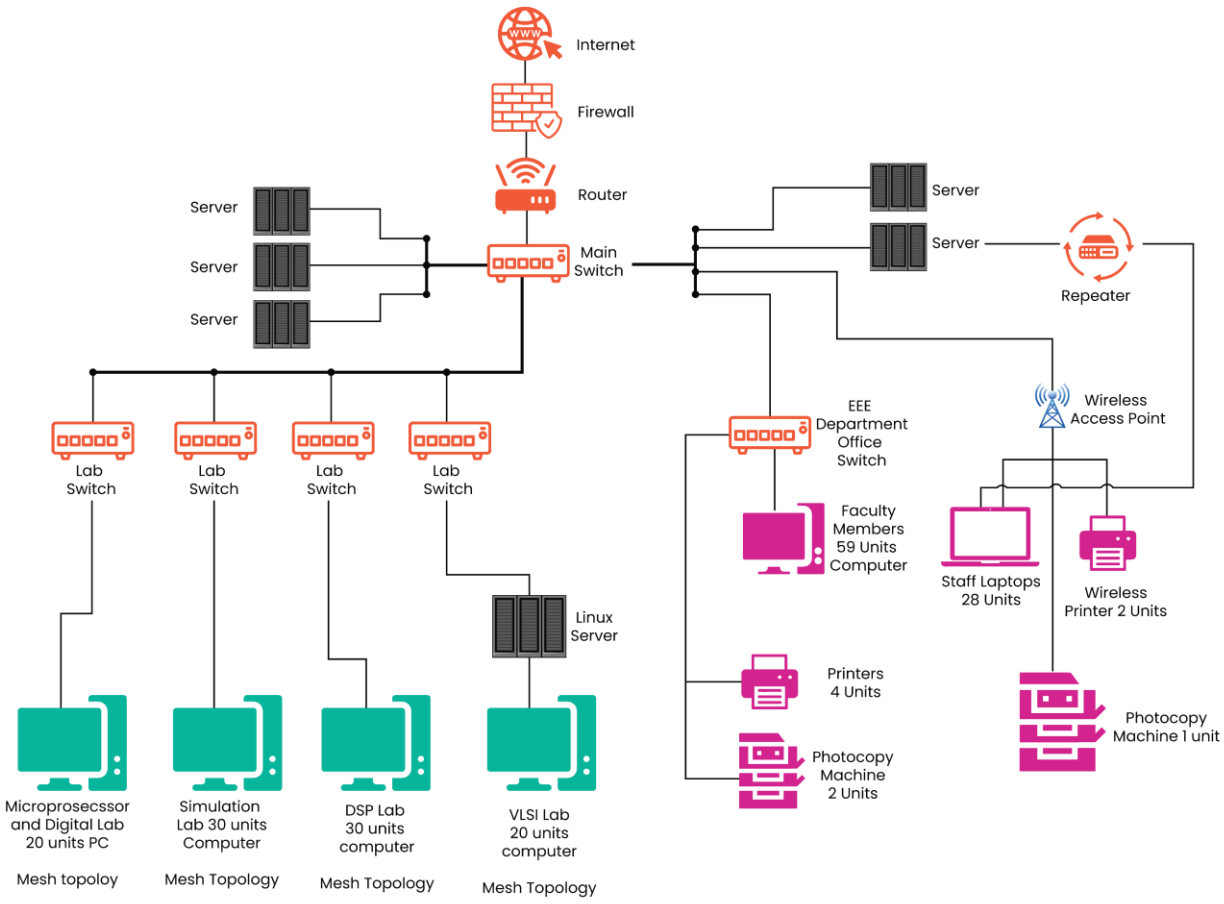


Fig: Network Infrastructure for EEE department of AUST using block diagram


Internet
Firewall
Router
Server
Server
Server
Main Switch
Server
Server
Repeater
Lab Switch
Lab Switch
Lab Switch
Lab Switch
EEE Department Office Switch
Wireless Access Point
Faculty Members 59 Units Computer
Staff Laptops 28 Units
Wireless Printer 2 Units
Linux Server
Printers 4 Units
Photocopy Machine 2 Units
Photocopy Machine 1 unit
Microprosecssor and Digital Lab 20 units PC
Simulation Lab 30 units Computer
DSP Lab 30 units computer
VLSI Lab 20 units computer
Mesh topoloy
Mesh Topology
Mesh Topology
Mesh Topology

Solutions of Question NO: 3

▪ Selection of Networking, Equipment and Estimated Cost:

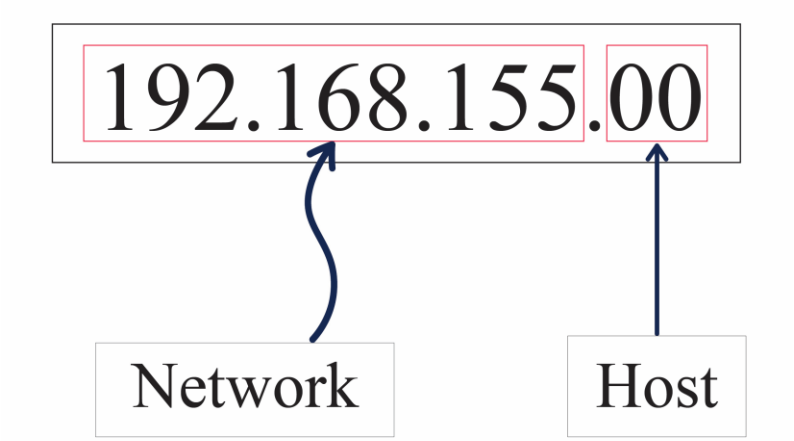
Device	Zone Wise	Specification	Unit Price	Quantity Required	Comment
1. Router	Entrire University Area	1. Throughtput and Capacity 2. Scalability 3. Secutiry Features 4. Traffic Routing and VLAN Support	9000/- BDT	9	Providing Routing Services, such as routing traffic between networks and providing security
2. Switches	• DSP Lab 1 (32 Port) • Simulation Lab 1 (32 Port	8/16/24/32/48 Port etc.	14,900/- BDT	60	Provide Switching services, such as forwarding traffic betwee devices and providing security
3. Network Monitoring Tools	Monitor and manage netwrok performance and security				Include Auvik SolarWinds Network Perf. monitor and PRTG Network Monitor
4. Access Point	Cisco Catalyst 9115AX or 9117AX series, Cisco Catalyst 9120AX series, and Cisco Catalyst 9130AX Series	Provide authentication services, such as authenticating users and providing security			Wireless network Connectivity to Devices
5. Network Cable		Used to protect the network from unauthorized			Some Common network Cable types include Ethernet cables, twisted pair cabling, and fiber optic cabling
6. Instrusion detection system (IDSs)					used to detect unauthorized access to the network
7. Antivirus Software AVAST	In Computer System		6,50,000/- BDT	10	Protect the network from malware
8. Firewalls		Protect the network from unauthorized access and cyber threats			The Cisco ASA 5500-X Series, Cisco Firepower Firewall and Fortinet, FortiGate Next Generation Firewall

Device	Zone Wise	Specification	Unit Price	Quantity Required	Comment
9. PC	Lab, Office	Ram: 8GB, SSD: 512 GB GFX Card: 4GB Processor: Corei 9 Windows: 11	95000/- BDT	200	Use for Study Purpose

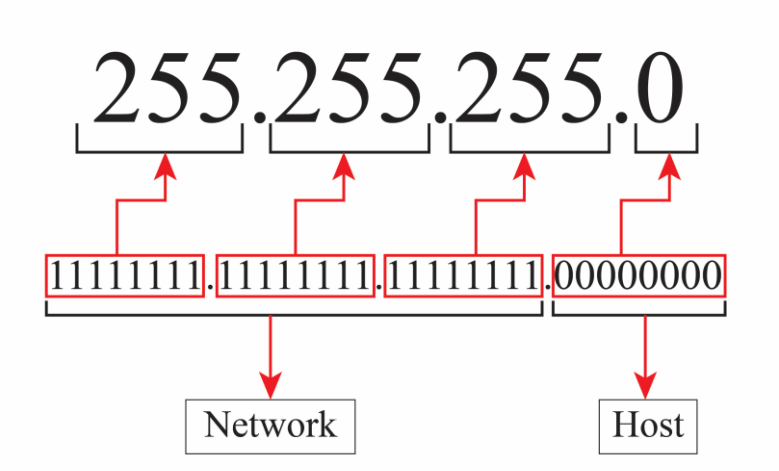
Solutions of Question NO: 4

▪ IP Addressing and Subnetting:

IP Addressing: Every device linked to a computer network that makes use of the Internet Protocol is given an IP (Internet Protocol) address, which is a numeric label. It accomplishes two major tasks: locating the host within the network and identifying the host or network interface. For example ,we can consider a IP address of



Subnet Mask: Each host for a network ,network part of the address will be same but the host part must be different. To identify the which portion of 32 bit numbers is network and which is host ,the idea of subnet mask arrived. For example,
32bit number



Conisdering a base IP address **192.168.155.0** with the subnet mask /24.
The binary form of IP address-

11000000.10101000.10011011 .00000000

Subnet mask - **11111111.11111111.11111111.00000000**

1. IP Addressing Scheme for the Network of the EEE Department-

Consider our Base Ip address is **192.168.155.0**

Subnet Mask /24

So IP address available is 256.

The available addresses are :

192.168.155.0
192.168.155.1
192.168.155.2
192.168.155.3
192.168.155.4
192.168.155.5
192.168.155.6
192.168.155.7
192.168.155.8
192.168.155.9
192.168.155.10
…….
…….
…….
…….
…….
…….
…….
…….
…….
…….

192.168.155.256

2. IP Address Allocation and Subnetting:
(Considering the design for Faculty members of 50,Staff members of 20 and students of 100)

- **Network arrangement for faculty members:**

Subnet Address: **192.168.155.0/26**
11111111.11111111.11111111.11000000
The available network is 2^2=4
Host available 2^6 = 64

Available IP addresses: 192.168.155.1 --- 192.168.155.62
Broadcast Address: 192.168.155.63
Usable IP Addresses: 2^6-2 = 62

- **Network arrangement for Staff members:**

Subnet Address: **192.168.155.64 /27**
11111111.11111111.11111111.11100000

Here network available 2^3=8 and host available 2^5=32

Available IP addresses: 192.168.155.65 --192.168.155.94
Broadcast Address: 192.168.155.95
Usable IP Addresses: 30

- **Network arrangement for Students:**

Subnet Address: **192.168.155.96 /25**
11111111.11111111.11111111.10000000

Here network available 2^3=8 and host available 2^7=128

Available IP addresses: 192.168.155.97--192.168.155.254
Broadcast Address: 192.168.155.255
Actual usable addresses - Between the subnet and broadcast addresses, which are 192.168.155.97 to 192.168.155.254=157

❑ IP Addressing Scheme:

Prefix length	Subnet mask	Subnet In binary	Available network	Usable Host
/25	255.255.255.128	11111111.11111111.11111111.10000000 NNNNNNNN. NNNNNNNN. NNNNNNNN. NHHHHHHHH	2^3=8	157
/26	255.255.255.192	11111111.11111111.11111111.11000000 NNNNNNNN. NNNNNNNN. NNNNNNNN. NNHHHHHHH	2^2=4	2^6-2=62
/27	255.255.255.224	11111111.11111111.11111111.11100000 NNNNNNNN. NNNNNNNN. NNNNNNNN. NNNHHHHHH	2^3=8	2^5-2=32

Figure: Breaking the network into smaller subnet

Solutions of Question NO: 5

▪ Network Device Configuration

1. PC Configuration:

❑ **Static IP Configuration:**

- Change adapter settings by going to Control Panel > Network and Sharing Centre.
- Right-click on the Ethernet/Wi-Fi connection and select Properties.
- Click Properties after selecting "Internet Protocol Version 4 (TCP/IPv4)".
- Selecting "Use the following IP address" and inputting the appropriate IP, subnet mask, gateway, and DNS server will work.

Example:
IP Address: 192.168.155.0
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.155.1
Preferred DNS Server: 8.8.8.8

2. Configuring a Wireless Access Point :

❑ **Setting up a Ubiquiti UniFi access point:**

- Go to the UniFi Controller.
- Select Networks under Settings.
- Establish separate networks for students (VLAN 20) and faculty (VLAN 10).

Go to Wireless Networks to configure your wireless network.

- Make new SSIDs for the networks for the faculty and students.
- Assign the SSIDs their appropriate VLANs.
- These configurations are basic examples that could need to be altered depending on the capabilities of the hardware and the particular needs. For some devices, graphical user interfaces (GUI) may also be used to perform some setups.

3.Configuration of a router:

- **Configuration of the interface:**

    - Open a web browser or specialised software to access the router's management interface.
    - Locate the section for LAN/WAN configuration.
    - Give the LAN interface a gateway, subnet mask, and IP address.

4. Configuring DHCP:

- Switch on the router's DHCP server.
- Establish a range of IP addresses that will be given to LAN-connected devices.
- Set the default router's IP address as well as the DNS server (for example, Google DNS: 8.8.8.8).

5. Configuration of the switch:

- Configuring a VLAN
- Use a web browser to access the switch's management interface.
- Create the relevant VLANs (such as Faculty and Students) by searching for VLAN settings.
- Give each VLAN a name and a VLAN ID.

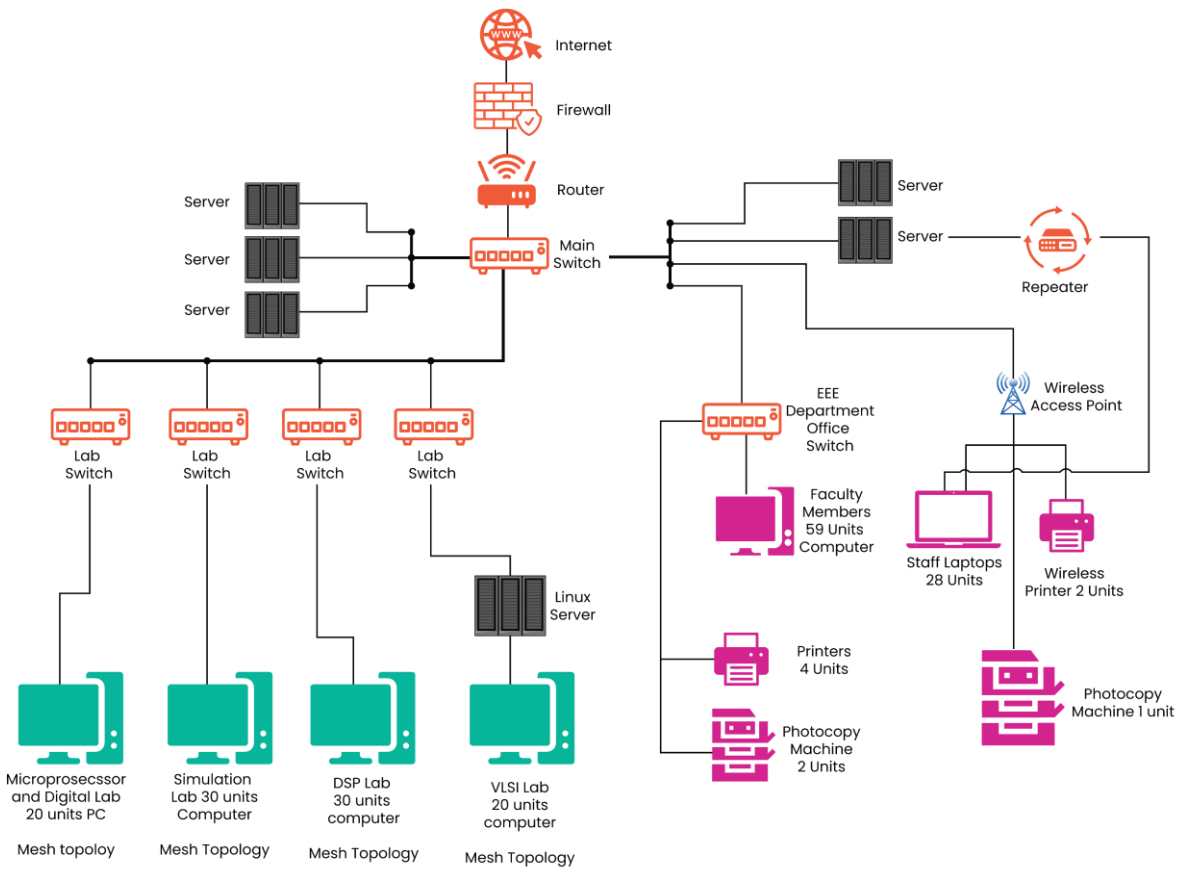
6. Configuring a port:

- Go to port configuration options by navigating.
- Based on how each port is used, assign VLANs to individual ports.
- As for example, VLAN 20 (Students) to ports where student devices are connected and VLAN 10 (Faculty) to ports where faculty devices are attached.

Solutions of Question NO: 6

▪ Documentation

❑ Networking Diagram with Mesh Topoloy:



❑ Establishing VLAN:

- **VLAN 10 (Faculty):** This VLAN is reserved for faculty members to use for resource sharing and internal communication.
- **VLAN 20 (Students):** This VLAN gives students internet access and connectivity.
- **VLAN 30 (Guest):** This VLAN offers restricted access to outside users and visitors.

- **Setting up QoS:**
  Set distinct QoS constraints for various traffic types:
  - Video Conferencing: First priority is given to video conferencing, which is guaranteed 20% of all bandwidth.
  - VoIP calls : VoIP calls are given top priority, and 15% of all bandwidth is ensured.
  - File downloads: File downloads have a 10% bandwidth allowance and a low priority.

- **Security Measures:**
  Describe the security measures put in place:

  - **Firewall:** The gateway router is configured with a stateful firewall that only permits necessary ports for services.
  - **IDS (Intrusion Detection System):** Snort IDS is configured to watch network traffic for irregularities and notify administrators.
  - **Encryption:** Wireless access points utilise WPA2 encryption with a strong passcode to ensure secure connections.

- **Hardware for the network:**
  Give thorough descriptions of the essential network hardware:
  - **Router:** OSPF routing protocol, Cisco ISR 4321, 2 Gigabit Ethernet interfaces.
  - **Access Points:** Dual-band, 2000 square foot Ubiquiti UniFi AP-AC-Pro access points from Ubiquiti.

- **Essential network services and applications:**
  - **File Sharing:** Microsoft OneDrive is the main sharing platform for files and documents.
  - **Video Conferencing:** Zoom is used for virtual meetings and webinars.

- **Troubleshooting Guides:**
  - Not having Internet access
  - Inspect any linked gadgets
  - Check the connections to the modem and router.
  - Switch on the router and modem.

- **Training Resources:**
  URLs to training resources

  - Guide to Video Conferencing: [**Click Here**]
  - Top Tips for Network Security: [**Click Here**]

❑ IP Addressing Scheme:

Prefix length	Subnet mask	Subnet In binary	Available network	Usable Host
/25	255.255.255.128	11111111.11111111.11111111.10000000 NNNNNNNN. NNNNNNNN. NNNNNNNN. NHHHHHHHH	2^3=8	157
/26	255.255.255.192	11111111.11111111.11111111.11000000 NNNNNNNN. NNNNNNNN. NNNNNNNN. NNHHHHHHH	2^2=4	2^6-2=62
/27	255.255.255.224	11111111.11111111.11111111.11100000 NNNNNNNN. NNNNNNNN. NNNNNNNN. NNNHHHHHH	2^3=8	2^5-2=32

Figure: Breaking the network into smaller subnet