Project Title: Designing a Multimedia-Enabled Computer Network for the EEE Department at Ahsanullah University of Science and Technology

Project Objective: The primary objective of this project is to architect a robust and efficient computer network for the Electrical and Electronic Engineering (EEE) Department at Ahsanullah University of Science and Technology. The network's aim is to facilitate seamless communication, resource sharing, and internet connectivity for both students and faculty members. The design should be based on careful considerations of the department's requirements and objectives, ensuring that it can handle multimedia data and applications effectively.

Project Phases:

1. Network Planning and Requirements Gathering:

Estimate the Network Requirements:

To design an effective network, we need to understand the requirements of the EEE Department. This involves estimating the following:

- **Number of Users:** Determine the current and anticipated number of students, faculty, and staff who will use the network.
- **Number of Devices:** Calculate the number of devices each user might have, including laptops and desktop computers.
- **Network Traffic**: Identify the different kinds and amounts of network traffic, such as multimedia data, online collaboration, research, and other prospective data-intensive jobs.

Goals and Objectives:

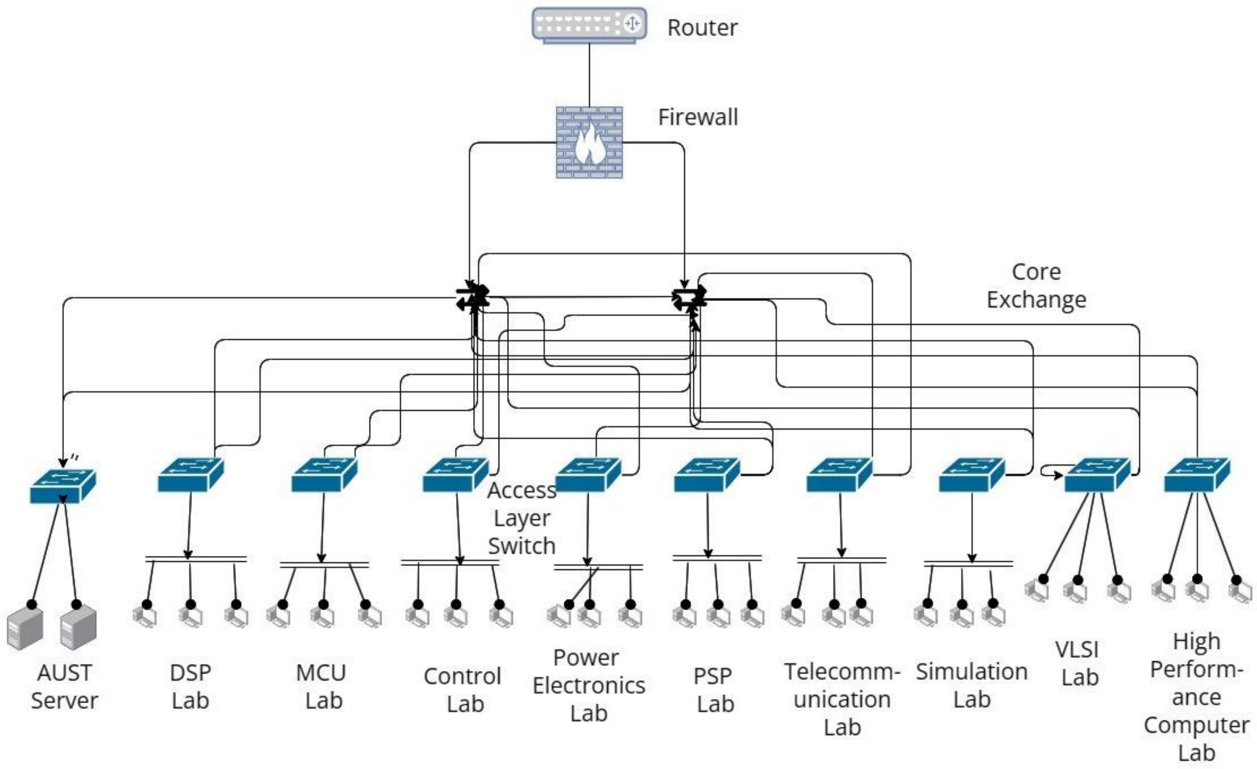
- **Seamless Communication:** Facilitate easy and timely communication between students, instructors, and staff for the benefit of education and teamwork.
- **Resource Sharing:** Ensure that users inside the department may easily share files, papers, and other resources.
- **Multimedia Capabilities:** Design the network to handle multimedia applications, such as video conferencing, online lectures, and multimedia project collaborations.
- **Reliability:** Ensure high network availability and minimal downtime to avoid disruptions to academic activities.
- **Scalability:** Design the network infrastructure to accommodate future growth in terms of users and devices.
- **Security:** Implement robust security measures to protect sensitive data and maintain the integrity of the network.

Table 1: Network Planning and Requirements Gathering

Zone	Total PC	Software Required	Network Service Required	Comment
DSP	30	Matlab,Octave,Codeblocks	Submission	1 PC needs internet
VLSI 1 Lab	20	Quartus 2,Quartus Prime,Cadence,Modelsim	Linux roaming server and submission	All the PC need internet
MCU and Digital Lab	27	Quartus 2,Arduino	Submission	All PCs are interconnected
High Performance Computer Lab	27	Autocad,Pspice,Matlab,Codeblocks	Submission	Internet needed in only 1 PC
Simulation Lab	31	Matlab,Pspice,codeblocks,Autocad	None	1 PC needs internet
Telecommunication Lab	03	None	None	2 PCs need internet
Switch,Gear Protection Lab	02	Power World Simulator	None	2 PCs need internet
Power Electronics Lab	03	None	None	2 PCs need internet
Electronics-02 Lab	01	None	None	None

2. Network Design and Topology:

Network Design For EEE Department:



Topology:

For this assignment, we consider nine lab such as DSP Lab, MCU Lab, Control Lab, Power Electronics Lab, PSP Lab, Telecommunication Lab, Simulation Lab, VLSI Lab and High-performance Computer Lab. For our network, we selected two topologies: Bus topology and Star Topology. They are briefly introduced and discussed below:

Bus Topology:

The term "bus topology" refers to a network design where every device is linked to a single, central wire, or "bus." Signals are sent down this shared communication line to transmit data. Although this design is straightforward and economical, it has drawbacks include the possibility of data collisions and difficulties in troubleshooting when the main connection breaks. Bus topology was frequently employed in early Ethernet networks, where nodes tapped into the main connection to access and share data, despite its disadvantages.

Without VLSI and High-Performance Lab, the rest of labs network we consider Bus topology because it is cost-effective, Cable required is least compared to other network topology and used in small networks.

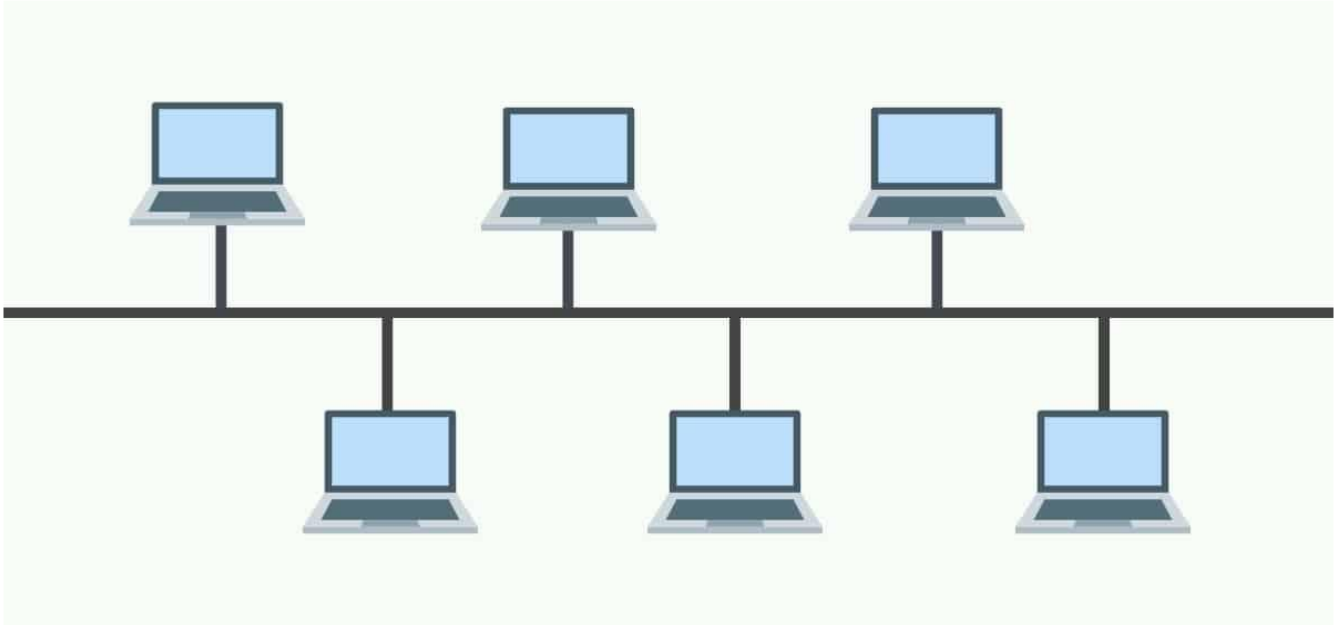


Fig: Bus Topology Network

Star Topology:

Star topology involves connecting all devices to a single hub or switch. Each device has a unique dedicated link to the hub, allowing for effective and autonomous communication. Given that only a portion of the network is affected when a device or cable fails, this architecture improves dependability. The system is susceptible, though, because it depends on the main hub; if the hub breaks down, the entire network may be damaged. Despite this disadvantage, star topology is frequently employed in contemporary networks because of it's simplicity in setup, scalability, and troubleshooting.

Even though there are topologies that are more efficient and faster than Bus topology,we avoided them and used Bus topology because we have to keep cost in our minds as well. As our network is not meant for professional usage, a little slower speed is acceptable if it saves a significant amount of money and resources.

We consider VLSI and High-Performance Lab under star topology because fast performance with few nodes and low network traffic, only that node is affected which has failed, rest of the nodes can work smoothly and easy to troubleshoot.

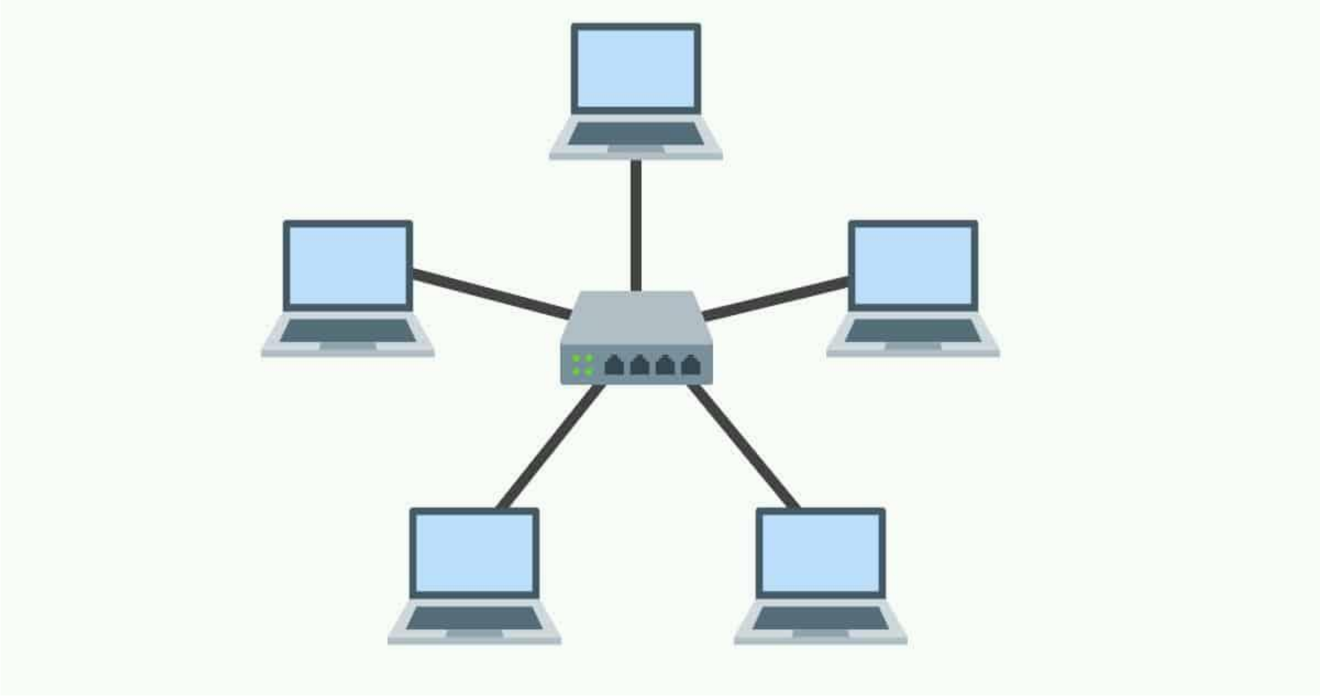


Fig: Star Topology Network

3. Selection of Networking Equipment and estimated cost:

Device	Zone wise	Specification	Unit Price	Quantiy Requird	Comment
1.Router	University Area	1.Mu-MIMO & Beamforming 2.Coverage Area 3.Throughput & Performance	6,000tk	18pcs	For providing internet connection Wi-fi through Router in entire University

2.Switches and Adapter	**#Dsp Lab 1 (32 port)** **#Simulation Lab 1(32 port)**	**8/16/24/32/48 port etc.**	**1,200tk**	**45pcs**	**Switches keep running of the lab.Also provide better work experience. Without switch no lab can running**
3.Network Monitoring Tool	**Every individual Lab**	**1.Bandwidth monitoring** **2.Real time monitoring** **3.Historical data analysis** **4.Network protocol support**	**-**	**-**	**A Network Monitoring Tool is a must-have for maintaining network health, improving performance, and assuring security.**
4.Access point **And Range Extender**	**Every individual Lab**	**1.Wireless Protocols** **2.Dual Band or Try Band** **3.Wireless data transfer rate.** **4.Security Options**	**19500tk**	**15pcs**	**It enables internet transmissions to be extended into rooms that would otherwise receive weak or no signals due to walls, general spacing, or furniture impediments.**
5.Network Cable	**Entire University**	**1.Cable type (cat5e,cat6,optic cables)** **2.Cable length**	**Copper cat-6Utp350MSoild networ**		**Modern connectivity relies on network wires. They transfer data and power crucial connections across businesses,**

		3.Twisted pair **4.Sheilding**	**k cable.**		**homes, and data centers using technologies ranging from Ethernet to fiber optics.**
6. Patch Panel	**Every individual Lab**	**Meet & Exceeds all Cat6 Standards.** **Metal With Aluminum**	**Dintek 1406-00011PC6 Cat6 24-Port Modular Patch Panel** **Accept 22~26AWG** **9,000 Tk**	**12,24,48-Port Patch Panel**	**Centralized Connectivity, Easy Troubleshooting, Reduced Downtime, Long-Term Reliability** **& Cable Management.**
7.Patch Cord	**Every individual Lab**	**Cable Length: 1 Meter** **Max Load: Short Term** **Core: 9 ± 2.5µm** **Single-mode, LSZH** **120N**	**350 tk**	**Ethernet patch cables (Cat5e, Cat6, Cat6a, Cat7)**	**Physical Connectivity,** **Data Transmission,** **Maintenance and Troubleshooting**

4. IP Addressing and Subnetting:

Lab Name	Number of Students Computer	Number of faculty Computer	Number of Staff Computer
DSP lab	28	1	1
VLSI lab	19	1	1
MCU lab	26	1	0
Control lab	5	1	0
Power electronics lab	0	3	0
PSP lab	0	2	0
TCL lab	0	3	0
Simulation lab	30	1	0
High-Performance Computer Lab.	26	1	1

For the IP addressing scheme, we will use the base IPv4 address 192.168.0.0 with a subnet mask of 255.255.240.0 (/20). This allows for a total of 4096 IP addresses per subnet.

We consider future expansion

Subnet	For	Address	Mask	Assignable Range
DSP Lab	Students	192.168.100.0	/24	192.168.100.1 - 192.168.100.30
	Faculty			192.168.100.31
	Staff			192.168.100.32
VLSI Lab	Students	192.168.101.0	/24	192.168.101.1 - 192.168.101.30
	Faculty			192.168.101.31
	Staff			192.168.101.32
MCU Lab	Students	192.168.102.0	/24	192.168.102.1 - 192.168.102.30
	Faculty			192.168.102.31
	Staff			192.168.102.32
Control Lab	Students	192.168.103.0	/27	192.168.103.1 - 192.168.103.15
	Faculty			192.168.103.16
	Staff			192.168.103.17
Power Electronics Lab	Students	192.168.103.32	/29	
	Faculty			192.168.103.33 - 192.168.103.38
PSP Lab	Students	192.168.103.40	/29	
	Faculty			192.168.103.41 - 192.168.103.43
Telecommunication Lab	Students	192.168.103.48	/29	
	Faculty			192.168.103.49 - 192.168.103.54
Simulation Lab	Students	192.168.104.0	/24	192.168.104.1 - 192.168.104.30
	Faculty			192.168.104.32
High-Performance Computer Lab	Students	192.168.105.0	/24	192.168.105.1 - 192.168.105.30
	Faculty			192.168.105.31
	Staff			192.168.105.32

5. Network Device Configuration:

Client PC

1. Assign an IP address to the PC.
2. Configure the default gateway and DNS server addresses.
3. Install the necessary network drivers.
4. Enable the network adapter.

Router

1. Assign an IP address to the router.
2. Configure the subnet mask and default gateway.
3. Configure the DHCP server (if applicable).
4. Configure the routing table.
5. Configure the firewall.

Switch

1. Assign an IP address to the switch.
2. Configure the VLANs (if applicable).
3. Configure the port security.

Wireless Access Point

1. Assign an IP address to the wireless access point.
2. Configure the SSID and security settings.
3. Configure the channel and power level.
4. Configure the DHCP server (if applicable).

Examples of configuration steps for each device:

Client PC

1. Assign an IP address to the PC. The IP address can be manually assigned or obtained through DHCP.
2. Configure the default gateway and DNS servers. The default gateway is the IP address of the router that the PC will use to connect to the rest of the network. The DNS servers are responsible for translating domain names into IP addresses.
3. Install the appropriate network drivers. The network drivers are software that allow the PC to communicate with the network.
4. Install any security software that is required. This may include antivirus software, firewall software, or intrusion detection software.

Router

1. Assign an IP address to the router.
2. Configure the subnet mask. The subnet mask is used to identify the network segment that the router is connected to.
3. Configure the default gateway. The default gateway is the IP address of the router that the other devices on the network will use to connect to the rest of the internet.
4. Configure the DNS servers.
5. Configure the DHCP server (if applicable). The DHCP server is responsible for automatically assigning IP addresses to devices on the network.
6. Configure the routing table. The routing table is used to determine the best path for packets to travel from one network segment to another.
7. Configure the firewall. The firewall is used to control the traffic that is allowed to pass through the router.

Switch

1. Assign an IP address to the switch.
2. Configure the VLANs (if applicable). VLANs are used to divide the network into smaller segments.

3. Configure the port security. Port security is used to prevent unauthorized devices from connecting to the switch.
4. Configure the spanning tree protocol. The spanning tree protocol is used to prevent loops in the network.

Wireless Access Point

1. Assign an IP address to the wireless access point.
2. Configure the SSID and security settings. The SSID is the name of the wireless network. The security settings are used to protect the wireless network from unauthorized access.
3. Configure the channel and bandwidth. The channel is the frequency that the wireless access point will use to communicate with devices. The bandwidth is the amount of data that can be transferred over the wireless network.
4. Configure the power output. The power output is used to control the range of the wireless network.

Wireless Access Point

1. To assign an IP address to the wireless access point, we can access the wireless access point's configuration page using a web browser. The IP address of the wireless access point is usually printed on the bottom or back of the wireless access point.
2. To configure the SSID and security settings, we can specify the SSID and the security type (such as WPA2-Personal) for the wireless network.
3. To configure the channel and power level, we can specify the channel and the power level for the wireless network.
4. To configure the DHCP server, we can enable the DHCP server and specify the range of IP addresses that the DHCP server will assign to devices on the network.

6.Documentation :

In this assignment, we followed very specific steps to design a computer network. At first, at first we collected all the data of computers regarding user number and usage type of every lab like DSP ,VLSI-01 ,MCU and Digital Electronics,High Performance Computer, Simulation, Telecommunication ,and many other listed laboratories. We used star topology in VLSI and High Performance Computer Lab because in these laboratories speed matters most and VLSI lab specifically requires server available for each computer individually .

We use bus topology in other laboratories because it is cheaper and easy to use and setup. In this case if we use other topology then it might be costly and became complex. We try to find a way which is cost effective and efficient. Then we calculate the amount of routers, switches and other equipment used and their buying cost.

Mapping out the network topology in a Diagram: First of all we created a topology diagram for easy understanding. This simple diagram shows the connections between the main network infrastructure components, including modems, routers, firewalls, switches, servers, and wireless access points. This diagram should enable an IT professional to easily understand the network and discover the key details, such as the component name, IP address, and MAC address. For a more complex network and professional use, incorporating static clients like cable PCs and printers/copiers would be a good idea. The most popular diagramming program is Microsoft Visio.

Evaluating network security: In order to better access, troubleshoot, upgrade, and secure the network, analyzed and compiled a security status summary for every part of the network like :Firewall, LAN, WLAN, and VPN server. By evaluation access of the network is established.Normally documentation is also used for backup and internet pathway detection. A gateway for guest users is also kept for future extension purposes.

Document client machines and devices: Every individual worker and client is treated as locks cameras and DVRs along with PCs and laptops.Information like Name,User ID,physical location and other information were collected for this task.

Label wiring outlets, runs, and ports: An identification scheme for Ethernet, fiber and other wiring was created for future troubleshooting and upgrade purposes.Every Ethernet wall-port and every other cable run to network components were physically labelled.

Creating a floor plan map: Even though a diagram is great for understanding but for visualization a floor plan would be very beneficial. A shortcoming of our network is that we were not able to create a floor plan for better visualization, but in future iteration of this assignment a floor plan may be developed.

Creating or updating policies and procedures: From our process of building the network and further documentation our policies and rules for the usage of the network is pretty clear.

This network is semi liberal considering many laboratories allow internet connection and file sharing whereas many other do not allow either, which is expected considering it is a network for an university department. And different laboratories require different kinds of teaching and evaluation process.