1 INTRODUCTION

The following proposal outlines the design and implementation of a robust backbone network infrastructure for the University of Moratuwa. The backbone network will connect different floors and buildings within the university premises, ensuring high-speed and reliable data transfer. The proposed solution incorporates fiber-optic cables for long-distance connectivity, network switches with high bandwidth capabilities, and advanced routing and switching protocols to optimize network performance.

1.1 The Internal network of one building (ENTC)

1.1.1 Features of the local area network of the department building of Department of Electronic and Telecommunication Engineering

* Electronic and Telecommunication Engineering Department A flat network is a LAN.
* Through ENTC node, a layer 3 switch, the LAN of the ENTC department building is connected to the University of Moratuwa's backbone network.
* ENTC node switch can support a maximum data rate of 10 Gigabits per second.
* The core switch of the ENTC LAN, which is once more a layer 3 switch, is connected to the ENTC node switch by a 10 Gigabits per second fiber connection.
* The following 8 24-Port Network Switches with a 2 layer topology have been linked to the ENTC core switch using 8 fiber cables at a speed of 1 Gigabit per second.

– Biomedical Engineering Laboratory.
– Computer Laboratory.
– Department Office.
– Digital Electronic Laboratory.
– Instructors' Room.
– Telecommunication Laboratory.
– Microwave Laboratory.
– Vision Laboratory.

* The ENTC Core switch has been connected to the following 24-Port network switches using copper UTP cables.

– Switch inside the Premium Biomedical Engineering laboratory.
– 2 switches inside the Network Room, Ground Floor.

* The building has 14 wireless access points that may be used to connect to the LAN. The following lists their locations as well as the switch to which each is linked.

1. From the 2 switches at the Network Room,

– ENTC1.
– 0.5 Student Area.
– UAV Laboratory.

2. from the switches at the Biomedical Engineering Laboratory,
   - Biomedical Laboratory.
3. From the switch at the Computer Laboratory,
   - Computer Laboratory
4. From the switch at the Department Office,
   - Near the HOD Office.
   - Near the lift of 1st floor.
5. From the switch at the Digital Electronic Laboratory,
   - Near the Digital Electronic Laboratory.
   - Inside the Analog Electronic Laboratory.
6. From the switch at the Department Office,
   - Near the Upper Common Student Area.
   - Near the Instructors' Room.
7. From the switch at the Telecommunication Laboratory,
   - Inside the Telecommunication Laboratory.
8. From the switch at the Vision Laboratory,
   - Near the Dialog Laboratory.
9. From the switch at the Microwave Laboratory,
   - Inside the Microwave Laboratory.

Their positions are depicted in the diagram below.

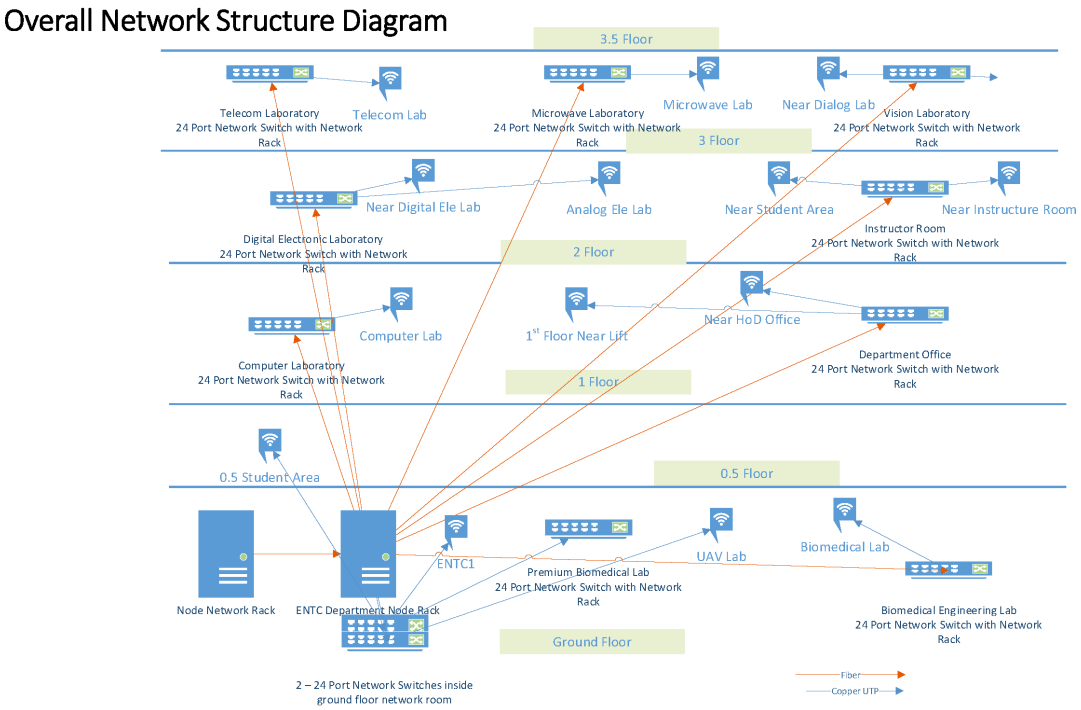

Figure 1 — Overall Network Structure Diagram of ENTC

2 THE APPROACH TO YOUR BACKBONE DESIGN WITH PROPER JUSTIFICATION. E.G. YOU NEED TO EXPLAIN WHY YOU HAVE CHOSEN A PARTICULAR TOPOLOGY.

2.1 University Backbone Network

2.1.1 Network Topology

The backbone network will be designed using a hierarchical model, comprising core, distribution, and access layers. This model ensures scalability, flexibility, and efficient data flow throughout the university premises.

2.1.2 Core Layer

At the core layer, high-performance network switches will be deployed to handle the interconnection between different buildings and floors. The switches should possess high bandwidth capabilities and support advanced routing protocols such as OSPF (Open Shortest Path First) or EIGRP (Enhanced Interior Gateway Routing Protocol) to enable fast and efficient data transfer.

2.1.3 Distribution Layer

The distribution layer will be responsible for connecting individual floors within each building. Network switches with sufficient port capacity and VLAN (Virtual Local Area Network) support will be installed at this layer to facilitate seamless communication between different departments and areas.

2.1.4 Access Layer

At the access layer, network switches will be deployed to connect end devices such as computers, printers, and other network-enabled equipment. These switches should support Power over Ethernet (PoE) to provide power to devices like IP phones and wireless access points.

2.1.5 Fiber-Optic Cabling

Fiber-optic cables will be used for long-distance connectivity between different buildings and floors. This technology offers high bandwidth, low latency, and resistance to electromagnetic interference, ensuring reliable and fast data transmission.

2.1.6 Redundancy and Failover

To enhance network reliability, redundant links will be implemented between core and distribution switches using link aggregation (e.g., LACP - Link Aggregation Control Protocol). Redundant power supplies and backup systems will also be considered to minimize downtime in case of power outages.

2.1.7 Routing and Switching Protocols

Routing protocols such as OSPF or EIGRP will be configured to enable efficient data routing and dynamic adaptation to network changes. Spanning Tree Protocol (STP) will be implemented to prevent network loops and ensure redundancy.

2.1.8 Security Measures

To protect the backbone network, access controls, and encryption mechanisms should be implemented. Firewalls and Intrusion Detection/Prevention Systems (IDS/IPS) can be deployed at the network perimeter to safeguard against unauthorized access and cyber threats.

2.1.9 Network Monitoring and Management

Network monitoring tools will be utilized to monitor network performance, detect anomalies, and ensure proactive maintenance. Network management protocols like SNMP (Simple Network Management Protocol) can be implemented for centralized control and configuration of network devices.

2.2 University of Moratuwa Core Network Architecture

* The backbone network of University of Moratuwa has a ring topology.
* Mainly there are 2 server locations namely,

1. Sumanadasa Building
2. Center for Information Technology Services (CITeS)

* There are 9 nodes to access the network. They are in the following locations.

1. Network Operating Center at CITeS
2. Faculty of Information Technology
3. Department of Electronic and Telecommunication Engineering
4. Sumanadasa Building
5. Department of Civil Engineering
6. Department of Transport Management and Logistics Engineering
7. Department of Material Science and Engineering
8. Department of Mechanical Engineering
9. Administration Building

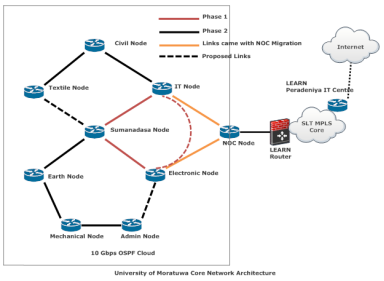

Figure 2 — University of Moratuwa Core Network Architecture

There are 25 access points have been installed based on the network traffic which can be extended up to 500 such points that can support 7000 clients.

These are the daily inward and outgoing traffic statistics for the University of Moratuwa network.

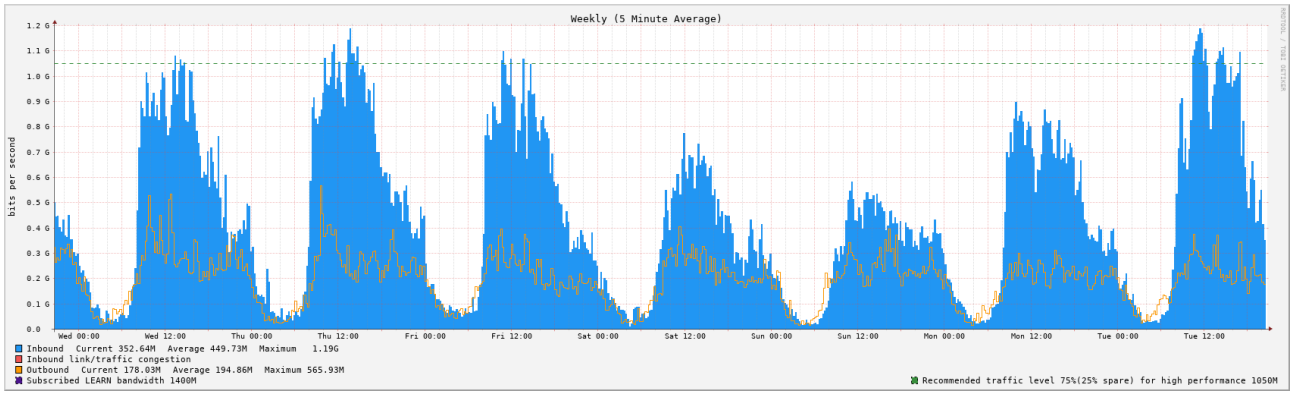

Figure 3 — Inbound connections are ones that are made to a particular device from a distant area.

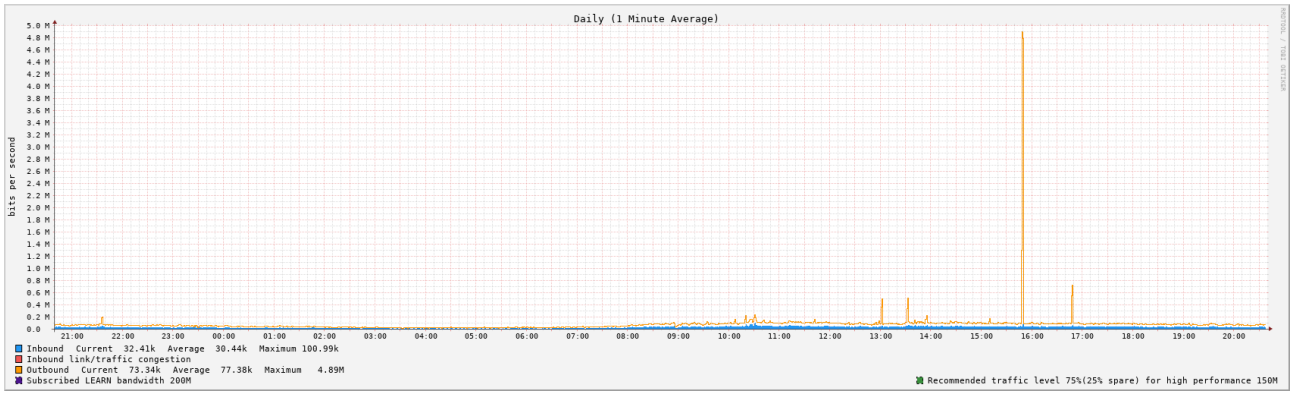

Figure 4 — Outbound refers to connections that are made from a device or host to a particular device.

2.3 Assumptions Made in Designing the Backbone Network

This backbone network design incorporates the specific requirements of heavy data transfer, cost-effectiveness, and efficient connectivity between the main site and branch offices. The utilization of leased lines for high-bandwidth connections, frame relay for low data transfer, and dedicated PVCs with CIR ensures reliable and guaranteed communication between the branch offices.

* Heavy Data Transfer between Main Site and Branch Offices:
  Considering the continuous heavy data transfer requirements between the main site and branch offices, the backbone network design prioritizes high-bandwidth connections for efficient data transmission.
  Leased line connections are chosen due to their dedicated and reliable nature, ensuring consistent high-speed connectivity between the main site and branch offices. Symmetrical

bandwidth offered by leased lines facilitates balanced data transfer in both directions, optimizing overall network performance.

* Cost-Effective Leased Line Connection for Branch Offices:
  Given the close proximity of the two branch offices to the main head office, a cost-effective approach is taken by establishing leased line connections between these sites. Leased lines provide dedicated point-to-point connections, ensuring secure and efficient data transfer without relying on public networks.
  Reduced distance between the main site and branch offices helps minimize costs associated with establishing leased line connections.
* Frame Relay for Low Data Transfer between Branch Offices:
  To accommodate low data transfer requirements between the two branch offices, a permanent virtual circuit (PVC) connection using frame relay is implemented.
  Frame relay offers a cost-effective solution for transmitting low to medium amounts of data over a wide area network (WAN). It efficiently utilizes bandwidth by multiplexing multiple logical connections over a single physical connection.
  By utilizing frame relay PVCs, the two branch offices establish a reliable and cost-efficient communication channel tailored to their specific needs.
* Dedicated PVC with CIR between Branch Offices:
  To ensure a consistent and guaranteed level of service, a dedicated PVC (Permanent Virtual Circuit) is established between the two branch offices.
  The PVC is provisioned with a Committed Information Rate (CIR) to specify the minimum bandwidth allocation for the connection. This ensures a certain amount of bandwidth is always available for communication between the two branch offices, regardless of network traffic conditions. By implementing a dedicated PVC with CIR, reliable and uninterrupted communication is ensured, promoting efficient collaboration and data sharing between the branch offices.
* Benefits of Leased Line for Main Site and Branch Sites:
  Leased lines are favored to connect the main site and branch offices due to their ability to meet the heavy data transfer requirements.
  With leased line connections, the main site and branch offices benefit from dedicated, high-speed, and reliable connectivity.
  Leased lines minimize latency and provide consistent network performance, which is crucial for data-intensive applications and real-time communication.
  Additionally, the simplicity of leased lines requiring only two interfaces on the gateway router to connect the main site and branches reduces the complexity of the network infrastructure and minimizes potential points of failure.

2.4 Considerations for the network design

The network design for the University of Moratuwa's backbone network includes the following components:

* Entrance Facility: Connects the ISP network to the customer's network using routers, switches, and demarcation points.
* Equipment Room: Houses networking equipment, such as switches, servers, firewalls, and other active devices. It provides a controlled environment with cooling, power supply, and physical security measures.
* Backbone Cabling: Uses high-speed fiber-optic cables to interconnect different floors, ensuring efficient and reliable data transmission throughout the building.
* Horizontal Cabling: Connects devices within the same floor using twisted-pair copper cables terminated with RJ45 connectors.
* Work Area: Consists of end-user workstations connected to the network infrastructure through wired or wireless connections.
* Telecommunication Enclosure: Acts as a central point of interconnection between the horizontal and backbone cabling subsystems. It houses patch panels, switches, and other equipment for network connections.

In this design, patch panels are used for easy identification and flexibility in changing network connections. Multiple switches are stacked in the switch chassis to simplify network management, provide scalability, and offer redundancy.
The backbone cabling subsystem uses fiber optics to connect the switch chassis on each floor to the core switches on the 2nd floor. Redundant links ensure uninterrupted connectivity.
The equipment room on the 2nd floor hosts core switches, core routers, a firewall, a gateway router, a server room, and a DMZ for web server hosting. Multiple core switches and routers provide redundancy, while the firewall filters incoming traffic and the gateway router connects to branch offices via leased lines for heavy data transfer.
The server room contains essential servers such as FTP, Mail, AD/RADIUS, DNS, and DHCP servers. Static IP addresses are assigned to the servers for stability and remote access. The servers connect to the central switch, which, in turn, connects to the two core switches. This network design ensures a structured and efficient infrastructure that offers scalability, redundancy, and ease of maintenance for the University of Moratuwa.

3 NETWORK DIAGRAM CLEARLY INDICATING ALL THE BUILDING NODES AND BANDWIDTH IN EACH LINK.

3.1 The backbone network for University of Moratuwa (UOM)

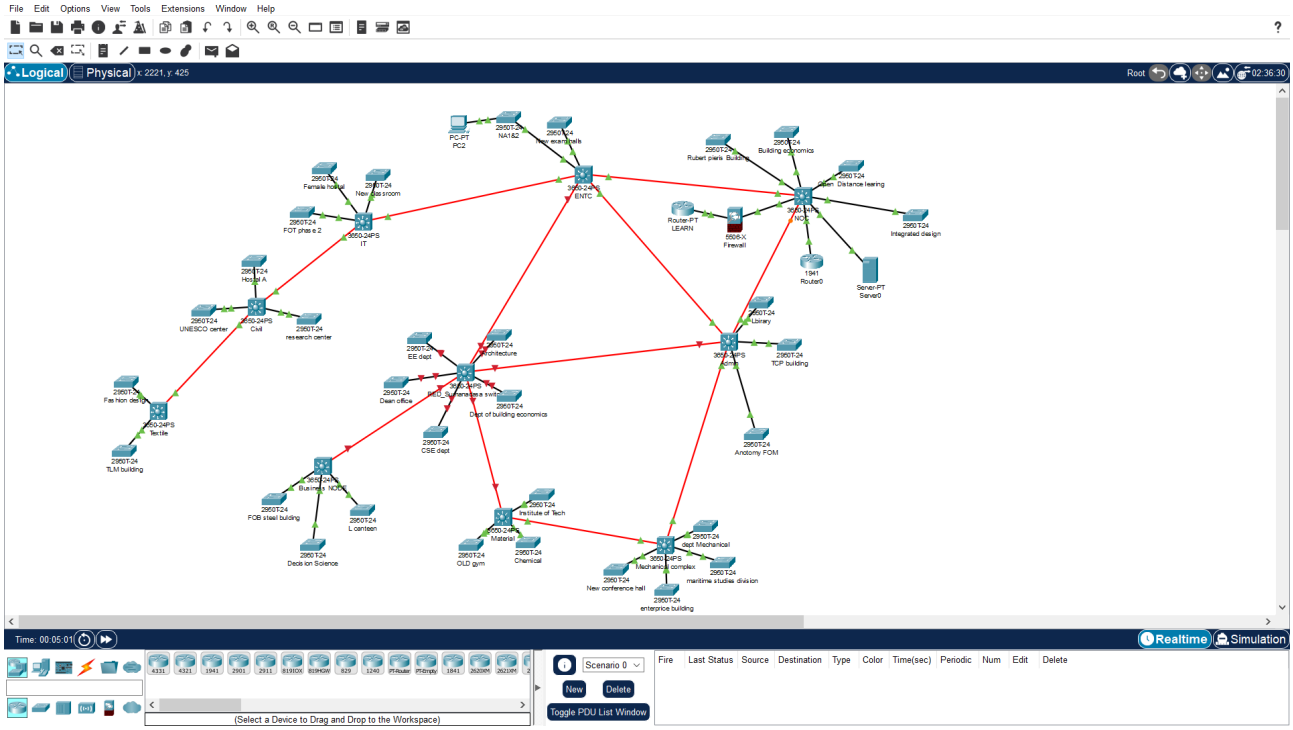

Figure 5 — The backbone network for University of Moratuwa (UOM)

3.2 The internal network of one building (ENTC)

3.2.1 Physical View

View From backbone

Figure 6 — Overall Network Structure Diagram of ENTC

Internal View of ENTC

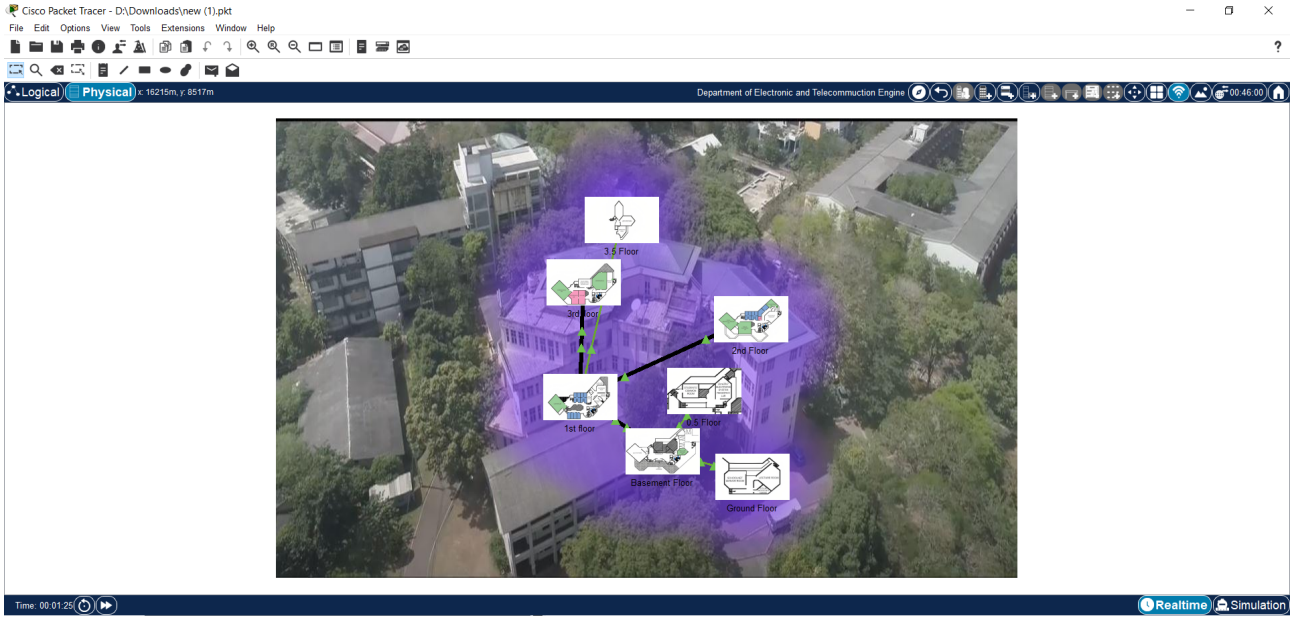

Figure 7 — Internal Network Structure Diagram of ENTC

View of Ground floor

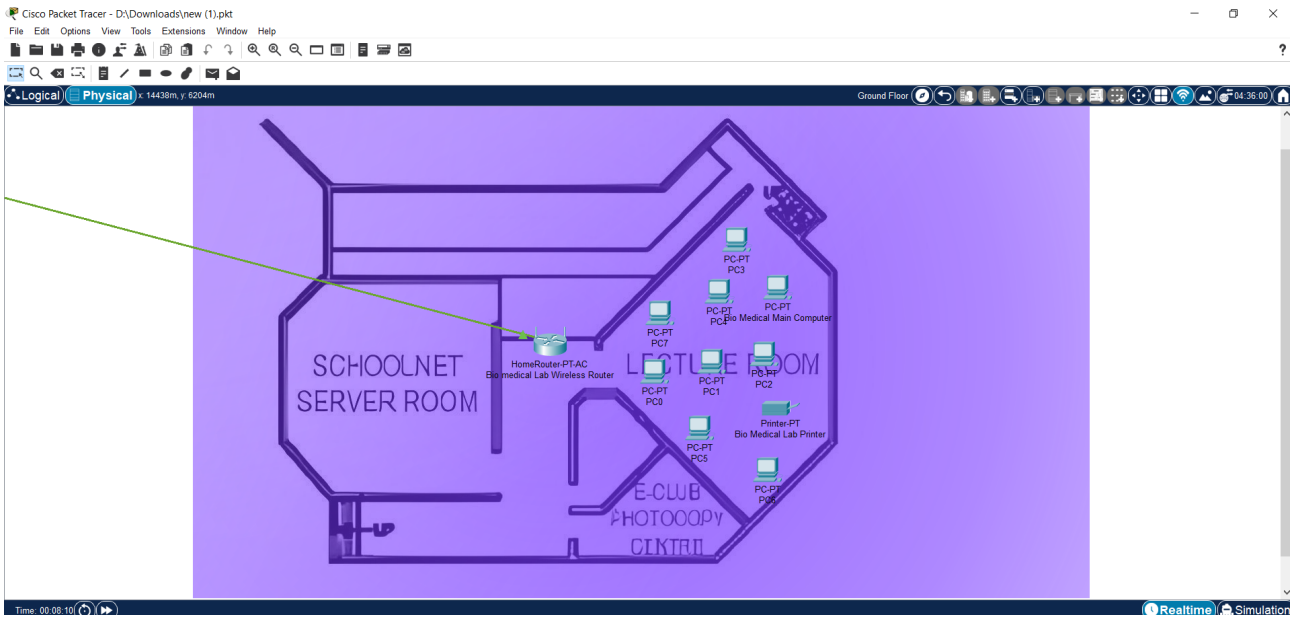

Figure 8 — View of Ground floor

View of Base

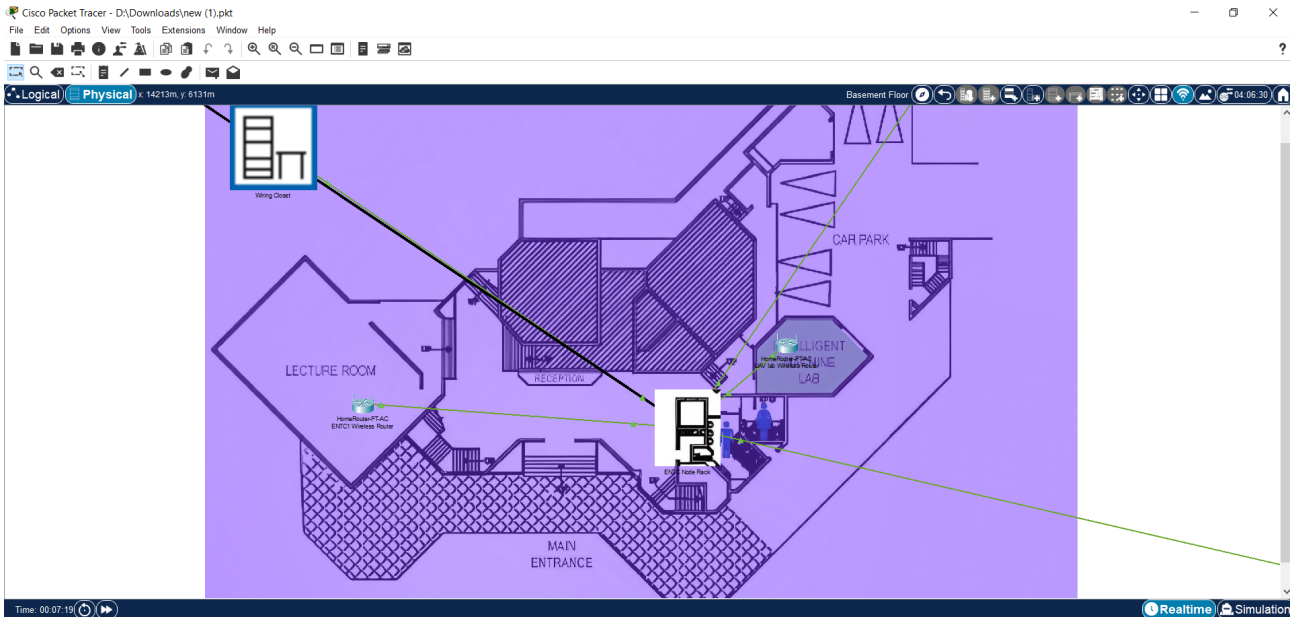

Figure 9 — View of Basement

View of 0.5 floor

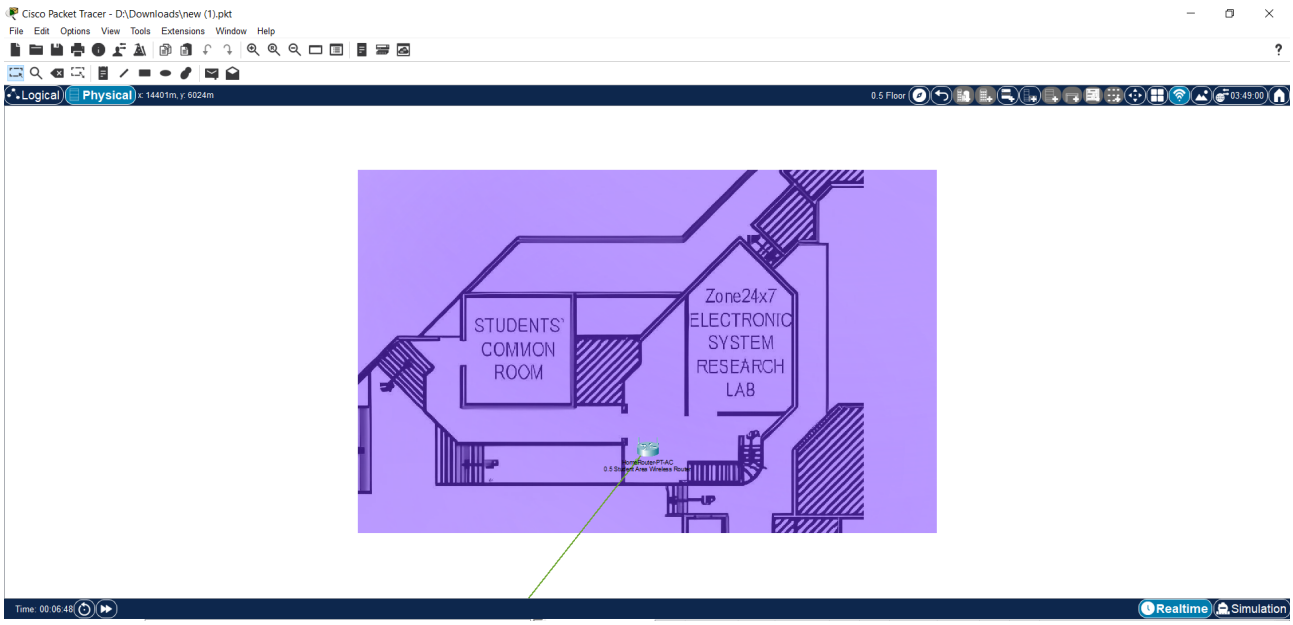

Figure 10 — View of 0.5 floor

View of first floor

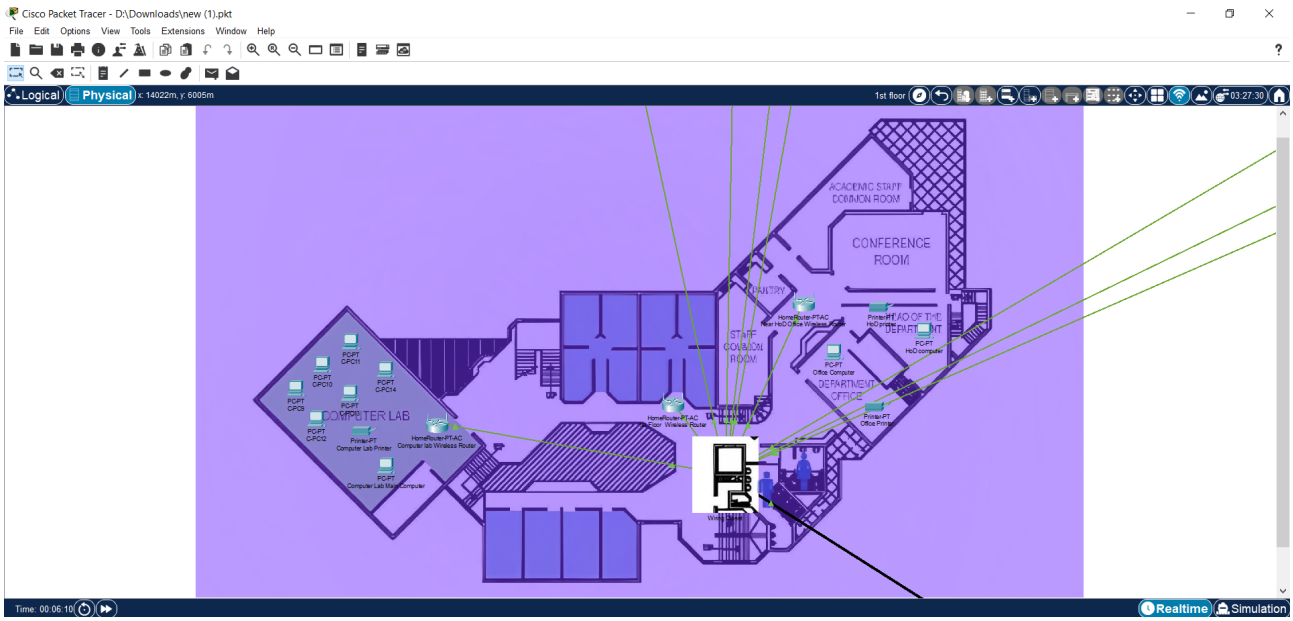

Figure 11 — View of first floor

View of second floor

Figure 12 — View of second floor

View of Third floor

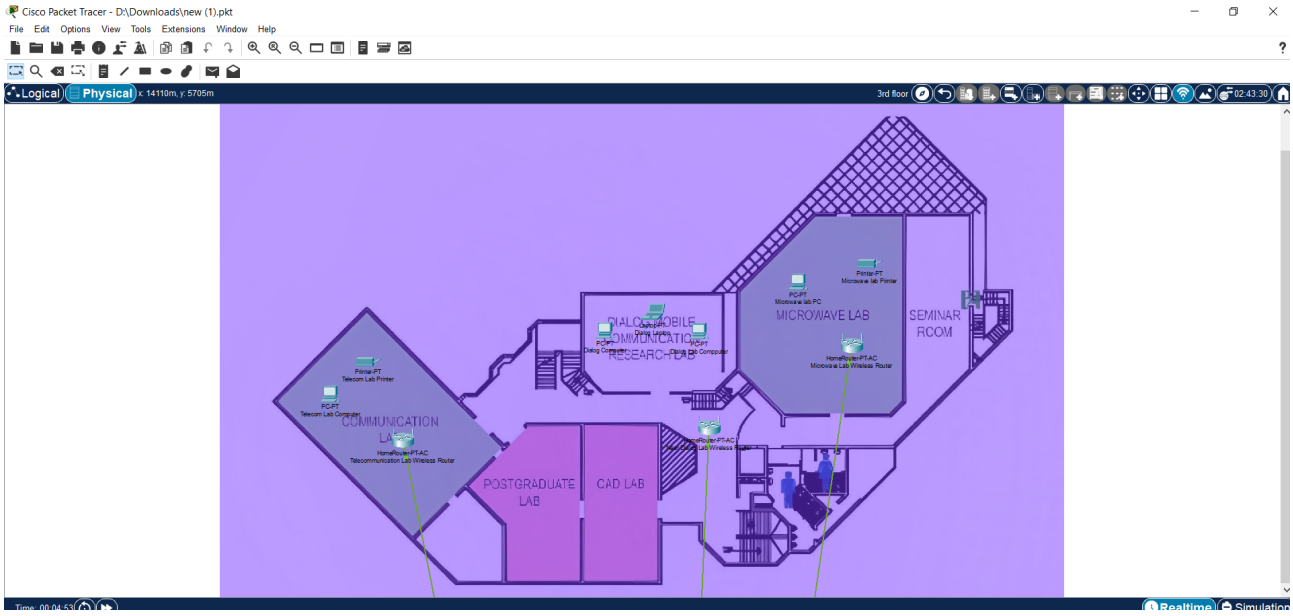

Figure 13 — View of Third floor

View of 3.5 floor

Figure 14 — View of 3.5 floor

3.2.2 Logical View

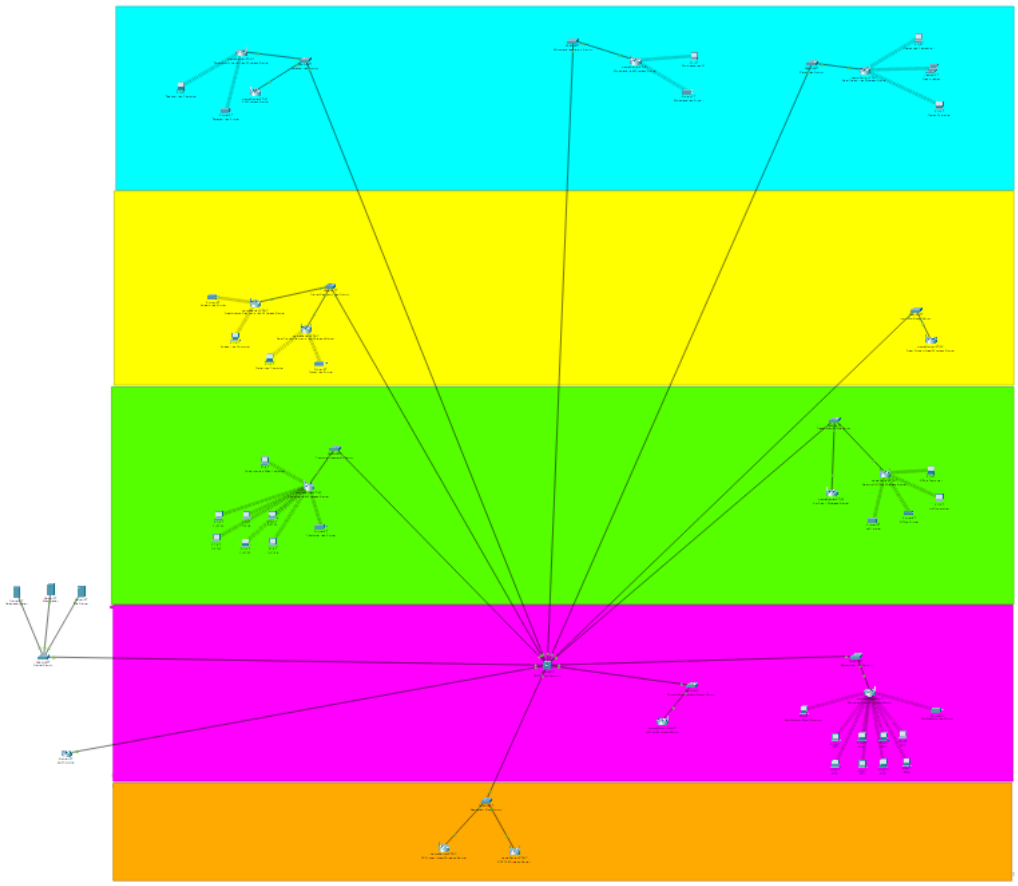

Figure 15 — Logical view of ENTC

4 IP ADDRESSING SCHEME FOR NETWORK (IPV4 AND IPV6)

4.1 IP address Allocation

Nodes	Number of IP address	Allocated bits	subnet mask	Ip adddress
NOC	1000	1024	255.255.252.0	10.10.2.1
ENTC	2000	2048	255.255.248.0	10.10.6.1
IT	2000	2048	255.255.248.0	10.10.10.1
Admin	4000	4096	255.255.240.0	10.10.18.1
Sumanadhasa	4000	4096	255.255.240.0	10.10.26.1
Mechanical	1500	2048	255.255.252.0	10.10.28.1
Material	1000	1024	255.255.252.0	10.10.30.1
Business	1000	1024	255.255.252.0	10.10.32.1
Textile	1000	1024	255.255.252.0	10.10.34.1
Civil	1000	1024	255.255.252.0	10.10.36.1

Table 1 — Ip address allocation

4.2 Network Protocols used in this Network Design

* Static Routing: Static routes are configured on gateway/core routers of each branch and the main site to route traffic between different networks. It provides a simple and secure way of routing without the need for routing advertisements or complex routing algorithms.
* Default Routing: Default routes are configured on core routers to route traffic from the internal network to the ISP router for destinations outside the network. It allows efficient routing for unknown traffic towards the internet.
* Inter-VLAN Routing: Core routers are configured to perform inter-VLAN routing, enabling communication between different VLANs within the network. This allows traffic to flow between VLANs using the core routers as the gateway.
* DNS (Domain Name System): The DNS server is configured in the server room on the 2nd floor. DNS resolves domain names to IP addresses, allowing hosts to access resources using easy-to-remember domain names instead of numerical IP addresses.
* DHCP (Dynamic Host Configuration Protocol): The DHCP server, located in the server room, dynamically assigns IP addresses to hosts in the network. It reduces network administration tasks by centrally managing IP address assignments and ensures reliable and efficient IP configuration for hosts.
* NAT (Network Address Translation): NAT is used to translate private IP addresses used within the network to public IP addresses for communication over the internet. It allows hosts with private IP addresses to access internet resources and protects the internal IP plan from external visibility.

* VLAN (Virtual Local Area Network): VLANs are created to logically separate hosts into different networks, reducing broadcast traffic and providing network security. VTP is used to manage VLANs and maintain consistency throughout the network.
* FTP (File Transfer Protocol): An FTP server is installed in the server room for file transfer within the network. It allows efficient and bulk transfer of files, supporting multiple files and directories transfers simultaneously.
* SMTP (Simple Mail Transfer Protocol): SMTP mail server is located in the server room and handles the sending and receiving of email messages. It ensures reliable delivery of emails, controls spam messages, and offers centralized management of mailbox capacity.

These network protocols are essential components of the network design, providing efficient communication, security, redundancy, and centralized management of network services.

5 JUSTIFICATION FOR THE SELECTION OF ACTIVE (SWITCHES/ROUTERS) AND PASSIVE COMPONENTS

5.1 Justification For Backbone

For the University of Moratuwa's backbone network, active routers are the preferred choice due to their advanced features, scalability, and ability to handle complex routing demands. With a large-scale infrastructure and numerous users, active routers offer dynamic routing protocols, advanced routing functionalities, QoS capabilities, and robust security features. These routers provide the necessary intelligence, flexibility, and scalability to support the university's expanding network requirements and ensure reliable connectivity for departments, research facilities, and campus-wide services.

When selecting between single mode and multi-mode for active and passive components such as routers and switches, several factors need to be considered. Single mode fiber optic cables are designed to transmit data over longer distances compared to multi-mode cables. They have a smaller core size and allow for a single pathway for light transmission. Single mode fiber is ideal for backbone networks that require long-distance connectivity, such as interconnecting routers in different buildings or across large campuses. It offers higher bandwidth and lower signal loss over longer distances, providing reliable and high-performance communication.

On the other hand, multi-mode fiber optic cables have a larger core size, allowing multiple pathways for light transmission. This makes them suitable for shorter distance communication within buildings or floors. Multi-mode fiber is commonly used for connecting devices within the same location, such as switches within a data center or routers within a building. It offers cost-effective connectivity for shorter distances and can handle moderate to high bandwidth requirements.

The selection of single mode or multi-mode fiber depends on the specific requirements of the network. Factors to consider include the distance between routers or switches, the bandwidth needs of the network, and the budget constraints. If the backbone network spans long distances, single mode fiber would be the appropriate choice to ensure reliable and efficient communication. However, if the network is contained within a limited area, such as a building or a floor, multi-mode fiber can provide cost-effective connectivity.

Regarding the number of ports in each router, the quantity should be determined based on the network's size and expected growth. It is important to consider the number of devices that will be connected to the router, including switches, access points, and other network equipment. Additionally, it is advisable to plan for future expansion and accommodate potential increases in network devices. By evaluating the network's current needs and considering future growth projections, the appropriate number of ports can be determined to ensure efficient connectivity and scalability.

5.2 How secure wireless access is ensured

To ensure secure wireless access for the high-level administrative offices at the University of Moratuwa, such as the Chancellor's and Vice-Chancellor's offices, the following measures are implemented: VLAN Segmentation: A dedicated VLAN is created specifically for wireless communication in the administrative offices. This VLAN separates the workstations connected to the access point (AP) in these offices, isolating them from other parts of the network. This segmentation prevents unnecessary broadcast traffic from reaching the wireless network in the administrative area. WPA2-Enterprise Protocol: The wireless network in the administrative offices utilizes the WPA2-Enterprise protocol, which provides advanced security features. This protocol ensures centralized control over the wireless network by requiring users to provide their unique login credentials for authentication. These credentials are preassigned to authorized users and verified through the RADIUS (Remote Authentication Dial-In User Service) server located elsewhere on the network. This centralized authentication process ensures that only authorized personnel can access the wireless network in the administrative area. Limited Wireless Signal Range: To enhance security further, the wireless signal from the access point in the administrative area is restricted to cover only the designated offices. This is achieved by utilizing a specialized antenna with a limited range, ensuring that the wireless network remains confined to the specific administrative offices. By limiting the signal range, the risk of unauthorized access to the wireless network is minimized. By implementing these measures, the University of Moratuwa ensures that the wireless network in the administrative offices remains secure, providing secure and reliable wireless connectivity for authorized personnel in these high-level positions.

6 FEATURES/SPECIFICATIONS OF THE ROUTERS/SWITCHES IN BACKBONE NETWORK

Routers play a crucial role in the backbone network by facilitating efficient routing and connectivity between different networks. When selecting routers for a backbone network, it is important to consider features such as support for routing protocols like OSPF or EIGRP, multiple WAN interfaces for external connectivity, built-in VPN capabilities for secure remote access, quality of service (QoS) mechanisms to prioritize critical traffic, robust security features including firewalls and access controls, and high availability through protocols like VRRP or HSRP. Scalability, management and monitoring capabilities, IPv6 support, and performance specifications such as processing power and throughput should also be considered to ensure the routers can meet the demands of the network.

Switches, on the other hand, are responsible for creating and managing VLANs, providing power over Ethernet (PoE) for devices, implementing link aggregation for increased bandwidth and redundancy, supporting spanning tree protocols for loop prevention, and offering QoS capabilities for traffic prioritization. Additional features include port security measures like MAC address filtering and port authentication, support for multicast traffic handling, network monitoring protocols for traffic analysis, high availability options such as stacking or virtual chassis, scalability for future expansion, and a sufficient number of ports to accommodate network devices.

Choosing routers and switches with the appropriate features and specifications for the backbone network ensures efficient routing, network segmentation, security, high availability, and performance. It is essential to evaluate the specific needs of the network and select devices that align with the network design requirements, scalability plans, and budget constraints.

7 BILL OF QUANTITIES SEPARATELY FOR PASSIVE AND ACTIVE COMPONENTS FOR THE BACKBONE

7.1 Active Components

* Network Switches: High-performance switches with advanced features such as VLAN support, QoS, and routing protocols, suitable for the network's requirements.
* Network Routers: Reliable routers capable of handling routing needs, connecting different networks, and ensuring efficient data transfer.
* Wireless Access Points (APs): Access points providing secure and reliable wireless connectivity throughout the network, supporting WPA2-Enterprise encryption and centralized management.
* Network Firewalls: Robust firewalls ensuring network security with intrusion prevention features, VPN support, and advanced security policies.
* Network Load Balancers: If required, load balancers for distributing network traffic across multiple servers or paths, ensuring optimal resource utilization and high availability.
* Network Servers: Servers for hosting critical services like DNS, DHCP, authentication (RADIUS or LDAP), and other applications specific to the university's needs.

7.2 Passive Components

* Fiber Optic Cables: Fiber optic cables (single-mode or multi-mode) meeting required specifications and standards for long or short-distance connections.
* Copper Ethernet Cables: High-quality Category 6 (or higher) twisted-pair copper cables for device connectivity within the network.
* Patch Panels: Panels for organizing and terminating fiber optic and Ethernet cables, providing a centralized point for easy management.
* Cable Management Accessories: Cable trays, cable ties, and labels for proper cable routing, identification, and reducing clutter.
* Network Racks or Cabinets: Secure and ventilated racks or cabinets to house network equipment, accommodating current and future needs.
* Power Distribution Units (PDUs): PDUs for power distribution to network equipment, including surge protection and monitoring capabilities.
* Cooling Solutions: Mechanisms such as fans or cooling units to maintain suitable operating temperatures for network components.
* Grounding and Bonding Equipment: Grounding bars, cables, and bonding materials for proper grounding and protection against electrical surges.
* Cable Management and Labeling Supplies: Accessories like cable management panels, organizers, and labeling materials for a well-documented and organized infrastructure.
* Tools and Testing Equipment: Network testing tools, cable testers, fiber optic testers, and necessary tools for installation, troubleshooting, and maintenance.

When creating the bill of materials, it is important to consider the compatibility, scalability, and reliability of both active and passive components to ensure an effective network design.

8 SIMULATION RESULTS

Cisco Packet Tracer simulates network traffic and communication by using a variety of packet types. Cisco Packet Tracer frequently uses the following packet types:

* Ethernet Frames: Communication inside a local area network (LAN) is conducted using Ethernet frames. They protect data and transmit it across Ethernet connections. Along with other control information, they provide source and destination MAC addresses.
* IP Packets: The fundamental data units in IP-based networks are IP (Internet Protocol) packets.They are in charge of addressing and routing information and transport data between various network devices.
* ARP (Address Resolution Protocol) Packets: ARP packets are used in local networks to translate IP addresses into MAC addresses. They aid in determining which MAC address corresponds to a given IP address.
* ICMP (Internet Control Message Protocol) Packets: ICMP packets are used to report errors and troubleshoot networks. To identify problems with network connectivity, they transmit error signals such as "ping" requests and answers.
* User Datagram Protocol (UDP) Packets: UDP packets offer lightweight, connectionless data transfer. They are used for services like real-time streaming and DNS that don't need dependable delivery.
* TCP (Transmission Control Protocol) packets offer dependable, connection-oriented data delivery. They make sure that the right data is supplied in the right sequence. TCP is frequently used for assured delivery applications such as online surfing, email, file transfer, and others.
* DNS (Domain Name System) Packets: DNS packets help domain names be translated into IP addresses. They transport requests and answers among DNS servers to speed up name resolution.

We investigated and simulated the local area network of the University of Moratuwa's Department of Electronic and Telecommunication Engineering using Cisco Packet Tracer. Below is an illustration of how we used Cisco Packet Tracer to create the ENTC local area network.

8.1 ENTC LAN Network

8.1.1 Implementation

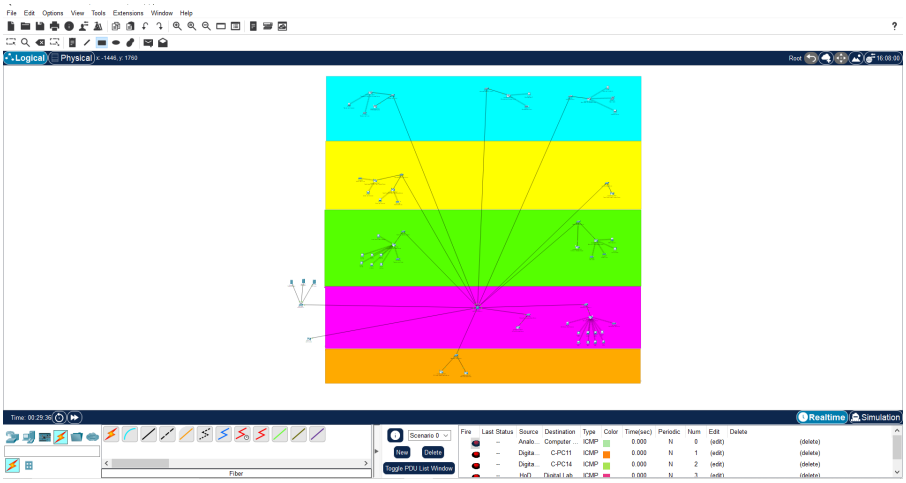

Figure 16 — Implementation of Network of ENTC using Packet Tracer

8.1.2 Simulation

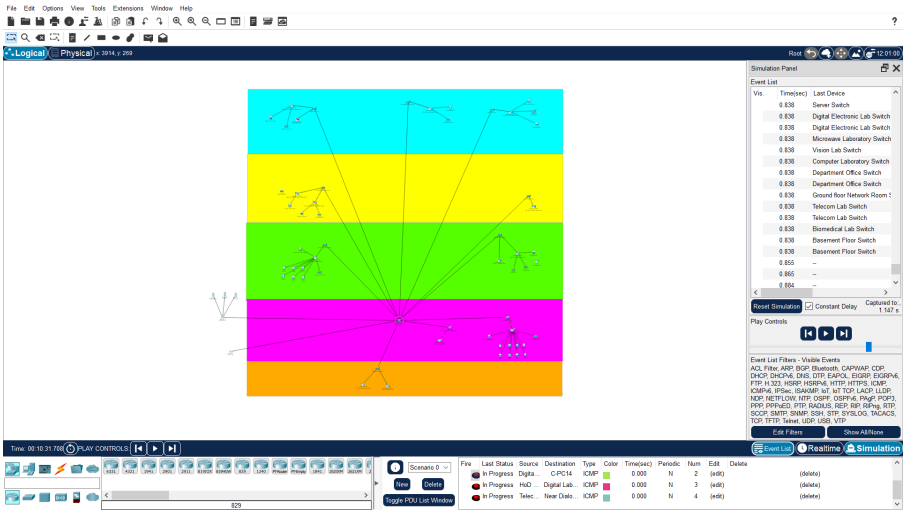

Figure 17 — Simulation of Network of ENTC using Packet Tracer

0.004	Telco	Biomedical Lab	ICMP
0.004	computer laboratory switch	Digital lab	ICMP
0.005	computer laboratory switch	ENTC1	ICMP
0.005	computer laboratory switch	Printer0	ICMP
0.005	Biomedical Lab	computer laboratory switch	ICMP
0.006	computer laboratory switch	Printer0	ICMP
5.000	--	Telecom lab	ICMP
5.000	--	Telecom lab	ICMP
5.001	Telecom lab	computer laboratory switch	ICMP
5.001	--	Telecom lab	ICMP
5.002	Telecom lab	computer laboratory switch	ICMP
5.002	computer laboratory switch	Printer0	ICMP
5.003	computer laboratory switch	Printer0	ICMP
5.003	Printer0	computer laboratory switch	ICMP
5.004	Printer0	computer laboratory switch	ICMP
5.004	computer laboratory switch	Telecom lab	ICMP
5.005	computer laboratory switch	ENTC1	ICMP
10.000	--	Telecom lab	ICMP
10.000	--	Telecom lab	ICMP

Figure 18 — Simulation of Network of ENTC using Packet Tracer

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	Telecom lab	ICMP
	0.000	--	Telecom lab	ICMP
	0.000	--	Printer0	ICMP
	0.000	--	Printer0	ICMP
	0.000	--	Digital lab	ICMP
	0.001	--	Telecom lab	ICMP
	0.001	Telecom lab	computer laboratory switch	ICMP
	0.001	Printer0	computer laboratory switch	ICMP
	0.001	Digital lab	computer laboratory switch	ICMP
	0.001	--	Printer0	ICMP
	0.002	Telecom lab	computer laboratory switch	ICMP
	0.002	Printer0	computer laboratory switch	ICMP
	0.002	computer laboratory switch	Printer0	ICMP
	0.002	computer laboratory switch	Biomedical Lab	ICMP
	0.002	computer laboratory switch	ENTC1	ICMP
	0.003	computer laboratory switch	Printer0	ICMP
	0.003	computer laboratory switch	Telecom lab	ICMP
	0.003	Printer0	computer laboratory switch	ICMP
	0.003	Biomedical Lab	Telco	ICMP

Figure 19 — Simulation of Network of ENTC using Packet Tracer

8.2 backbone

8.2.1 Implementation

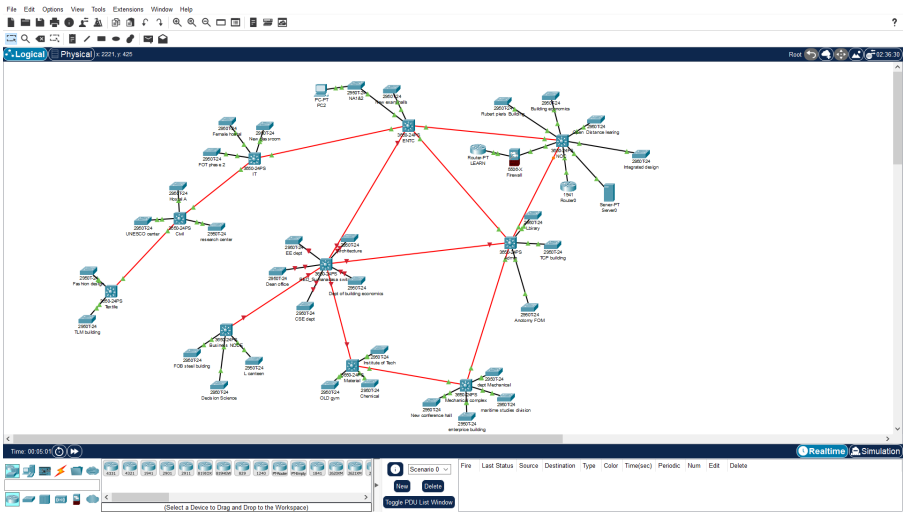

Figure 20 — Implementation of Backbone using Packet Tracer

9 RREFERENCES

* Inbound Traffic of the Network of UOM
* Outbound Traffic of the Network of UOM
* Manage the Backbone Network - CITeS