DEPARTMENT OF ELECTRONICS AND TELECOMMUNICATION ENGINEERING

UNIVERSITY OF MORATUWA

EN2150: COMMUNICATION NETWORK ENGINEERING

NETWORK DESIGN PROJECT

DirectNetz

M.K.D.M. Mirihagalla	200397A
S.N. Pushpakumara	200489H
T.S. Rathnasekara	200529H
S.A.P.U.Satharasighe	200589N

16th May 2023

Table of Contents

1. Back Bone Network

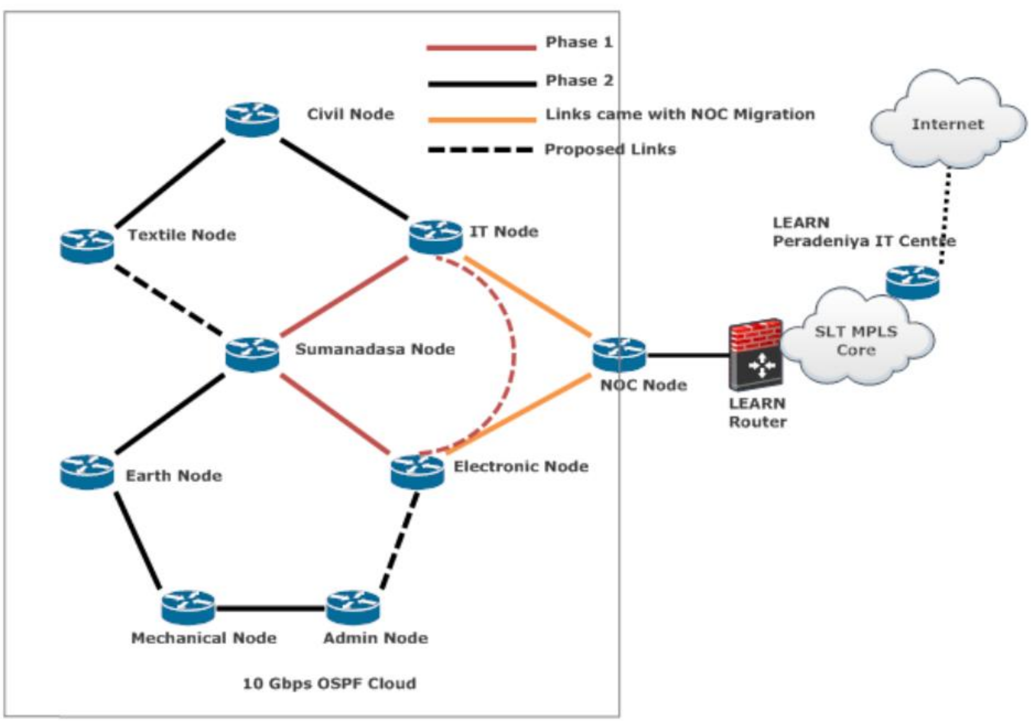
1.1. Current Network

When scope down our sight on the current existing backbone network in the university of Moratuwa, we can clearly observe that it contains a hybrid combination of the ring and star topology. So, it can hardly be refined further, regarding the way it is designed.

So, in the present backbone network, there is a main node named NOC node, which can be regarded as the core device in the backbone network. We can see that from there on, the connection is divided into two main nodes which are named ENTC node and IT node. And finally, from there on the two nodes provide the connection to more and more nodes.

The backbone network which is mentioned above is shown below. According to the pictorial view of the existing backbone network, we can observe that there are some improvements which can be made to make this even faster and less filled with traffic. So, in order to achieve that goal, we had to come up with a new backbone network design, which is designed with a proper topology.

On the other hand, we have to consider how much this consumes both resource-wise and cost-wise. To make the new network a maximum cost effective one, we can use a minimum number of devices (routers, switches etc.) and also we can do the cabling between all buildings in a maximum cost effective manner.



University of Moratuwa Core Network Architecture

1.2. Approach to a new designing

Since this existing network design can be replaced with a new one, with new topologies and new cabling system and several other modest stuff, we came up with a new topology which is a hybrid topology which is made with both ring and star topologies. So, this can be considered as the core layer of the new backbone network design for the university.

After the core layer designing, then we can set our sight on the distribution layer. Starting from the core router we have connected that to a layer 3 switch as the main node, which is the latter one to the firewall used, for the whole university. From there we have created three main layer 3 switches which are implemented hierarchically. These switches can be enlisted as follows.

- ENTC Node
- IT Node
- Admin Node

Physically those we implemented where the building density is much higher.

From these 3 nodes we are going to use the same type of switches beneath those main switches mentioned above. This switch configuration can be gotten into a tabular representation as follows.

ENTC Node	IT Node	Admin Node
Sumanadasa Node	Civil Node	Mechanical Node
Library Node	Female Hostels Node	Library Node
Architecture Node	Faculty of Business Node	
	Male Hostels Node	

After getting these done, we have to consider how the access layer is designed. From the above nodes we can connect them to the layer 2 switches which are implemented in the buildings. Then from that layer 2 switches, connection goes to the wireless access points and finally the end users (laptops, PCs, desktops, mobile phones etc.).

Network diagram clearly indicating all the building nodes and bandwidth in each link.

IP addressing scheme for network (IPv4 and IPv6). Please note that for each node in the network to which a building network is connected an appropriately dimensioned IPv4/IPv6 network is to be given.

1.3. IP addressing scheme for the backbone network (IPv4)

DHCP configuration process using the second option of using the CIDR method, which can be denoted as 169.220.128.11/15.

1.4. Determining the IP Address Range:

1.4.1. IPV4 address allocation for each premises

Node	Expected No of Users	Subnet Size
CITeS		1024
Office	250	1024
Library	1000	2048
ENTC	500	1024
Mechanical	500	1024
Civil	500	2048
Chemical	900	1024
Architecture	800	2048
Textile	850	1024
Sumanadasa	1500	4096
IT	500	2048
Hostel	800	1024
Total		20,000 (approximately)

Decide on the IP address range that falls within the larger subnet. In this case, with a subnet mask of 255.255.128.0, the network portion will span from 169.220.128.11 to 169.220.255.254.

Choose a range within this subnet that can accommodate the desired number of users. For example, you could use the range from 169.220.128.11 to a particular IP address indicating one particular subnet. So, that top of this one subnet can be one of the three main nodes which are mentioned in the approach to the new backbone network design, providing approximately 8192 IPs.

1.4.2. Configuring DHCP Server:

Set up a DHCP server on your network. This can be a dedicated server, or a feature integrated into network equipment like routers or switches. Configure the DHCP server to assign IP addresses within the chosen IP address range.

Specify the lease duration for IP addresses (e.g., 7 days) and any additional DHCP options as needed.

1.4.3. Defining DHCP Scope:

Create a DHCP scope to define the IP address range and other parameters for DHCP clients.

For example, configure a DHCP scope with the following settings:

- Start IP address: 169.220.128.11

- Subnet Mask: 255.255.128.0
- CIDR: 169.220.128.11/15
- Default gateway: The IP address of the default gateway/router: 169.220.128.1
- DNS servers: The IP addresses of one or more DNS servers.

Lease duration: Set the duration for how long the IP addresses will be leased to clients.

1.4.4. Enable DHCP on Network Devices:

Ensure that DHCP is enabled on the network devices (routers or switches) that connect the users' devices. The network devices should be configured to receive their IP addresses automatically from the DHCP server.

1.4.5. DHCP Client Configuration:

Configure the users' devices (computers, IP phones, etc.) to obtain IP addresses automatically via DHCP.

Set the devices to use DHCP for IP address assignment instead of manually assigning static IP addresses.

With this configuration, when a user device connects to the network and requests an IP address, the DHCP server will assign an available IP address from the specified DHCP scope (169.220.128.11 to 169.220.255.254) within the larger subnet (255.255.128.0). The assigned IP address will have the appropriate subnet mask, default gateway, DNS server, and lease duration. This allows for efficient IP address management, automatic configuration, and easy scalability as new devices are added to the network.

2. Justification

1) Core Router

Core router is a major part of the backbone network of the university. Therefore, this should be a high-performance router which is capable of handling major traffic within the network. To tackle that problem, high speed packet forwarding, advanced hardware components and high-speed routing processors are embedded to the system. This uses routing protocols such as OSPF, BGP and IS-IS to exchange data between other routers. Scalability and redundancy of the router are the main features of the router, and this allows us to expand the network further in future without any hesitation. VPN and firewall functionality provide great protection for the network. We can interconnect this with other routers or layer 3 switches by using multiple high-speed interfaces such as gigabit ethernet, 10 gigabit ethernet, 40 gigabit ethernet and 100 gigabit ethernet.

2) Layer 3 Switches for aggregating layer 2 switches

Layer 3 switches are able to decide which paths packet should go by intelligently considering all the factors that affect the latency of the transmission. Therefore, this can manage the traffic between VLANs and increase the network performance by reducing the load on core router. As well as this layer 3 routers uses hardware-based switching technique and provides them fast packet forwarding functionality. This reduces the latency and enhances the throughput of the network. Architecture of the layer 3 switches facilitate for flatter and scalable design in the most of networks. Because here we are not relying on the core router. Hence, it prevents a single point of failures and provides flexible network expansion.

3) Layer 2 Switches for aggregating access points

In our Design we used layer 2 switches for aggregating access points in simple manner to reduce the complexity of the network. This can be used to create necessary features as such VLANs. In these switches we use copper cable to interconnect access points with layer 2 switches. In our design we try to reduce daisy chain by adding switches to subnets as much as possible. Since layer 2 switches have high switching power, we can reduce the latency of subnets.

4) Access Points

End users directly connect to the access point via wi-fi. As a result of that, there may be huge traffic when a high number of users occupy one access point. Therefore, access points manage the downfall effectively. This is a centralized management process and administrators with a convenient interface are able to configure and monitor the access points, apply consistent network policies, and ensure good

performance. Scalability is another advantage of these access points. If the allowable number of devices which connect to one access point is filled, then we can add another access point to expand the network. Since this is a wireless connection, guest access capability can be handled in a convenient manner. As well as costs for the cabling and maintenance are reduced while providing the same network connectivity benefits.

5) DHCP Server

Using DHCP server, we assigned IP addresses for servers, layer 3 switches and hosts in automatic manner. By assigning IP addresses in this manner, we can efficiently utilize the IP addresses and provide flexibility to manipulate the assignment of IP addresses. This allows us to enhance the scale of the network in a very productive manner. In addition to that, network administration is much easier than assigning IP addresses manually.

6) Web server, SMTP server, DNS Server, and FTP server

In our backbone, several numbers of servers have been connected for different kinds of tasks.

First, we consider the Web server. This maintains the data of the University web site, LMS and Moodle. Therefore, this is directly connected to layer 3 switch and that reduces congestion to server.

SMTP server handles the university email service by giving reliable service for the clients. FTP server manages the Data Management System of the university.

DNS of the backbone provides a mapping between IP addresses and domain names of the university. Therefore, this is a critical part of the backbone of the university. This provides accessibility to each service provided by the university.

7) Single mode Fiber Optic cables

In backbone, we are going to use 40 Gbps single mode fiber optic cables for interconnecting layer 3 switches. Due to high demand in network accessing, we have to use physical medium which has high bandwidth. Since optical waves are propagating along the cables, attenuations and distortions are not considered that much in single mode fiber cables. As well as one of the main requirements of the network is high speed data transmission. Hence, we decided to use 40 Gbps fiber instead of 10Gbps fibers.

8) Fast Ethernet Cables

Fast ethernet cables are used the places where the data speed requirement and bandwidth requirement are low. By implementing this in such a manner, we can reduce the unnecessary costs and reduce the complexity of the network.

Features/specifications of the routers/switches in backbone network

2.1. Specifications and features of the Core Router

- High speed switching and performance – Complex hardware and high-power processors are used to manage the traffic and to provide services.
- Supports IPv6
- Provides secured channel by using Virtual Private networks (VPN), firewalls and Access Control Lists (ACLs)
- Supports network interfaces such as gigabit ethernet ,10 gigabit ethernet, 40 gigabit ethernet, 100 gigabit ethernet and fast ethernet

2.2. Specifications and Features of Layer 3 Switches

- VLAN supports – this feature is used to logically separate the network. This will enhance the security of the network and ensure efficiency. Management of VLAN is relatively less complicated.
- Supports for IPv6
- Access control features – reduce the incoming and outgoing traffic of the network and increase the security of the network.

- High speed switching capability than layer 2 switches
- Supports various routing protocols such as BGP, RIP, OSPF and EIGRP
- 4 gigabit Ethernet connections and multiple fast ethernet connections

2.3. Specifications and Features of layer 2 Switches

- High speed switching power
- Supports VLAN feature.
- Spanning Tree Protocol (STP) is used for preventing network loops and adding redundancy for the network.
- Incorporates security features such as Access Control Lists (ACLs)
- 24 fast ethernet connections

2.4. Specifications and Features of Access Points

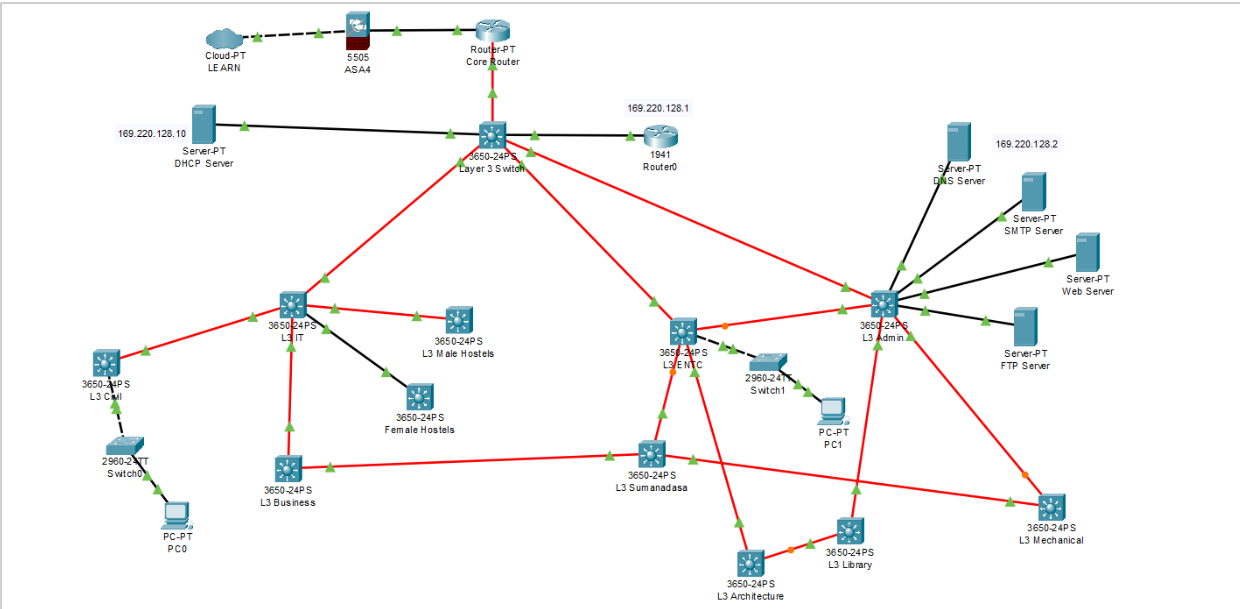
- Wireless connection (wi-fi)
- Allows to access more than 500 users at once.
- 100 Mbps maximum data transferring rate in both uplink and downlink
- Operate between either in 2.4GHz or 5GHz frequency bands.
- Uses data encryption method such as WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) , WPA2 and WPA3
- Provides guest access capability.
-

2.5. Bill of Quantities

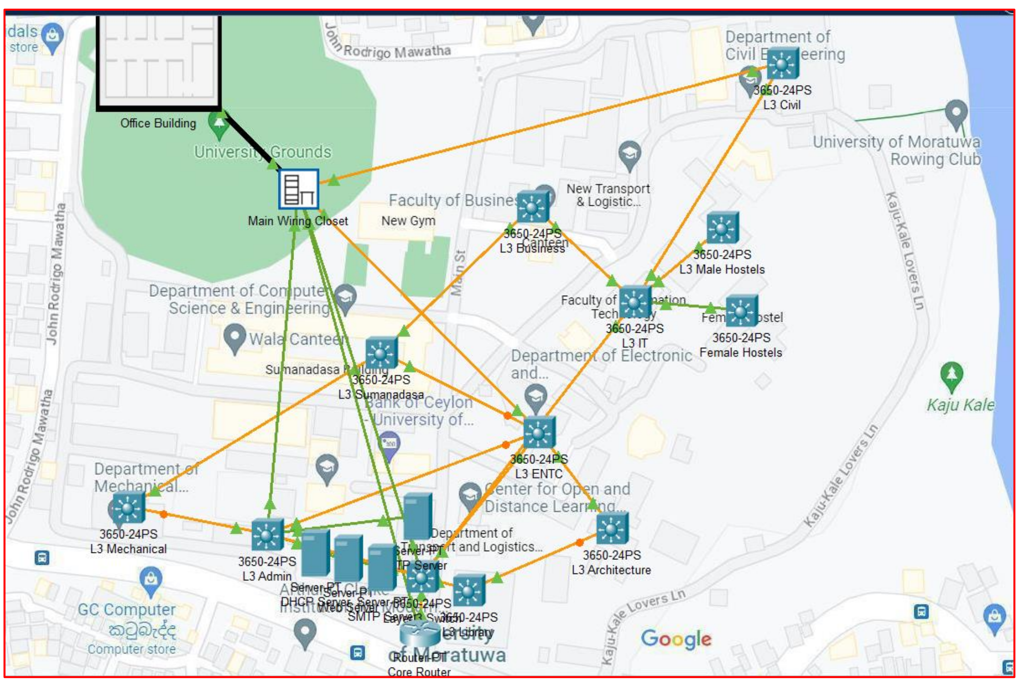
Component	*Price*	*Quantity*	*Total Cost*
Catalyst 3650 Switch - *WS-C3650-48PS-S*	$5,200.00	12	$20,800.00
Cisco ASR 1000 Series router (ASR1002-x)	$21,200.00	*1*	$21,200.00
Cisco Router ISR 4221 / K9	$1,222.00	*1*	$1,222.00
10Gb OM3 Multimode Duplex Fiber Optic Cable – 100 m	$90.11	*9*	$810.99
40Gb OM3 Multimode Duplex Fiber Optic Cable – 100 m	$123	*4*	$492

2.6. Simulation results

Logical View of Back born



Physical View of Back Born



2.6.1. Pinging inside backbone Network

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 169.220.128.14

Pinging 169.220.128.14 with 32 bytes of data:

Reply from 169.220.128.14: bytes=32 time=15ms TTL=128
Reply from 169.220.128.14: bytes=32 time<1ms TTL=128
Reply from 169.220.128.14: bytes=32 time=11ms TTL=128
Reply from 169.220.128.14: bytes=32 time<1ms TTL=128

Ping statistics for 169.220.128.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 15ms, Average = 6ms
```

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 169.220.128.13

Pinging 169.220.128.13 with 32 bytes of data:

Reply from 169.220.128.13: bytes=32 time<1ms TTL=128
Reply from 169.220.128.13: bytes=32 time<1ms TTL=128
Reply from 169.220.128.13: bytes=32 time=1ms TTL=128
Reply from 169.220.128.13: bytes=32 time<1ms TTL=128

Ping statistics for 169.220.128.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

2.6.2. Trace route

```
C:\>tracert 169.220.128.14

Tracing route to 169.220.128.14 over a maximum of 30 hops:

  1   0 ms      0 ms      6 ms      169.220.128.14

Trace complete.
```

```
C:\>tracert 169.220.128.13

Tracing route to 169.220.128.13 over a maximum of 30 hops:

  1   1 ms      0 ms      0 ms      169.220.128.13

Trace complete.
```

2.6.3. Arp Table

```
C:\>arp -a
  Internet Address      Physical Address      Type
  169.220.128.14        0001.c75c.e7cd        dynamic
```

2.6.4. ICMP packet sending in Simulation view

Root 04:32:00

Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC0	ICMP
	0.001	PC0	Switch0	ICMP
	0.002	Switch0	L3 Civil	ICMP
	0.003	L3 Civil	L3 IT	ICMP
	0.004	L3 IT	Layer 3 Switch	ICMP
	0.005	Layer 3 Switch	L3 ENTC	ICMP
	0.006	L3 ENTC	Switch1	ICMP
	0.007	Switch1	PC1	ICMP
	0.008	PC1	Switch1	ICMP
	0.009	Switch1	L3 ENTC	ICMP
	0.010	L3 ENTC	Layer 3 Switch	ICMP
	0.011	Layer 3 Switch	L3 IT	ICMP
	0.012	L3 IT	L3 Civil	ICMP
	0.013	L3 Civil	Switch0	ICMP
	0.014	Switch0	PC0	ICMP

3. ENTC network

3.1. Introduction regarding the Basics to Look into, at ENTC Network

Designing a complete network infrastructure involves carefully considering and planning various elements to ensure a reliable, efficient, and scalable network. Let us see some critical elements in a network when we are replicating ENTC network and what they are doing in a network.

- **The cabling network** is an important part of any network. It is responsible for transporting data between devices. The cabling network should be designed to be reliable, secure, and scalable.

These are some of the key factors when deciding the cabling system for a network.

- Use high-quality cables and connectors.
- Install the cabling network in a secure location.
- Label the cables and connectors for easy identification.
- Use a structured cabling system to organize the cables.
- Plan for future expansion.

- **Network sockets:**

  also known as wall outlets or data jacks, are installed in various locations throughout the building. These sockets provide the physical connection point for devices such as computers, IP phones, or wireless access points.

- **Patch panels:**

  Mainly there can be 2 types of patch panels used.

  - Copper Patch Panels: These panels provide termination points for copper cables. They have multiple ports on the front for connecting patch cords and are typically installed in a structured cabling or server room. Each port on the patch panel corresponds to a network socket in the building.
  - Fiber Patch Panels: Fiber patch panels serve a similar purpose but specifically for terminating and managing fiber optic cables. They provide connectivity and organization for fiber connections within the network infrastructure.

  .

- **Distribution racks:** Distribution racks are cabinets that house patch panels, switches, and other network equipment. They provide a central location for network equipment and make it easy to manage the cabling network.

- **Copper and fiber patch cords**

    - **Copper Patch Cords:** These are short Ethernet cables with connectors on both ends (often RJ45 connectors) used to establish connections between devices and patch panels.
    - **Fiber Patch Cords:** Fiber patch cords are used to connect devices or equipment to fiber optic patch panels. They have fiber connectors (such as LC, SC, or ST) on both ends.

- **Network switches and Routers**

    Network **switches** are responsible for connecting multiple devices within a local network (LAN). They receive data packets from connected devices and forward them to the appropriate destination within the network. Our designing of ENTC network, we have considered an hierarchical design such that ENTC would be getting connected to outside with a 3-Layer switch. Below that level we have added layer 2 switches with fiber cabling until 2-layer switches. Then the copper cabling was used.

    Routers are responsible for routing data packets between different networks, such as connecting a local network to the internet or linking multiple LANs together. But in ENTC network does not contain any routers. One router is there in the UOM backbone and with which we connect the network to "Learn", the ISP.

3.2.IP addressing scheme for the network (IPv4)

In DHCP configuration process using a larger subnet mask (255.255.128.0) to accommodate 32 000 users:

3.2.1. Determining the IP Address Range:

Decide on the IP address range that falls within the larger subnet. In this case, with a subnet mask of 255.255.128.0 the network portion will span from 169.220.128.11 to 169.220.255.254.

Choose a range within this subnet that can accommodate the desired number of users. For example, we could use the range from 169.220.128.11 to 169.220.255.254 providing 32,768 Ip addresses.

3.2.2. Configuring DHCP Server:

Set up a DHCP server on your network. This can be a dedicated server, or a feature integrated into network equipment like routers or switches. Configure the DHCP server to assign IP addresses within the chosen IP address range.

By Specifying the lease duration for IP addresses (e.g., 7 days) and any additional DHCP options as needed.

3.2.3. Defining DHCP Scope:

Create a DHCP scope to define the IP address range and other parameters for DHCP clients.

For example, configure a DHCP scope with the following settings:

- Start IP address: 169.220.128.11
- End IP address: 169.220.255.254
- Subnet mask: 255.255.128.0
- Default gateway: The IP address of the default gateway/router. (169.220.224.1)
- DNS servers: The IP addresses of one or more DNS servers.

Lease duration: Set the duration for how long the IP addresses will be leased to clients.

3.2.4. Enable DHCP on Network Devices:

Ensure that DHCP is enabled on the network devices (routers or switches) that connect the users' devices. The network devices should be configured to receive their IP addresses automatically from the DHCP server.

3.2.5. DHCP Client Configuration:

Configure the users' devices (computers, IP phones, etc.) to obtain IP addresses automatically via DHCP. Set the devices to use DHCP for IP address assignment instead of manually assigning static IP addresses. With this configuration, when a user device connects to the network and requests an IP address, the DHCP server will assign an available IP address from the specified DHCP scope from 169.220.128.11 to 169.220.255.254. within the larger subnet (255.255.128.0). The assigned IP address will have the appropriate subnet mask, default gateway, DNS server, and lease duration. This allows for efficient IP address management, automatic configuration, and easy scalability as new devices are added to the network.

3.2.6. Access Points:

In total we have used 15 access points for the ENTC department building. Using multiple access points for the floors allows for easier movement throughout the floor and ensures compliance with accessibility codes and regulations. Depending on the size and layout of the floor, multiple access points can help distribute people more evenly, reducing congestion and improving the flow of foot traffic.

In detail, for the ground floor, there are 3 access points, one for UAV lab, one for ENTC-1 and the remaining one for bio medical lab. Ans 0.5 has also been allocated an access point. Above places are always crowded I.e., number of users for internet is very high in those area. Hence, in order to reduce congestion and improve the flow of foot traffic those access points are needed.

In addition, on the 1st floor access points are places near the lecturer's rooms and the other access point is near the conference room. That placement covers the entire floor very easily.

The number of access points required for a floor can vary depending on local building codes, regulations, and the specific needs of the building occupants. In that theory, for the second floor 4 access points were placed in analog lab, digital lab, up common and instructors' area. Likewise, congestion in those areas can be reduced more than it used to be.

In contrast to the existing network, an access point has been established near the 3.5 which covers the PG seminar rooms and other rooms. And the access points cover the floor as well. So and so for access points are placed.

3.2.7. **Switches:**

L3:

Because of advanced routing capabilities L3 switches are used for buildings**.** L3 switches are able to route traffic based on IP addresses. Allowing them to efficiently direct data between different subnets or Lans within the buildings. L3 switches can efficiently manage the flow of data within a building, ensuring smooth communication between different devices and networks.

L2:

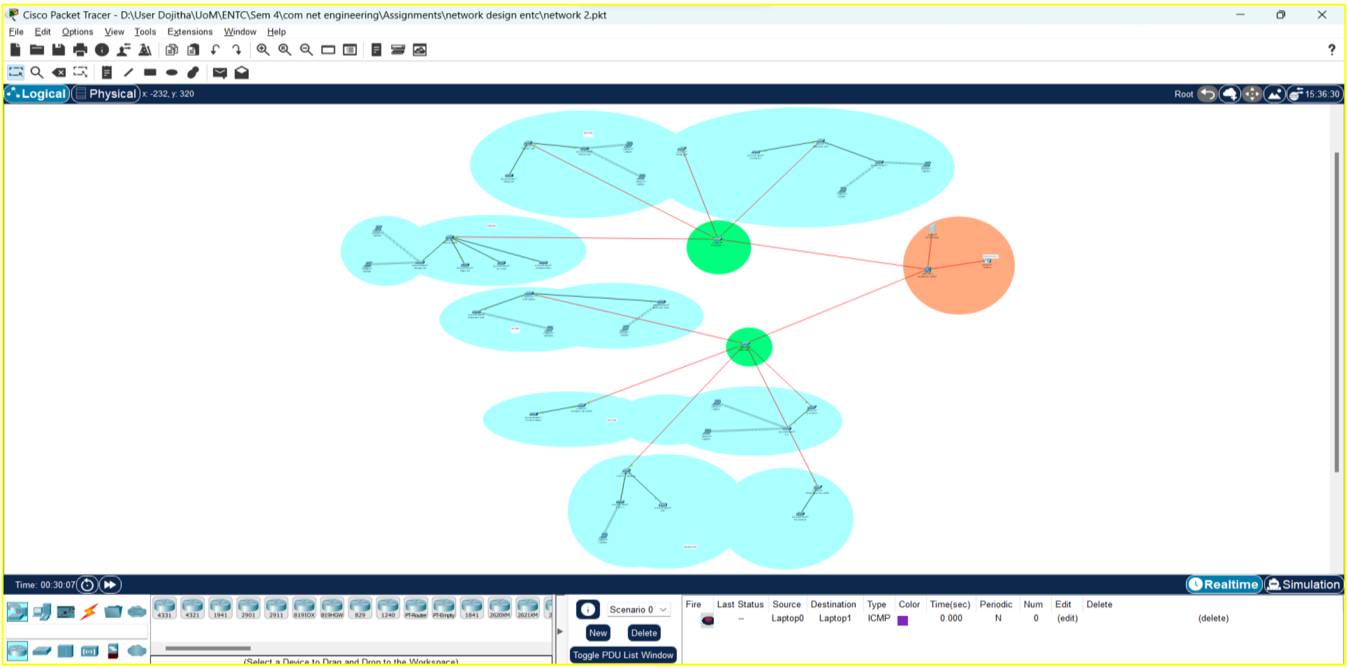
In order to handle ethernet frames and make forwarding decisions based on MAC addresses. And also, a cost-effective solution for reducing the overall network congestion and improving performance. L2 switches efficiently forward frames directly to the intended destination without flooding the entire network.

Cables:

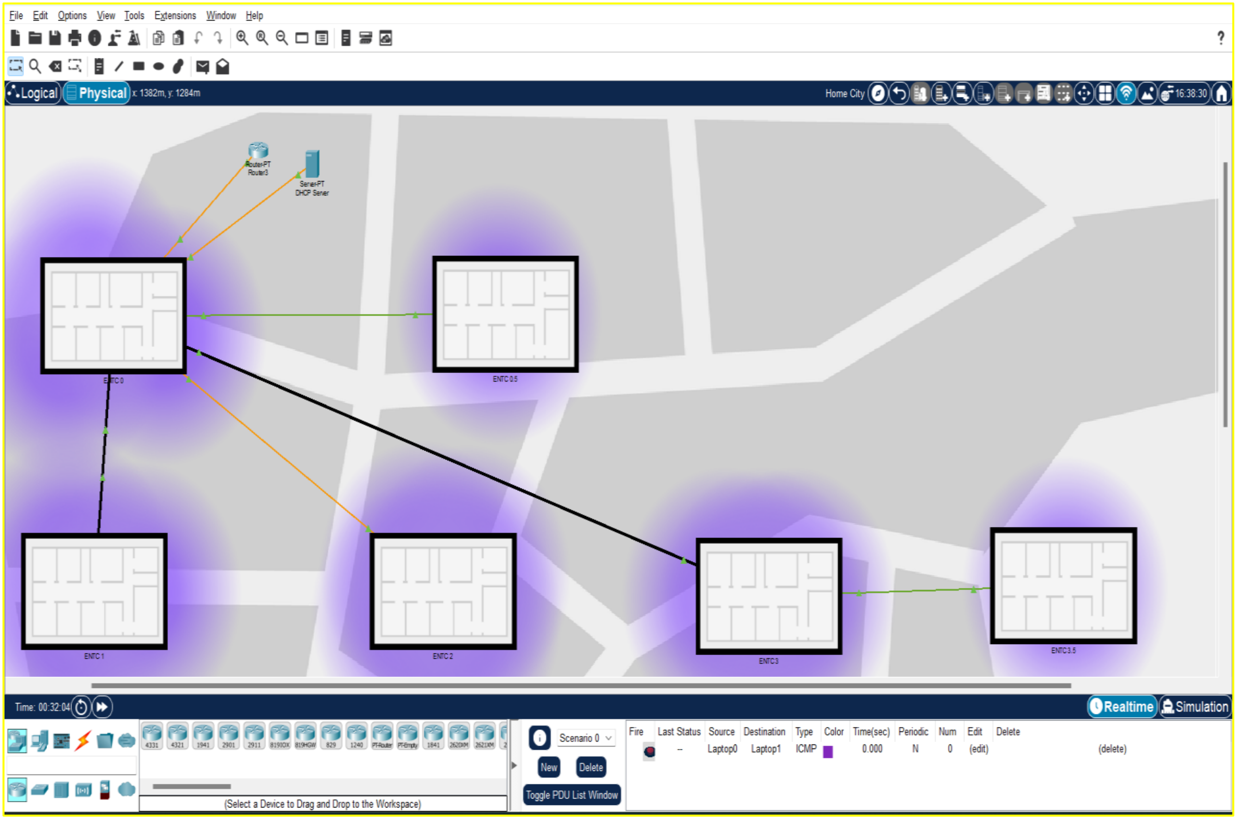
In order to achieve High Speed and Bandwidth, Gig fiber cables are able to support data transfer rates of up to 10 gigabit per second. This helps to get rid of the congestion that arise when the higher number of users are accessing the internet. On the other hand, the reliability of those cables ensures consistent and stable compared to copper cables.

RJ-45 cables are used to make the connection between access points and relevant switches

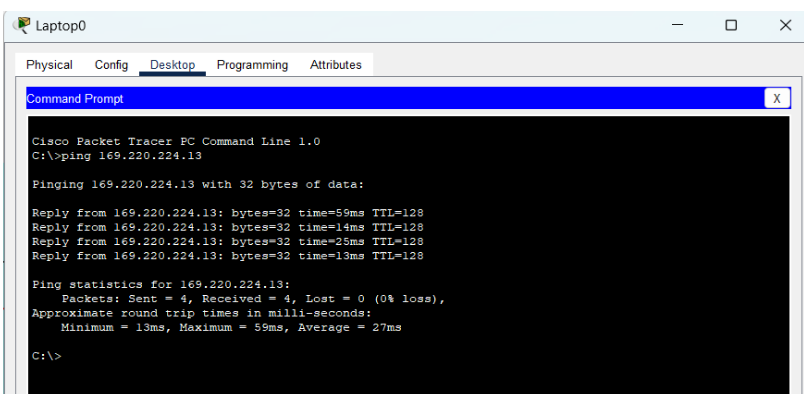
3.3. Simulation results



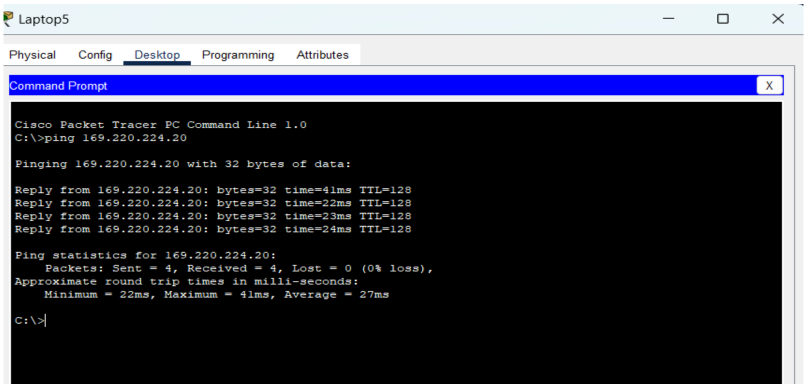
Logical View of ENTC Hierarchical network



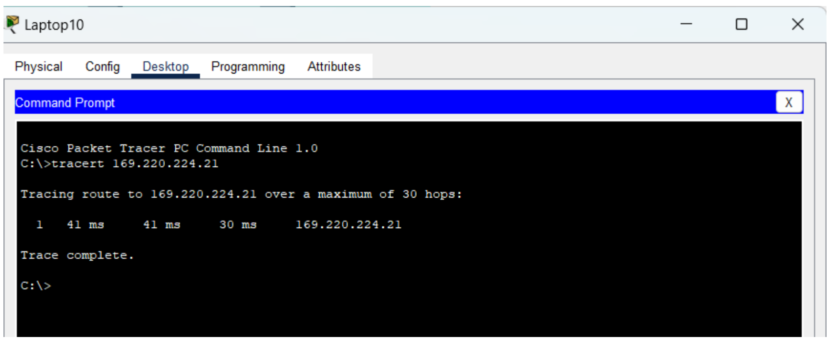
Physical View of the network in each floor



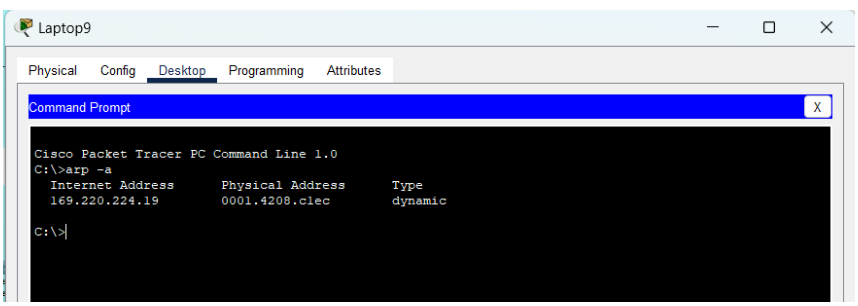
Pinging a laptop in 3rd floor from ground floor



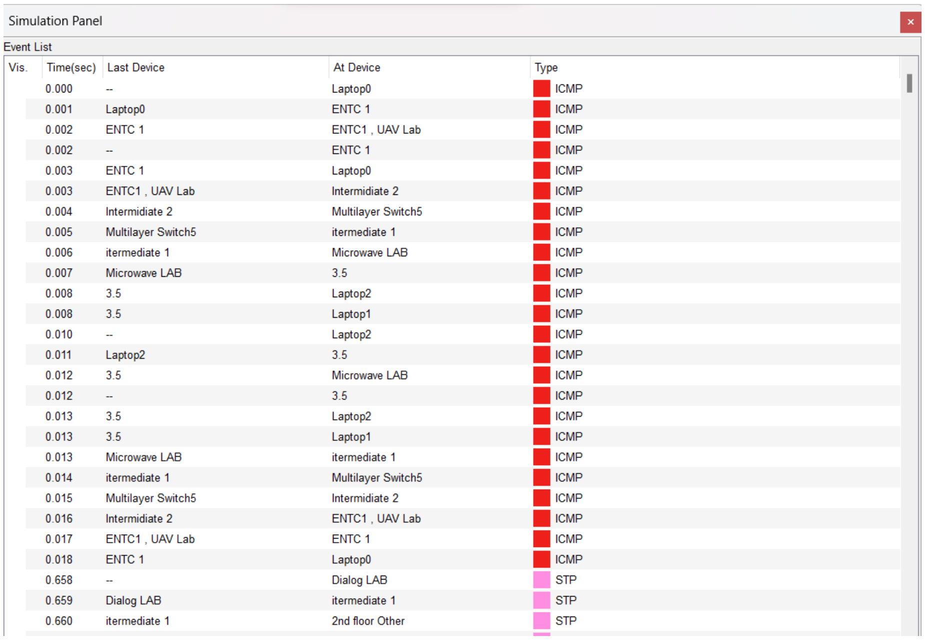
Pinging a laptop in 2nd floor from ground floor



Trace route a laptop inside the ENTC network.



ARP table



Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	Laptop0	ICMP
	0.001	Laptop0	ENTC 1	ICMP
	0.002	ENTC 1	ENTC1 , UAV Lab	ICMP
	0.002	--	ENTC 1	ICMP
	0.003	ENTC 1	Laptop0	ICMP
	0.003	ENTC1 , UAV Lab	Intermidiate 2	ICMP
	0.004	Intermidiate 2	Multilayer Switch5	ICMP
	0.005	Multilayer Switch5	itermediate 1	ICMP
	0.006	itermediate 1	Microwave LAB	ICMP
	0.007	Microwave LAB	3.5	ICMP
	0.008	3.5	Laptop2	ICMP
	0.008	3.5	Laptop1	ICMP
	0.010	--	Laptop2	ICMP
	0.011	Laptop2	3.5	ICMP
	0.012	3.5	Microwave LAB	ICMP
	0.012	--	3.5	ICMP
	0.013	3.5	Laptop2	ICMP
	0.013	3.5	Laptop1	ICMP
	0.013	Microwave LAB	itermediate 1	ICMP
	0.014	itermediate 1	Multilayer Switch5	ICMP
	0.015	Multilayer Switch5	Intermidiate 2	ICMP
	0.016	Intermidiate 2	ENTC1 , UAV Lab	ICMP
	0.017	ENTC1 , UAV Lab	ENTC 1	ICMP
	0.018	ENTC 1	Laptop0	ICMP
	0.658	--	Dialog LAB	STP
	0.659	Dialog LAB	itermediate 1	STP
	0.660	itermediate 1	2nd floor Other	STP

ICMP packet transmission check – Simulation view