EE4718 Project Report

Group Members: Cheng Kejun,Merchant Mahek Isak,Sanjena Suresh

School of Electrical and Electronic Engineering
Academic Year 2022/23
Semester 1

Table of Content

Chapter 1. Introduction and design objectives

The rapid expansion and development in the field of education have led to the growth of institutions and the need for robust and efficient network infrastructure. The School of Electrical and Electronic Engineering (EEE) has recently added two new buildings, S2.1 and S2.2, to its campus in order to provide cutting-edge research and lab facilities for its students and staff. This report aims to present a comprehensive network design project for the school, addressing the requirements and constraints of the enterprise network to ensure seamless communication, resource sharing, and remote networking capabilities among various user groups and buildings.

The primary objective of this network design project is to create an efficient, secure, and scalable enterprise network that meets the needs of the different user groups and supports the seamless interconnection of local area networks (LANs) in various labs and offices through a wide area network (WAN). The design must take into consideration the following key requirements:

1. Enable interworking, file sharing, printer access, and remote networking for the School of EEE's new buildings, S2.1 and S2.2.
2. Accommodate four user groups, namely academic staff (Acad), administrative staff (Admin), research students (RS), and lab PC users (Lab), while ensuring access to shared resources and workgroup functionality.
3. Implement a secure and optimized IP addressing scheme using variable length subnet mask (VLSM) subnetting to maximize route aggregation and minimize address wastage.

4. Ensure that all users have access to shared printers within their respective rooms and dedicated printers for each workgroup when different user groups share the same room.
5. Adhere to the specific access restrictions for different user groups to maintain security and prevent unauthorized access to sensitive data and services.
6. Incorporate efficient network services such as DHCP and dynamic routing to facilitate the flexible implementation of the enterprise network.
7. Design the network based on the TCP/IP protocol to ensure compatibility with existing systems and devices.

By addressing these objectives and requirements, this network design project aims to provide the School of EEE with a robust and efficient enterprise network that supports its research and educational activities while facilitating seamless communication and resource sharing among its users.

Chapter 2. Top-down analysis of network requirements

In this chapter, we introduce the top-down approach to network design and explain how we implemented this method in our project. The top-down strategy focuses on understanding the organization's needs, objectives, and constraints before diving into the specifics of individual components and configurations. This approach ensures that the network design aligns with the organization's goals and requirements, resulting in a tailored solution that is efficient and scalable.

The general steps in a top-down approach to network design are as follows:

1. Identify business objectives and requirements: Begin by understanding the organization's goals, needs, and constraints, such as budget, timelines, and desired performance levels. Consider the required network services, applications, and user expectations.
2. Perform a needs analysis: Assess the current network infrastructure, if one exists, and identify its shortcomings and areas for improvement. Collect information on the projected growth of the organization, user count, and future requirements.
3. Develop a high-level network architecture: Design a high-level network architecture that addresses the identified needs and objectives. This may include defining the overall topology, connectivity between locations, and core network services.
4. Select network technologies: Choose the appropriate network technologies and protocols that best meet the organization's requirements, such as Ethernet, Wi-Fi, or

MPLS. Consider factors like performance, scalability, and compatibility with existing infrastructure.

5. Develop a detailed network design: Break down the high-level architecture into individual components, such as routers, switches, and firewalls, and design their configurations. This step may involve planning IP addressing, routing protocols, VLANs, and other specific configurations.
6. Plan for network security: Develop a comprehensive security strategy that addresses potential threats and vulnerabilities. This may include firewalls, intrusion detection systems, access control lists, and encryption mechanisms.
7. Implement and test the network: Deploy the designed network infrastructure and configurations, and thoroughly test the network to ensure it meets the desired performance levels, security measures, and functionality.
8. Monitor and optimize the network: Continuously monitor the network's performance, troubleshoot any issues, and optimize the network to ensure it meets the organization's evolving needs.

A Local Area Network (LAN) segment refers to a portion of the network utilized by a specific user group and isolated from the rest of the LAN by a bridge, router, or switch. Networks are separated into different segments for security purposes and to enhance traffic flow by filtering out packets that are not intended for the segment.

When implementing LAN segmentation, the following constraints are considered based on the project requirements:

1. The link between the various LAN segments should be restricted to connect only across one room.

2. Hosts are limited to a combination of two neighboring rooms within a single LAN segment.

Depending on the need to minimize network address waste, a LAN segment can either join a larger LAN that connects to an adjacent room or be divided into smaller LAN segments to optimize address space usage. LAN segments within a lab should not be connected to those in another lab or workgroup; however, LAN segments within the same workgroup can be connected to form a larger LAN. LAN segments must not exceed the network's maximum operational diameter, which, for convenience, will be the distance between two adjacent labs or offices.

Chapter 3. Bottom-up network implementation of logical networks

In this chapter, we discuss the bottom-up approach to network design, which focuses on building the network infrastructure from the ground up, starting with the selection of individual components and progressing towards the implementation of higher-level configurations and services. This method enables effective communication between devices connected to LANs and WANs within the network.

The general guidelines in a bottom-up strategy for network design are as follows:

- Define basic requirements: Start by determining the network's goals, including its user base, service offerings, and performance standards. This will help identify the necessary hardware and software.
- Choose network devices: Select the suitable switches, routers, access points, and firewalls for your network while taking into account variables like cost, productivity, and scalability.
- Plan the physical layout: Establish the network's physical layout, taking into account the locations of devices, cable lines, and access points. This action is essential for maintaining a secure and reliable network infrastructure.
- Implement the data link layer: To ensure effective data transmission between devices, design and configure data link layer protocols like Ethernet. Setting up VLANs, trunking, and other link layer configurations are included in this category.

- Configure network layer protocols: To guarantee proper communication between devices on the network, configure network layer protocols including IP addressing and routing protocols. Subnetting, IP address assignment, and routing table configuration are included in this stage.
- Setup network services: To enable various network operations and make administrative duties easier, implement and configure network services including DHCP, DNS, and Network Time Protocol (NTP).
- Deploy security measures: To protect the network from illegal access and potential threats, design and implement security mechanisms including firewalls, access control lists (ACLs), and encryption.
- Improve and monitor the network: Network monitoring and optimization are essential to ensuring that the network is operating at the required levels of performance and that user needs are being met.

Following the top-down analysis outlined in Chapter 2, we employ a bottom-up network design approach to enable devices connected to LANs and WANs to communicate effectively. This method utilizes a three-layer hierarchical structure to construct the physical network, laying the foundation for efficient and scalable network infrastructure.

Planning of Host-IP addresses:

This project makes use of IPv4 addressing. This indicates that each IP address has a length of 32 bits. Moreover, a globally unique IP address should be given to each host (PC, printer, server) in the network. There are three main classes of IP addresses (Class A, B, and C) that can be assigned to a host.

Table 3-1. IPv4 classes and number of addresses available

Class	No. of Host IDs	No. of hosts a network address can support
A	24	2^24 – 2 = 16 million
B	16	2^16 – 2 = 65534
C	8	2^8 – 2 = 254

The host ID bits cannot be all 0's or all 1's. Hence in order to exclude the 2 cases we subtract by 2.

Before we can choose the most appropriate class of IP address to use, we need to find the largest possible total number of hosts in Blocks S2.1 and S2.2.

Table 3-2. Total number of Hosts in S2.1 and S2.2

Location	Acad		Admin		RS		Lab		
Block S2.1	**Host**	**Net#Subnet Bits**	**Host**	**Net#Subnet Bits**	**Host**	**Net#Subnet Bits**	**Host**	**Net#Subnet Bits**	**Total Number**
S2.1-b2	36		12						
S2.1-b3-01			4		20		56		
S2.1-b3-02			4		6				
S2.1-b4-01			2		15		26		
S2.1-b4-02			1		15		20		
S2.1-b4-04			4		20		40		
S2.1-b5-02			1				6		
S2.1-b6-01							8		
S2.1-b6-02			1				6		
Total Hosts	**36**		**29**		**76**		**162**		**303**

Block S2.2	**Host**	**Net#Subnet Bits**	**Host**	**Net#Subnet Bits**	**Host**	**Net#Subnet Bits**	**Host**	**Net#Subnet Bits**	**Total Number**
S2.2-b2	24		3						
S2.2-b3-03					5				
S2.2-b3-04			2		6		28		
S2.2-b3-05			2		20				
S2.2-b3-06									
S2.2-b3-07			1		12				
S2.2-b3-08			1		6				
S2.2-b4-02			2		12		24		
S2.2-b4-03			1		15		16		
S2.2-b4-04			4		10		50		
S2.2-b5-02			2				12		
S2.2-b6-02			1				12		
Total Hosts	**24**		**19**		**86**		**142**		**271**

The total number of hosts needed is a lot less than what an individual Class B network address can provide which is 65534. Hence, a tremendous number of the host-IDs available will be wasted if only one Class B network address is utilized. Utilizing a single Class C

network is not sufficient as all hosts cannot be supported because it can only support up to 254 hosts. Therefore, using a few Class C network addresses, one for each logical network, is a preferable alternative.

Initially, the user groups “Acad” and “Admin” are allocated to one logical network. Next, a different logical network is given the designation "RS." Finally, "Lab" has two logical networks since the total number of hosts for "Lab" will be 162 + 142 = 304. This is greater than the maximum number of hosts that may be supported by a single Class C network address. One Class C network address is also needed for this architecture to cover some serial link interfaces. Hence, a total of five Class C network addresses are required.

Table 3-3. Supernet assignment for workgroups

User Group	Supernet	
	Block S2.1	Block S2.2
Acad + Admin	**200.10.10.0 / 25**	**200.10.10.128 / 25**
RS	**200.10.11.128 / 25**	**200.10.11.0 / 25**
Lab	**200.10.12.0 / 23**	**200.10.14.0 / 24**

Variable Length Subnet Mask (VLSM) and Fixed Length Subnet Mask (FLSM)

The two methods we employ for subnetting an IP are:

- Fixed length subnet mask (FLSM)
- Variable length subnet mask (VLSM)

The allocation of IP address space inside each organization is described by FLSM and VLSM.

When using a fixed-length subnet mask (FLSM), a block of IP addresses is divided into many subnets that are all of the equivalent size. This is also known as classful subnetting.

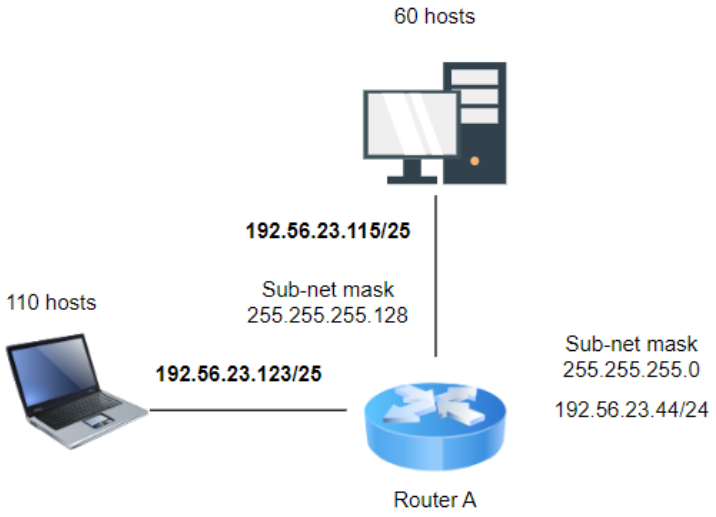


Fig 3-1. classful subnetting

Variable-length subnet mask (VLSM) describes a technique that enables all subnetworks to have variable sizes. In order to partition an IP address space into subnets of different lengths and allocate them according to the specifications of the network, network administrators can utilize VLSM subnetting. This is also known as classless subnetting.

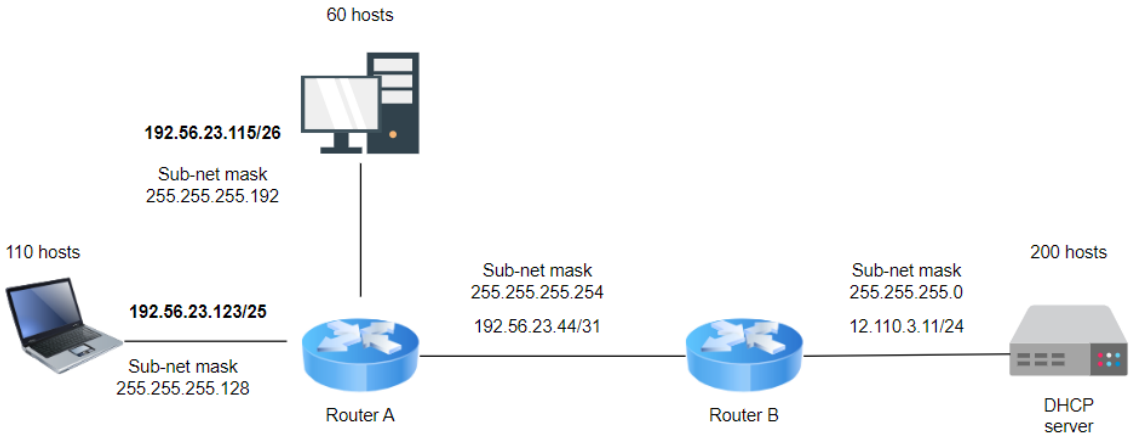


Fig 3-2. VLSM subnetting

While VLSM is more appropriate for public IP addresses, FLSM is a better option for private IP addresses. FLSM frequently wastes IP addresses by using more of them than are required. VLSM utilizes a specific IP address range more effectively, resulting in less waste.

Requirements:

- Additional IP addresses for assignment to printers for all user groups
- Additional IP addresses for assignment to server for each lab
- Additional IP addresses for assignment to file server for RS, Acad and Admin respectively
- Additional IP addresses for assignment to group email server, accessed by Acad and Admin, and its router interfaces
- Additional IP addresses for assignment to router interfaces for all user groups within Access layer
- Additional IP addresses for router interfaces within Core layer

Table 3-3. Subnet assignment for supernet 200.10.10.0/25

	Location								
Department	**Block S2.1**	**Net#Subnet Bits**	**Binary Rep**	**Subnet Mask**	**Router Address**	**First Host**	**Last Host**	**Printer**	**DHCP Server**
Acad	S2.1-b2	200.10.10.96/27	200.10.10.011/27	255.255.255.224	200.10.10.97	200.10.10.98	200.10.10.125	200.10.10.126	
Acad	S2.1-b2	200.10.10.64/28	200.10.10.0100/28	255.255.255.240	200.10.10.65	200.10.10.66	200.10.10.73	200.10.10.74	200.10.10.78
Admin	S2.1-b2	200.10.10.48/28	200.10.10.0011/28	255.255.255.240	200.10.10.49	200.10.10.50	200.10.10.55	200.10.10.56	200.10.10.62
	S2.1-b3-01					200.10.10.57	200.10.10.60	200.10.10.61	
Admin	S2.1-b2	200.10.10.32/28	200.10.10.0010/28	255.255.255.240	200.10.10.33	200.10.10.34	200.10.10.39	200.10.10.40	200.10.10.46
	S2.1-b3-02					200.10.10.41	200.10.10.44	200.10.10.45	
Admin	S2.1-b4-01	200.10.10.24/29	200.10.10.00011/29	255.255.255.248	200.10.10.25	200.10.10.26	200.10.10.27	200.10.10.28	
	S2.1-b4-02						200.10.10.29	200.10.10.30	
Admin	S2.1-b4-04	200.10.10.16/29	200.10.10.00010/29	255.255.255.248	200.10.10.17	200.10.10.18	200.10.10.21	200.10.10.22	
Admin	S2.1-b5-02	200.10.10.8/29	200.10.10.00001/29	255.255.255.248	200.10.10.9	200.10.10.10		200.10.10.11	200.10.10.14
	S2.1-b6-02						200.10.10.12	200.10.10.13	

Table 3-4. Subnet assignment for supernet 200.10.10.128/25

Department	**Block S2.2**	**Net#Subnet Bits**	**Binary Rep**	**Subnet Mask**	**Router Address**	**First Host**	**Last Host**	**Printer**	**DHCP Server**
Acad	S2.2-b2	200.10.10.208/28	200.10.10.1101/28	255.255.255.240	200.10.10.209	200.10.10.210	200.10.10.221	200.10.10.222	
Acad	S2.2-b2	200.10.10.192/28	200.10.10.1100/28	255.255.255.240	200.10.10.193	200.10.10.194	200.10.10.205	200.10.10.206	
Admin	S2.2-b2	200.10.10.168/29	200.10.10.10101/29	255.255.255.248	200.10.10.169	200.10.10.170	200.10.10.172	200.10.10.173	200.10.10.174
Admin	S2.2-b3-04	200.10.10.160/29	200.10.10.10100/29	255.255.255.248	200.10.10.161	200.10.10.162	200.10.10.163	200.10.10.164	
	S2.2-b3-07						200.10.10.165	200.10.10.166	
Admin	S2.2-b3-06	200.10.10.152/29	200.10.10.10011/29	255.255.255.248	200.10.10.153	200.10.10.154	200.10.10.155	200.10.10.156	
	S2.2-b3-08						200.10.10.157	200.10.10.158	
Admin	S2.2-b4-02	200.10.10.144/29	200.10.10.10010/29	255.255.255.248	200.10.10.145	200.10.10.146	200.10.10.147	200.10.10.148	
	S2.2-b4-03						200.10.10.149	200.10.10.150	
Admin	S2.2-b4-04	200.10.10.136/29	200.10.10.10001/29	255.255.255.248	200.10.10.137	200.10.10.138	200.10.10.141	200.10.10.142	
Admin	S2.2-b5-02	200.10.10.128/29	200.10.10.10000/29	255.255.255.248	200.10.10.129	200.10.10.130	200.10.10.131	200.10.10.132	
	S2.2-b6-02						200.10.10.133	200.10.10.134	

Table 3-5. Subnet assignment for supernet 200.10.11.128/25

Location	RS	Network: 200.10.11						
Block S2.1	**Net#Subnet Bits**	**Binary Rep**	**Subnet Mask**	**Router Address**	**First Host**	**Last Host**	**Printer**	**DHCP Server**
S2.1-b3-01	200.10.11.128/27	200.10.11.100/27	255.255.255.224	200.10.11.129	200.10.11.130	200.10.11.139	200.10.11.140	200.10.11.158
S2.1-b4-01					200.10.11.141	200.10.11.155	200.10.11.156	
S2.1-b3-01	200.10.11.160/27	200.10.11.101/27	255.255.255.224	200.10.11.161	200.10.11.162	200.10.11.171	200.10.11.172	200.10.11.190
S2.1-b4-02					200.10.11.173	200.10.11.187	200.10.11.188	
S2.1-b3-02	200.10.11.192/27	200.10.11.110/27	255.255.255.224	200.10.11.193	200.10.11.194	200.10.11.199	200.10.11.200	200.10.11.222
S2.1-b4-04					200.10.11.201	200.10.11.220	200.10.11.221	

Table 3-6. Subnet assignment for supernet 200.10.11.0/25

Block S2.2	**Net#Subnet Bits**	**Binary Rep**	**Subnet Mask**	**Router Address**	**First Host**	**Last Host**	**Printer**	**DHCP Server**
S2.2-b3-03	200.10.11.16/28	200.10.11.0001/28	255.255.255.240	200.10.11.17	200.10.11.18	200.10.11.22	200.10.11.23	
S2.2-b3-04					200.10.11.24	200.10.11.29	200.10.11.30	
S2.2-b3-07	200.10.11.32/28	200.10.11.0010/28	255.255.255.240	200.10.11.33	200.10.11.34	200.10.11.45	200.10.11.46	
S2.2-b4-02	200.10.11.48/28	200.10.11.0011/28	255.255.255.240	200.10.11.49	200.10.11.50	200.10.11.61	200.10.11.62	
S2.2-b3-06	200.10.11.64/27	200.10.11.010/27	255.255.255.224	200.10.11.65	200.10.11.66	200.10.11.85	200.10.11.86	200.10.11.94
S2.2-b3-08					200.10.11.87	200.10.11.92	200.10.11.93	
S2.2-b4-03	200.10.11.96/27	200.10.11.011/27	255.255.255.224	200.10.11.97	200.10.11.98	200.10.11.112	200.10.11.113	200.10.11.126
S2.2-b4-04					200.10.11.114	200.10.11.123	200.10.11.124	

Table 3-7. Subnet assignment for supernet 200.10.12.0/23

Lab Name	**Block S2.1**	**Net#Subnet Bits**	**Binary Rep**	**Subnet Mask**	**Router Address**	**First Host**	**Last Host**	**Printer**	**Server**	**Supernet**
Integrated Circuits & Systems	S2.1-b3-01	200.10.12.128/27	200.10.12.100/27	255.255.255.224	200.10.12.129	200.10.12.130	200.10.12.157	200.10.12.158		
		200.10.12.160/27	200.10.12.101/27	255.255.255.224	200.10.12.161	200.10.12.162	200.10.12.189	200.10.12.190		**200.10.12.128 / 26**
	Local Server	200.10.12.244/30	200.10.12.111101/30	255.255.255.252	200.10.12.245				200.10.12.246	
Intelligent Robotics	S2.1-b4-01	200.10.12.96/27	200.10.12.011/27	255.255.255.224	200.10.12.97	200.10.12.98	200.10.12.123	200.10.12.125	200.10.12.126	**200.10.12.96 / 27**
Biomedical Instrumentation	S2.1-b4-02	200.10.12.64/28	200.10.12.0100/28	255.255.255.240	200.10.12.65	200.10.12.66	200.10.12.75	200.10.12.78		
		200.10.12.80/28	200.10.12.0101/28	255.255.255.240	200.10.12.81	200.10.12.82	200.10.12.91	200.10.12.94		**200.10.12.64 / 27**
	Local Server	200.10.12.8/30	200.10.12.000010/30	255.255.255.252	200.10.12.9				200.10.12.10	
Infocomm Research	S2.1-b4-04	200.10.12.192/27	200.10.12.110/27	255.255.255.224	200.10.12.193	200.10.12.194	200.10.12.221	200.10.12.222		
		200.10.12.224/28	200.10.12.1110/28	255.255.255.240	200.10.12.225	200.10.12.226	200.10.12.237	200.10.12.238		**200.10.12.192 / 26**
	Local Server	200.10.12.240/30	200.10.12.111100/30	255.255.255.252	200.10.12.241				200.10.12.242	
Sensors & Actuators I	S2.1-b5-02	200.10.12.16/28	200.10.12.0001/28	255.255.255.240	200.10.12.17	200.10.12.18	200.10.12.23	200.10.12.30		
Sensors & Actuators I	S2.1-b6-02	200.10.12.32/28	200.10.12.0010/28	255.255.255.240	200.10.12.33	200.10.12.34	200.10.12.39	200.10.12.46		**200.10.12.0 / 26**
	Local Server	200.10.12.12/30	200.10.12.000011/30	255.255.255.252	200.10.12.13				200.10.12.14	
Photonics Training	S2.1-b6-01	200.10.12.48/28	200.10.12.0011/28	255.255.255.240	200.10.12.49	200.10.12.50	200.10.12.57	200.10.12.61	200.10.12.62	**200.10.12.48 / 28**

Table 3-8. Subnet assignment for supernet 200.10.14.0/24

Lab Name	**Block S2.2**	**Net#Subnet Bits**	**Binary Rep**	**Subnet Mask**	**Router Address**	**First Host**	**Last Host**	**Printer**	**Server**	**Supernet**
Satellite Engineering	S2.2-b3-04	200.10.14.192/27	200.10.14.110/27	255.255.255.224	200.10.14.193	200.10.14.194	200.10.14.221	200.10.14.222		**200.10.14.192 / 27**
	Local Server	200.10.14.8/30	200.10.14.000010/30	255.255.255.252	200.10.14.9				200.10.14.10	
Media Technology	S2.2-b4-02	200.10.14.160/27	200.10.14.101/27	255.255.255.224	200.10.14.161	200.10.14.162	200.10.14.185	200.10.14.189	200.10.14.190	**200.10.14.160 / 27**
Process Instrumentation	S2.2-b4-03	200.10.14.32/28	200.10.14.0010/28	255.255.255.240	200.10.14.33	200.10.14.34	200.10.14.45	200.10.14.46		
		200.10.14.16/29	200.10.14.00010/29	255.255.255.248	200.10.14.17	200.10.14.18	200.10.14.21	200.10.14.22		**200.10.14.0 / 26**
	Local Server	200.10.14.12/30	200.10.14.000011/30	255.255.255.252	200.10.14.13				200.10.14.14	
Software Engineering A	S2.2-b4-04	200.10.14.128/27	200.10.14.100/27	255.255.255.224	200.10.14.129	200.10.14.130	200.10.14.154	200.10.14.157	200.10.14.158	**200.10.14.128 / 27**
Software Engineering B	S2.2-b4-04	200.10.14.96/27	200.10.14.011/27	255.255.255.224	200.10.14.97	200.10.14.98	200.10.14.122	200.10.14.125	200.10.14.126	**200.10.14.96 / 27**
Microfabrication Facilities	S2.2-b5-02	200.10.14.64/28	200.10.14.0100/28	255.255.255.240	200.10.14.65	200.10.14.66	200.10.14.77	200.10.14.78		
Microfabrication Facilities	S2.2-b6-02	200.10.14.48/28	200.10.14.0011/28	255.255.255.240	200.10.14.49	200.10.14.50	200.10.14.61	200.10.14.62		**200.10.14.0 / 25**
	Local Server	200.10.14.4/30	200.10.14.000001/30	255.255.255.252	200.10.14.5				200.10.14.6	

Table 3-9. Subnet assignment for Acad+Admin Serial Links

Network: 200.10.10					
Link	**Net#Subnet Bits**	**Binary Rep**	**Subnet Mask**	**Router Address**	**Second Host**
Workgroup Router to Campus Backbone	200.10.10.4/30	200.10.10.000001/30	255.255.255.252	200.10.10.5	200.10.10.6
Workgroup Router to Campus Backbone	200.10.10.224/30	200.10.10.111000/30	255.255.255.252	200.10.10.225	200.10.10.226
Acad & Admin Shared Server	200.10.10.228/30	200.10.10.111001/30	255.255.255.252	200.10.10.229	200.10.10.230
Acad Server	200.10.10.232/30	200.10.10.111010/30	255.255.255.252	200.10.10.233	200.10.10.234
Admin Server	200.10.10.236/30	200.10.10.111011/30	255.255.255.252	200.10.10.237	200.10.10.238
Workgroup Router to S2.1 Router	200.10.10.240/30	200.10.10.111100/30	255.255.255.252	200.10.10.241	200.10.10.242
Workgroup Router to S2.2 Router	200.10.10.244/30	200.10.10.111101/30	255.255.255.252	200.10.10.245	200.10.10.246
S2.1 Router to S2.2 Router	200.10.10.248/30	200.10.10.111110/30	255.255.255.252	200.10.10.249	200.10.10.250
Extra Space for the following subnets:					
	Net#Subnet Bits	**Binary Rep**	**Subnet Mask**	**Start Address**	**End Address**
	200.10.10.80/28	200.10.10.0101/28	255.255.255.240	200.10.10.81	200.10.10.94
	200.10.10.176/28	200.10.10.1011/28	255.255.255.240	200.10.10.177	200.10.10.190

Table 3-10. Subnet assignment for RS Serial Links

Network: 200.10.11					
Link	**Net#Subnet Bits**	**Binary Rep**	**Subnet Mask**	**Router Address**	**Second Host**
Workgroup Router to Campus Backbone Router	200.10.11.4/30	200.10.11.000001/30	255.255.255.252	200.10.11.5	200.10.11.6
Workgroup Router to Campus Backbone Router	200.10.11.248/30	200.10.11.111110/30	255.255.255.252	200.10.11.249	200.10.11.250
RS Server	200.10.11.244/30	200.10.11.111101/30	255.255.255.252	200.10.11.245	200.10.11.246
Workgroup Router to S2.1 Router	200.10.11.232/30	200.10.11.111010/30	255.255.255.252	200.10.11.233	200.10.11.234
Workgroup Router to S2.2 Router	200.10.11.236/30	200.10.11.111011/30	255.255.255.252	200.10.11.237	200.10.11.238
S2.1 Router to S2.2 Router	200.10.11.240/30	200.10.11.111100/30	255.255.255.252	200.10.11.241	200.10.11.242
Extra Space for the following subnets:					
	Net#Subnet Bits	**Binary Rep**	**Subnet Mask**	**Start Address**	**End Address**
	200.10.11.8/29	200.10.11.00001/29	255.255.255.248	200.10.11.9	200.10.11.14
	200.10.11.224/29	200.10.11.11100/29	255.255.255.248	200.10.11.225	200.10.11.230

Table 3-11. Subnet assignment for Lab Serial Links

Lab S2.1	Network: 200.10.12				
Link	**Net#Subnet Bits**	**Binary Rep**	**Subnet Mask**	**Router Address**	**Second Host**
Workgroup Router to Campus Backbone Router	200.10.12.4/30	200.10.12.000001/30	255.255.255.252	200.10.12.5	200.10.12.6
Workgroup Router to Campus Backbone Router	200.10.12.248/30	200.10.12.111110/30	255.255.255.252	200.10.12.249	200.10.12.250
Lab S2.1	**Network: 200.10.13 (Exhausted all address spaces in 200.10.12)**				
Workgroup Router to Integrated Circuits & Systems	200.10.13.4/30	200.10.13.000001/30	255.255.255.252	200.10.13.5	200.10.13.6
Workgroup Router to Biomedical Instrumentation	200.10.13.240/30	200.10.13.111100/30	255.255.255.252	200.10.13.241	200.10.13.242
Workgroup Router to Infocomm Research	200.10.13.244/30	200.10.13.111101/30	255.255.255.252	200.10.13.245	200.10.13.246
Workgroup Router to Sensors & Actuators	200.10.13.248/30	200.10.13.111110/30	255.255.255.252	200.10.13.249	200.10.13.250
Lab S2.2	**Network: 200.10.14**				
Link	**Net#Subnet Bits**	**Binary Rep**	**Subnet Mask**	**Router Address**	**Second Host**
Workgroup Router to Campus Backbone Router	200.10.14.224/30	200.10.14.111000/30	255.255.255.252	200.10.14.225	200.10.14.226
Workgroup Router to Campus Backbone Router	200.10.14.228/30	200.10.14.111001/30	255.255.255.252	200.10.14.229	200.10.14.230
Workgroup Router to Satellite Engineering	200.10.14.240/30	200.10.14.111100/30	255.255.255.252	200.10.14.241	200.10.14.242
Workgroup Router to Process Instrumentation	200.10.14.244/30	200.10.14.111101/30	255.255.255.252	200.10.14.245	200.10.14.246
Workgroup Router to Microfabrication Facilities	200.10.14.248/30	200.10.14.111110/30	255.255.255.252	200.10.14.249	200.10.14.250
Extra Space for the following subnets in Lab S2.2:	**Network: 200.10.14**				
	Net#Subnet Bits	**Binary Rep**	**Subnet Mask**	**Start Address**	**End Address**
	200.10.14.80/28	200.10.14.0101/28	255.255.255.240	200.10.14.81	200.10.14.94
	200.10.14.232/29	200.10.14.11101/29	255.255.255.248	200.10.14.233	200.10.14.238
	200.10.14.24/29	200.10.14.00011/29	255.255.255.248	200.10.14.25	200.10.14.30

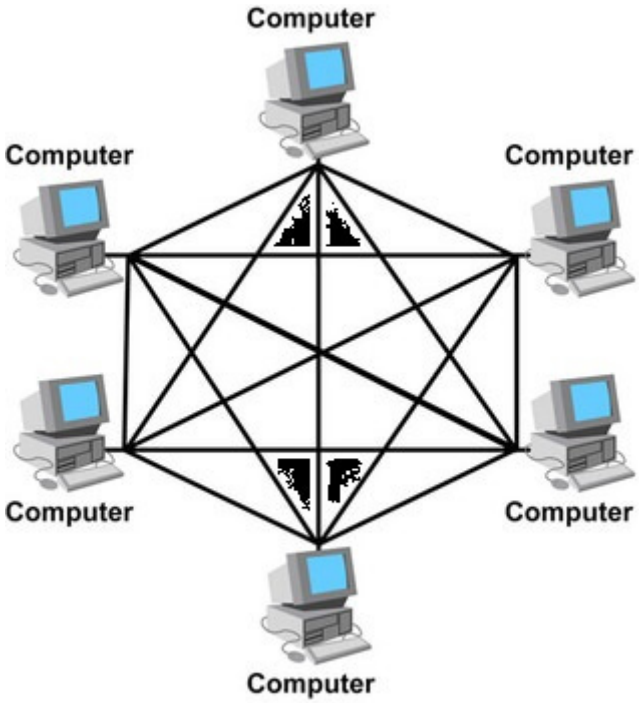
Table 3-12. Subnet assignment for servers

Network: 200.10.9						
Link	**Net#Subnet Bits**	**Binary Rep**	**Subnet Mask**	**Router Name**	**Router Address**	**Second Host**
Serial link between 2 Campus Backbone Routers	200.10.9.4/30	200.10.9.000001/30	255.255.255.252		200.10.9.5	200.10.9.6
Enterprise SQL Server	200.10.9.240/30	200.10.9.111100/30	255.255.255.252	Core Router 1	200.10.9.241	200.10.9.242
Email Server	200.10.9.244/30	200.10.9.111101/30	255.255.255.252	Core Router 1	200.10.9.245	200.10.9.246
Enterprise Web Server for HTTP Service	200.10.9.248/30	200.10.9.111110/30	255.255.255.252	Core Router 2	200.10.9.249	200.10.9.250
External Host	195.168.9.248/30	195.168.9.111110/30	255.255.255.252	Core Router 2	195.168.9.249	195.168.9.250

Chapter 4. Multi Layered network design

Network topology describes how nodes, or end points, linked to the network (such as PCs, routers, and printers), are connected to one another. Topologies that are frequently used include star, bus, ring, tree, mesh, etc. Core and Distribution layers in this project use "Mesh topology," whereas the Access layer uses "Tree topology."

With a mesh network structure, each node relays data for the network and the idea of routes is crucial. It is a cheap option that offers redundancy in the event of a physical failure, like a LAN cable breaking. Redundancy boosts the network's robustness and reliability since packets can take numerous routes to go from source to destination. Moreover, as the Core layer is the highest level, it should have more redundancy than a lower level layer in order to reduce the effects of a physical failure.



In terms of tree topology, a physical failure would prevent the child node from contacting its parent node or nodes if one or more were involved. The Tree architecture nevertheless allows for network expansion in the future due to its straightforward implementation.

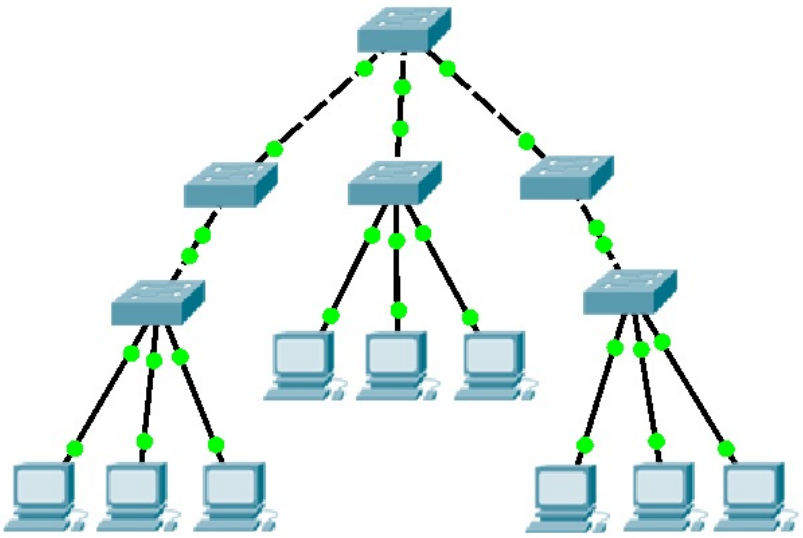


Fig 4-1. Tree topology

4.1 Hierarchical Layered Design

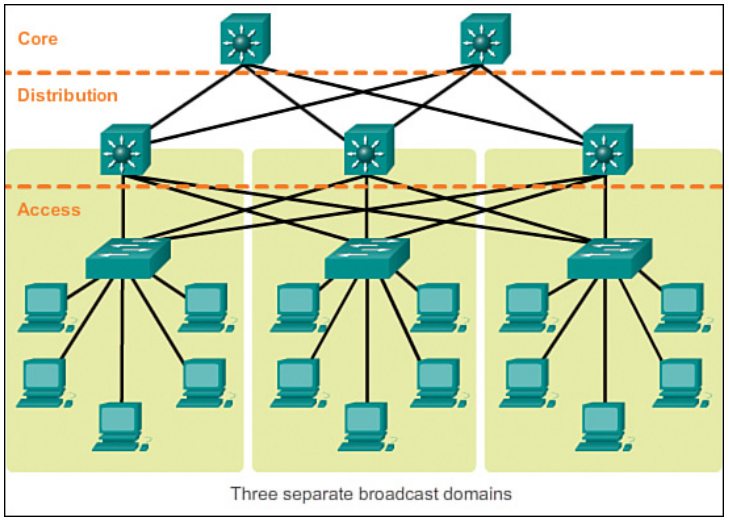


Fig 4-2. Hierarchical Layered Design

In this project, we are introducing a Hierarchical Network Design to create a flexible, cost-effective, and scalable network architecture. One of the key advantages of this approach is the ability to quickly identify and resolve potential failure points, ensuring high availability and performance for the entire network.

The Hierarchical Network Design is organized into three distinct layers, each with its specific functions and responsibilities:

1. Core layer: focuses network traffic for remote access and access control
2. Distribution layer: distributes traffic from the Access layer equitably among local network segments by compiling routes.
3. Access layer: expands the requirements for local network segments and end-user physical locations.

4.1.1 Core Layer

The core layer, also known as the backbone layer, is a critical component in the hierarchical network design model. The primary purpose of the core layer is to provide high-speed, reliable, and scalable data transport between different parts of the network, such as between distribution layers, data centers, or remote sites.

As shown in Fig. 1, our model has a dual-router core layer. The core layer is connected to all the campus workgroups as well as the core servers (SQL, Email and HTTP) for the campus network.

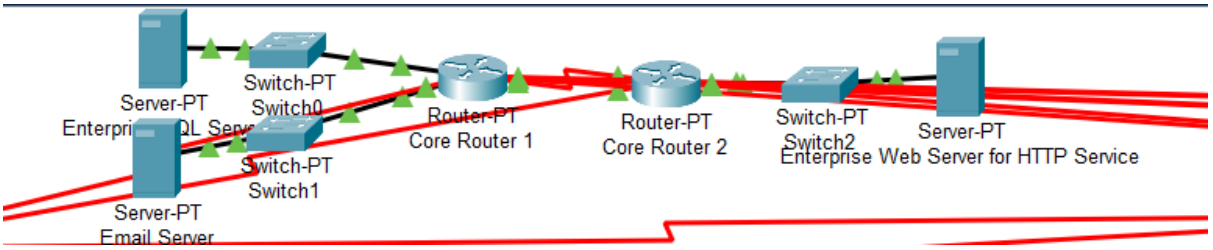


Fig 4-3. Core layer routers

This design of the core layer offers the following advantages:

1. Redundancy: One of the primary benefits of using two core routers in the core layer is redundancy. If one of the routers fails, the other router can take over and continue to provide connectivity, ensuring that the network remains operational and minimizing downtime.
2. Load balancing: With two routers in the core layer, traffic can be distributed evenly between them, which helps prevent any single router from becoming a bottleneck. This load balancing can enhance overall network performance and provide more efficient use of available bandwidth.
3. Scalability: As the network grows, having two core routers in the core layer can help maintain high-performance levels. The addition of new distribution or access layer devices can be handled more easily by the dual-router setup, allowing the network to scale while maintaining efficient and reliable connectivity.
4. Flexibility: A dual-router core layer offers flexibility in terms of routing and traffic management. Network administrators can implement various routing protocols and configurations on each router to optimize traffic flow, control traffic patterns, and prioritize specific types of traffic based on the organization's requirements.
5. Cost-effective solution: In some cases, using two core routers can be a more budget-friendly option compared to investing in a single high-performance router. By

leveraging the capabilities of two routers, organizations can achieve similar levels of performance and redundancy at a lower overall cost, making it an attractive choice for organizations with budget constraints.

4.1.2 Distribution Layer

The distribution layer acts as the intermediary between the core and access layers. It is responsible for aggregating and routing traffic from the access layer and distributing it evenly among the local network segments. This layer also manages routing updates, implements policies, and provides redundancy and load balancing to enhance network resiliency. Additionally, the distribution layer serves as the primary point for implementing security measures, such as access control lists (ACLs) and firewalls, to protect the network from unauthorized access and potential threats.

For different work groups, different sets of distribution routers are used. Fig 2 shows the layout of the distribution layer for the Acad and Admin combined workgroup. Three interconnecting routers are used in the distribution layer of the Acad and Admin workgroup. This design takes into consideration the redundancy of the network, and provides a better segmentation for the two groups separated in two buildings (S1 and S2).

Fig 4-4. Distribution Layer design for Acad & Admin

The distribution layer of the RS workgroup shares a similar design, as shown in Fig 3.

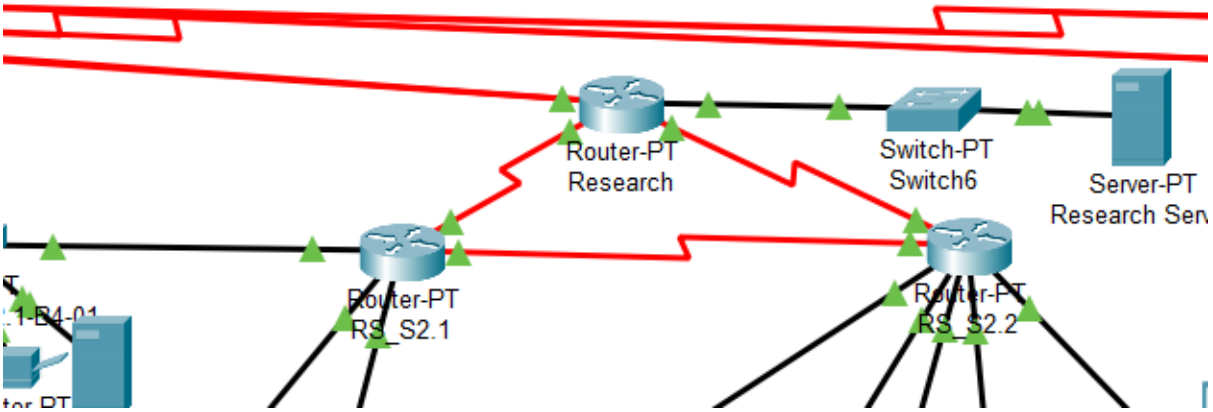


Fig 4-5. Distribution Layer design for RS

The distribution layer for the labs are however separated. The two routers that connect to the lab users in the two buildings are directly connected to the core layer individually. This is to provide a better segmentation between the labs, as they are supposed to be isolated.

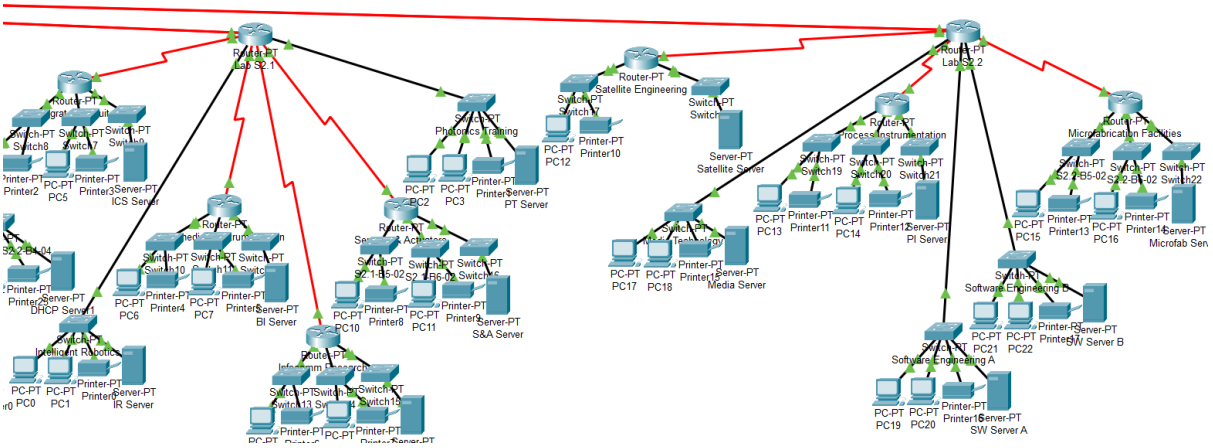


Fig 4-6. Distribution Layer design for labs

4.1.3 Access Layer

The access layer is the point of entry for end-users and devices into the network. It focuses on meeting the connectivity requirements of local network segments and provides physical connections for end-user devices, such as computers, printers, and IP phones. This layer is responsible for implementing features such as port security, VLANs, and Quality of Service

(QoS) policies to ensure secure, organized, and efficient communication between end-users and the network infrastructure.

In our design, the access layer is mainly made up of the switches which provide network access to all the hosts and end devices. The switches are separated based on the work group and subnet groups they are assigned to. A total of 55 switches are used in the access layer of our design.

4.2 Server Placement

In this project, various servers are required to fulfill different functions within the network. These servers are strategically placed within the network to optimize performance, accessibility, and minimize redundant network traffic.

4.2.1 Campus Wide Services

Three core campus network servers (SQL, Email, and HTTP) provide essential campus wide services to the entire campus network. These servers are connected directly to the two core routers via a switch, enabling all workgroups to access these services without needing to traverse the router of another workgroup. This placement reduces redundant network traffic and ensures efficient and reliable access to critical services.

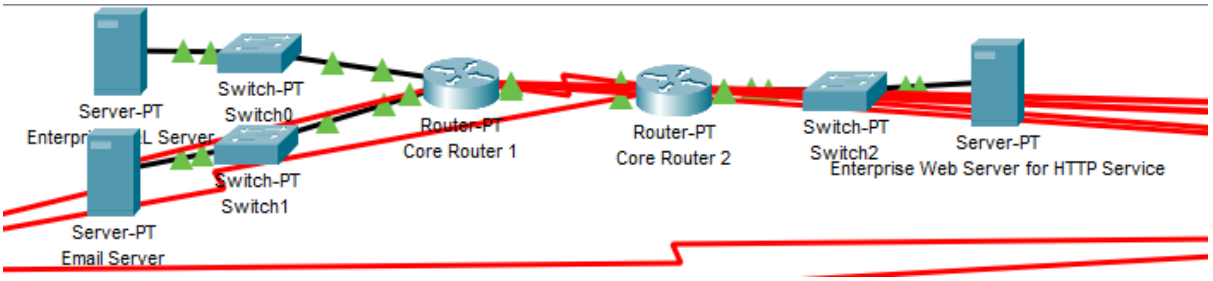


Fig 4-7. Placement for Enterprise SQL, Email and HTTP server

4.2.2 Workgroup-Specific Servers

Servers that cater to the needs of specific workgroups are connected to the distribution layer routers of the corresponding workgroups. This arrangement ensures that these servers are easily accessible to their target users while maintaining appropriate network segmentation.

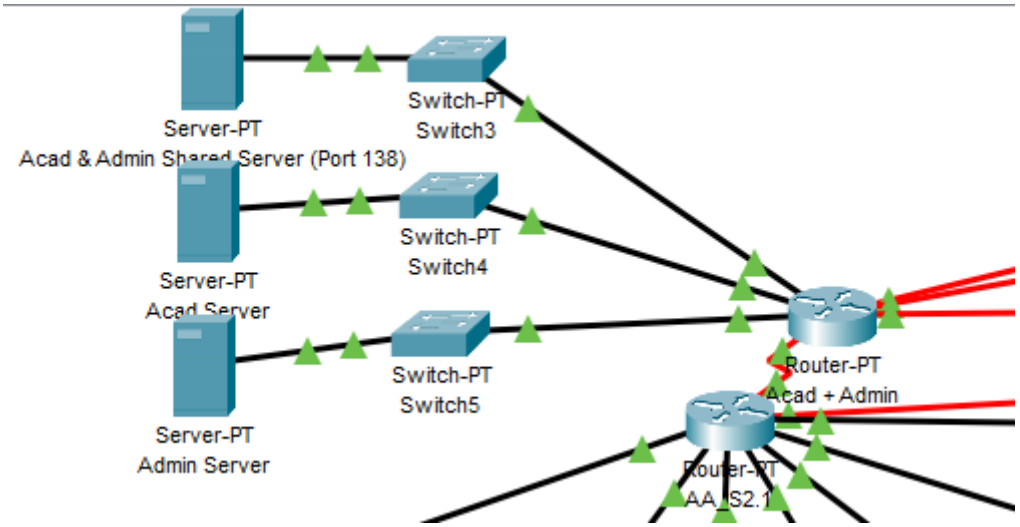


Fig 4-8. Placement of Acad and Admin servers

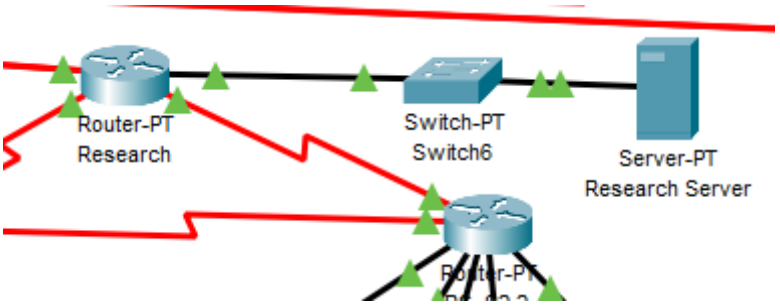


Fig 4-9. Placement of RS server

4.2.3 DHCP Servers

Dynamic Host Configuration Protocol (DHCP) servers are employed whenever there are excess IPs available in a subnet. These servers are placed under the switch for the respective subnet, allowing for efficient IP address assignment and management within the network segment. This placement also contributes to overall network organization and simplifies administration tasks.

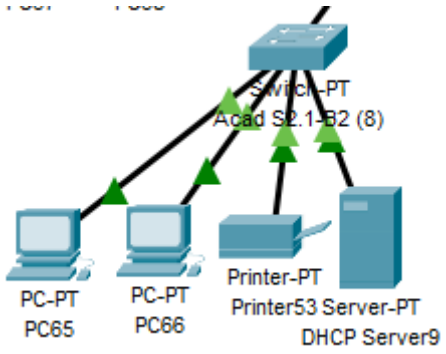


Fig 4-10. Placement of a typical DHCP server

4.2.4 Lab Servers

Lab servers are treated similarly to DHCP servers in terms of placement. Each lab server should only be accessible from its specific lab, ensuring a secure and controlled environment for lab users. Placing the lab servers under the switches for their respective subnets allows for easy access while maintaining the necessary separation from other network segments. However, for some lab groups with insufficient IPs in the subnet, a /30 subnet is assigned to the server and placed under the same router as the respective lab work group.

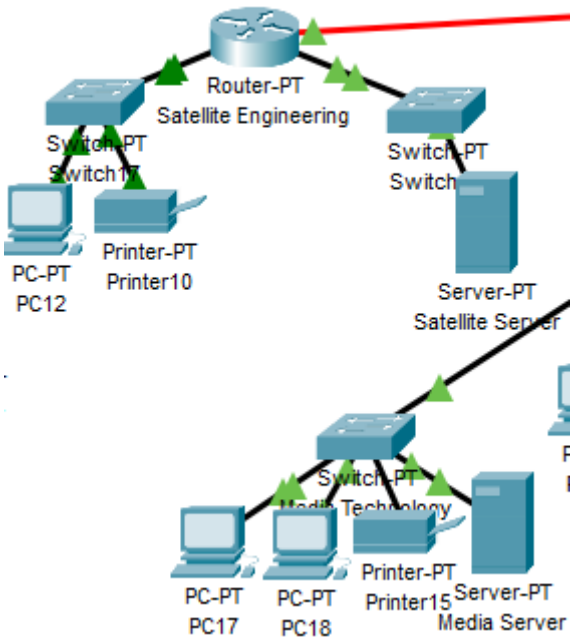


Fig 4-11. Placement of lab servers

Chapter 5. Network security requirements

The network security architecture is accomplished using access control lists (ACLs). ACL usage controls access to shared servers and restricts/enables communication between user groups. ACLs employ a series of commands to regulate inter-user and inter-workgroup communication.

There are two types of ACLs used in networking to control access to network resources, namely Standard ACLs and Extended ACLs.

Standard ACLs:

- Standard ACLs are numbered between 1-99 and 1300-1999. They are used to filter traffic solely based on the source IP address of traffic.
- Standard ACLs are utilized to limit access to particular networks or hosts by restricting traffic from a specific source
- They can only be applied on the interface nearest to source of traffic
- They are less powerful as compared to extended ACLs but simpler and much faster.

Extended ACLs:

- Extended ACLs are numbered within 100-199 and 2000-2699.
- Extended ACLs are used to filter traffic based on multiple criteria such as source, destination IP addresses, ports and protocols.
- They are more flexible compared to standard ACLs but also more complex hence taking longer to process.
- They can be applied on any interface in the path of traffic.
- Extended ACLs are used to control access to particular network addresses like FTP and HTTP by either denying or permitting traffic on the basis of service port numbers.

The movement of network traffic into and out of a network is known as traffic flow. In network security, the direction of traffic flow is vital as it aids in determining placement of network security devices to filter and monitor incoming and outgoing traffic.

IN: Network traffic that is flowing into a network from external sources. For example, when traffic is coming through the port into the router

OUT: Network traffic that is flowing out of a network to other destinations. For example, when traffic has gone through the router and leaves the interface.

A basic template for extended ACL commands is as follows:

access-list <ACL_number> {permit | deny} <protocol> <source_IP> [wildcard_mask] <destination_IP> [wildcard_mask] [operator [port]]

- `<ACL_number>`: A number from 1 to 99 or 1300 to 1999, representing the standard ACL identifier.
- `permit` or `deny`: The action to take (allow or block) for traffic that matches the specified criteria.
- `<source_IP>`: The source IP address to match against.
- `[wildcard_mask]`: An optional wildcard mask that represents the range of source IP addresses to match.
- `<ACL_number>`: A number from 100 to 199 or 2000 to 2699, representing the extended ACL identifier.
- `permit` or `deny`: The action to take (allow or block) for traffic that matches the specified criteria.
- `<protocol>`: The protocol to match, such as IP, TCP, UDP, ICMP, or others.

- `<source_IP>` and `<destination_IP>`: The source and destination IP addresses to match against.
- `[wildcard_mask]`: An optional wildcard mask that represents the range of source and destination IP addresses to match.
- `[operator]`: An optional operator, such as `eq` (equal), `gt` (greater than), or `lt` (less than), to further specify the port criteria.
- `[port]`: An optional port number or well-known service name (e.g., www, ftp, ssh) to match against.

In this project, several ACLs are applied to meet various security requirements.

1. Lab users are not allowed to access the SQL server, email server, other labs or other work groups.
2. Only Acad and Admin workgroups can access a shared server on Port 138 for data sharing.
3. Only Acad and Admin workgroups can access the Admin server.
4. The Acad server and RS server allow only access from their respective workgroups
5. Only RS students can establish FTP connection with Acad server through port 21.
6. All external access into the campus network is denied, except for the access to the enterprise web server for HTTP service.

Table 5-1 shows the ACL applied to achieve the requirements.

Table 5-1. ACL commands to deny external access into the campus networks

Router	ACL Statement	Port	Config	Purpose
Acad + Admin Router	access-list 1 permit 200.10.8.0 0.0.3.255	Serial 0/0	ip acc 1 in	To deny access from external hosts and laboratory users
		Serial 1/0	ip acc 1 in	
Research Router	access-list 2 permit 200.10.8.0 0.0.3.255	Serial 0/0	ip acc 2 in	To deny access from external hosts and laboratory users
		Serial 1/0	ip acc 2 in	
Lab S2.1	access-list 3 permit host 200.10.9.250	Serial 0/0	ip acc 3 in	To only allow access to and from the enterprise web server for HTTP service
		Serial 1/0	ip acc 3 in	
Lab S2.2	access-list 4 permit host 200.10.9.250	Serial 0/0	ip acc 4 in	To only allow access to and from the enterprise web server for HTTP service
		Serial 1/0	ip acc 4 in	
Lab S2.1	access-list 5 permit host 200.10.9.250	Serial 2/0	ip acc 5 out	To deny access to other laboratory users
		Serial 3/0		To only allow access to and from the enterprise web server for HTTP service
		Serial 4/0		
		Serial 5/0		
		Fast Ethernet 6/0		
		Fast Ethernet 7/0		
Lab S2.2	access-list 6 permit host 200.10.9.250	Serial 2/0	ip acc 6 out	To deny access to other laboratory users
		Serial 3/0		To only allow access to and from the enterprise web server for HTTP service
		Serial 4/0		
		Fast Ethernet 5/0		
		Fast Ethernet 6/0		
		Fast Ethernet 7/0		
Core Router 1	access-list 7 permit 200.10.8.0 0.0.3.255	Fast Ethernet 6/0	ip acc 7 out	To deny access to the Enterrise SQL Server and Email Server from external hosts and laboratory users
		Fast Ethernet 7/0		

Table 5-2. ACL commands to establish FTP connections and server access

Acad/Admin S2.2 Router	access-list 101 permit tcp 200.10.11.0 0.0.0.255 200.10.10.208 0.0.0.15 eq 21	Fast Ethernet 2/0	config	To allow FTP connections between Acad and RS
	access-list 101 deny tcp any 200.10.10.208 0.0.0.15 eq 21		inter fast 2/0	
	access-list 101 permit ip any any		ip acc 101 out	
Acad/Admin S2.2 Router	access-list 102 permit tcp 200.10.11.0 0.0.0.255 200.10.10.192 0.0.0.15 eq 21	Fast Ethernet 3/0	config	
	access-list 102 deny tcp any 200.10.10.192 0.0.0.15 eq 21		inter fast 3/0	
	access-list 102 permit ip any any		ip acc 102 out	
Acad/Admin S2.1 Router	access-list 103 permit tcp 200.10.11.0 0.0.0.255 200.10.10.96 0.0.0.31 eq 21	Fast Ethernet 2/0	config	
	access-list 103 deny tcp any 200.10.10.96 0.0.0.31 eq 21		inter fast 2/0	
	access-list 103 permit ip any any		ip acc 103 out	
Acad/Admin S2.1 Router	access-list 104 permit tcp 200.10.11.0 0.0.0.255 200.10.10.64 0.0.0.15 eq 21	Fast Ethernet 3/0	config	
	access-list 104 deny tcp any 200.10.10.64 0.0.0.15 eq 21		inter fast 3/0	
	access-list 104 permit ip any any		ip acc 104 out	
Acad/Admin Router	access-list 105 permit tcp 200.10.10.0 0.0.0.255 200.10.10.230 0.0.0.0 eq 138	Fast Ethernet 6/0	config	To allow Acad & Admin staff to access a shared server on Port 138 for data sharing
	access-list 105 deny tcp any 200.10.10.230 0.0.0.0 eq 138		inter fast 6/0	
	access-list 105 permit ip 200.10.10.0 0.0.0.255 200.10.10.230 0.0.0.0		ip acc 105 out	
	access-list 8 permit 200.10.10.192 0.0.0.31	Fast Ethernet 7/0	config	To restrict access of the Acad server to Acad users only
	access-list 8 permit 200.10.10.64 0.0.0.15		inter fast 7/0	
	access-list 8 permit 200.10.10.96 0.0.0.31		ip acc 8 out	
	access-list 9 permit 200.10.10.0 0.0.0.255	Fast Ethernet 8/0	ip acc 9 out	To allow Acad & Admin staff to access Admin Server
Research Router	access-list 10 permit 200.10.11.0 0.0.0.255	Fast Ethernet 6/0	ip acc 10 out	To restrict access of the RS server to Acad users only

The services on the Enterprise SQL server, Email Server, and Enterprise Web server for HTTP service were configured according to their functionality. Hence, port numbers in access lists were not specified.

Chapter 6. Simulation and Testing

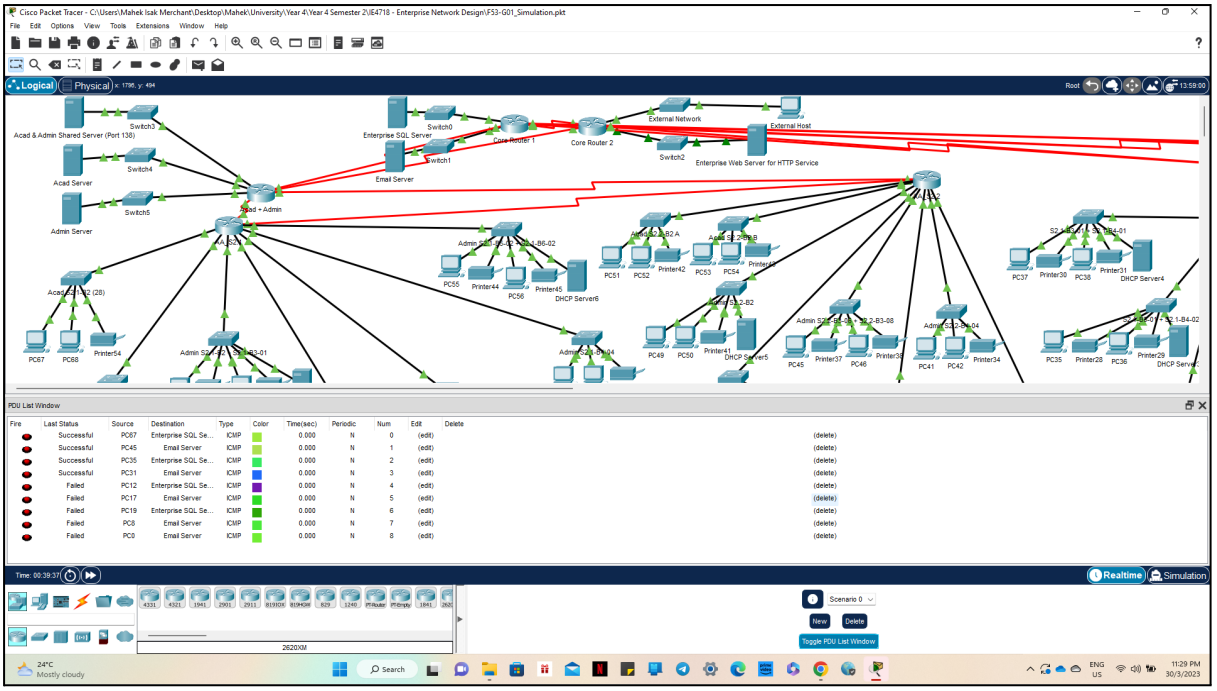
Tests are conducted to evaluate the functionality of the network under different scenarios. Packets are sent from various hosts to different destinations to test if the ACLs and availability of services are functioning as planned.

6.1 Scenario 0

Only lab users should be unable to access the campus SQL and email server. Hence the accessibility of all users to the two servers are tested in this scenario.

Table 6-1. Test 1

Source	Destination	Accessibility
Acad S2.1	SQL/Email server	Allow
Admin S2.2	SQL/Email server	Allow
RS 2.1	SQL/Email server	Allow
RS 2.2	SQL/Email server	Allow
Satellite Engineering Lab	SQL/Email server	Deny
Media Technology Lab	SQL/Email server	Deny
Software Engineering Lab A	SQL/Email server	Deny
Infocomm Research Lab	SQL/Email server	Deny
Intelligent Robotic Lab	SQL/Email server	Deny



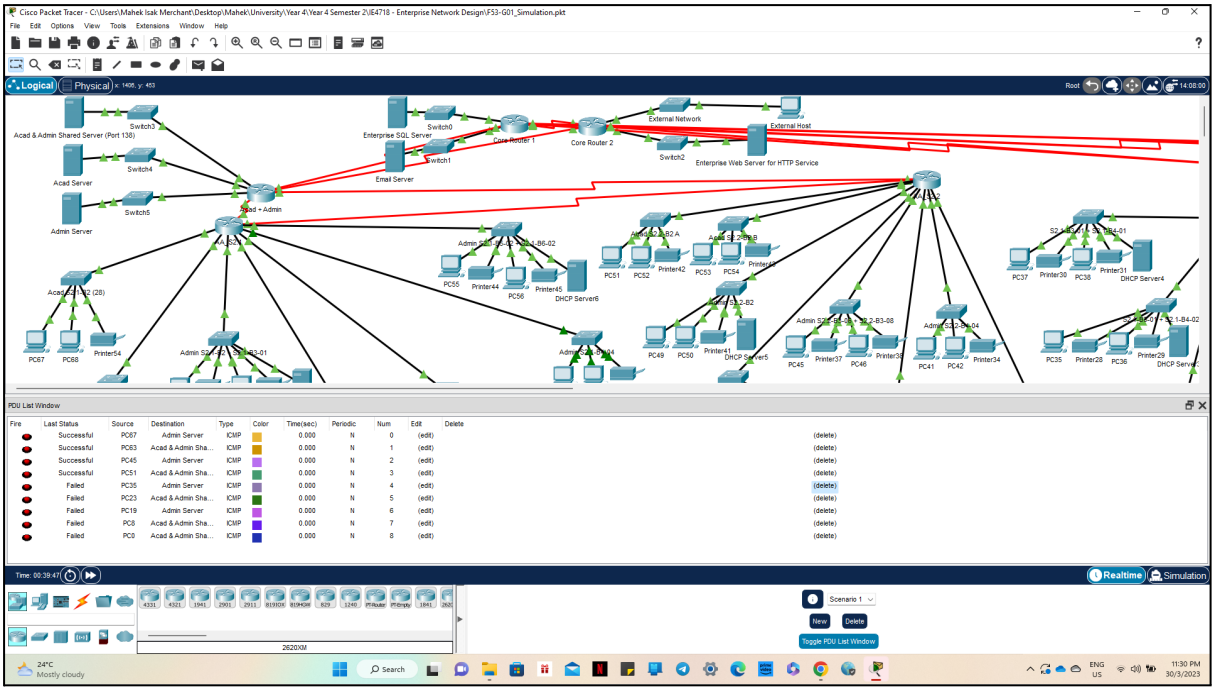
6.2 Scenario 1

Admin server and Acad Admin shared server should be accessible by only Acad and Admin workgroup

Table 6-2. Test 2

Source	Destination	Accessibility
Acad S2.1	Admin Server	Allow
Admin S2.1	Admin/Acad Admin share server	Allow
Admin S2.2	Admin Server	Allow
Acad S2.2	Admin/Acad Admin share server	Allow
RS 2.1	Admin Server	Deny
RS 2.2	Admin/Acad Admin share server	Deny
Software Engineering Lab A	Admin Server	Deny
Infocomm Research Lab	Admin/Acad Admin share	Deny

	server	
Intelligent Robotic Lab	Admin/Acad Admin share server	Deny



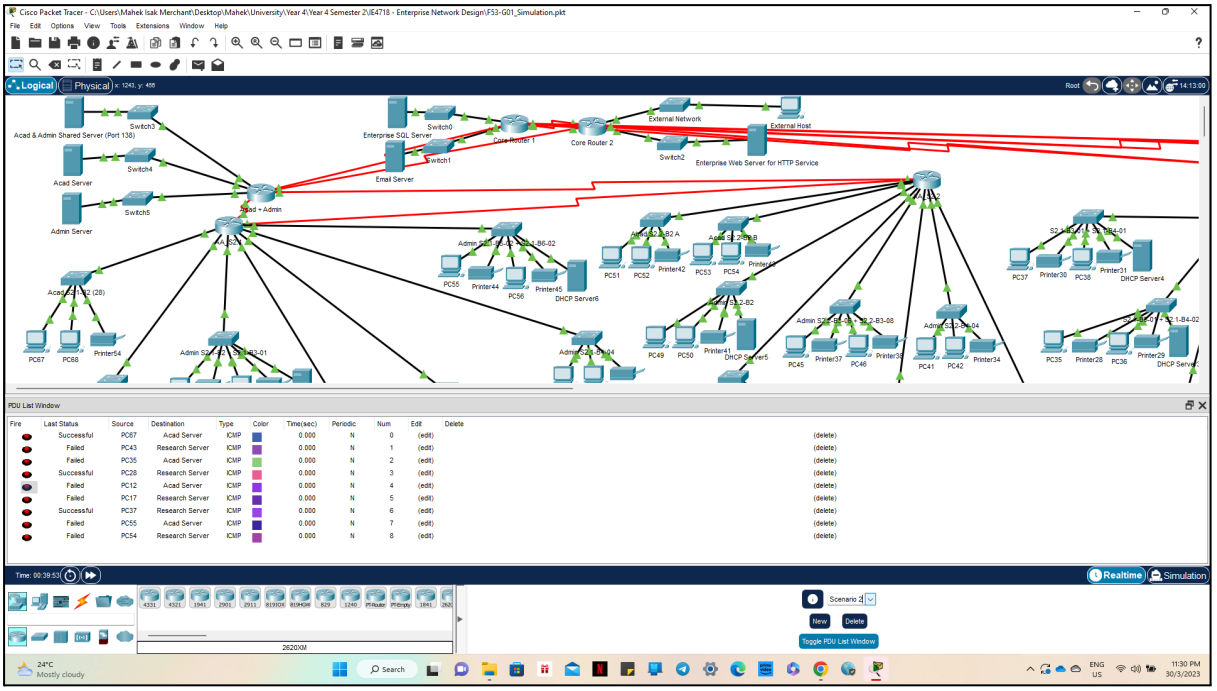
6.3 Scenario 2

The Acad server should only be accessible by an Acad user. The RS server should only be accessible by RS users.

Table 6-3. Test 3

Source	Destination	Accessibility
Acad S2.1	Acad server	Allow
Admin S2.2	RS server	Deny
RS 2.1	Acad server	Deny
RS 2.2	RS server	Allow
Satellite Engineering Lab	Acad server	Deny
Media Technology Lab	RS server	Deny

RS 2.1	RS Server	Allow
Admin S2.1	Acad Server	Deny
Acad S2.2	RS Server	Deny



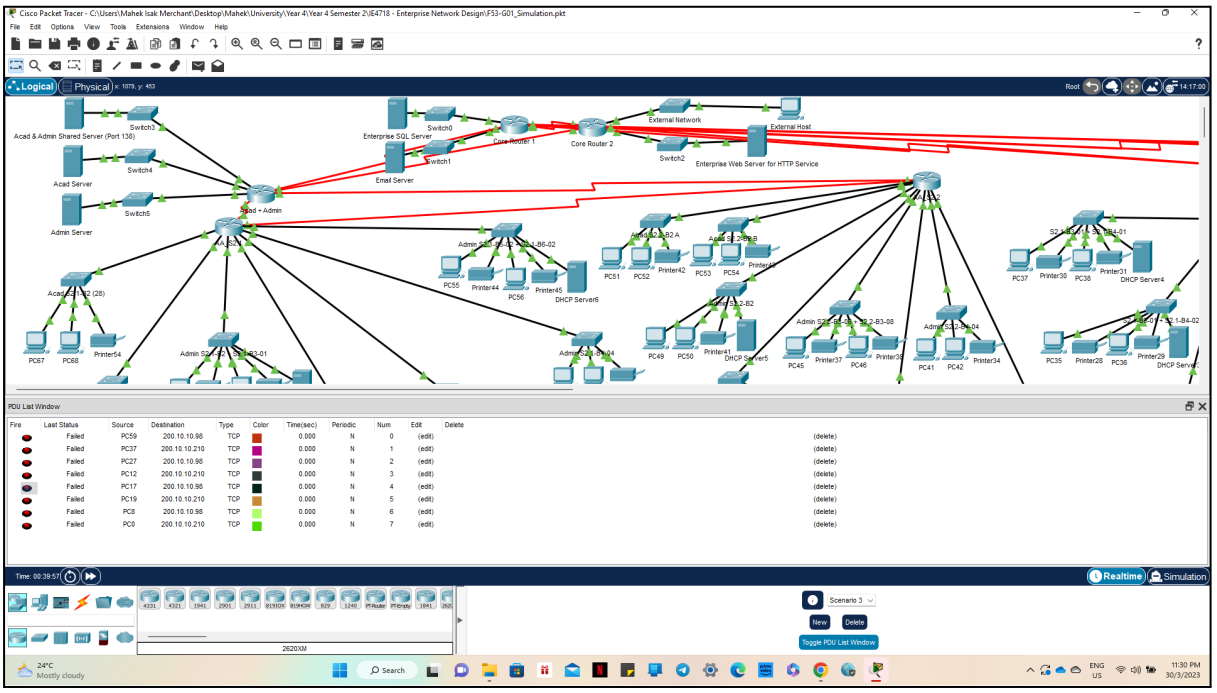
6.4 Scenario 3

Only Research students can establish FTP connections (Port 21) with the Acad staff for file exchange. The displayed simulation status was ‘Failed’ in cases of FTP between RS and Acad as the PCs were not configured to offer FTP service in Packet Tracer. Otherwise, the ACL was successful in blocking FTP requests from Admin and Laboratory users.

Table 6-4. Test 4

Source	Destination (port 21)	Accessibility
Admin S2.1	Acad S2.1	Deny
RS S2.1	Acad S2.2	Allow
RS S2.2	Acad S2.1	Allow

Satellite Engineering Lab	Acad S2.2	Deny
Media Technology Lab	Acad S2.1	Deny
Software Engineering Lab A	Acad S2.2	Deny
Infocomm Research Lab	Acad S2.1	Deny
Intelligent Robotic Lab	Acad S2.2	Deny



6.5 Scenario 4

External IPs should only be allowed to access the HTTP server. The external IP is simulated by attaching another switch to the core router 2. The external switch is attached to a single end user.

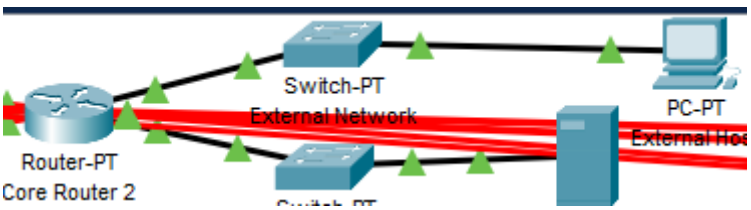
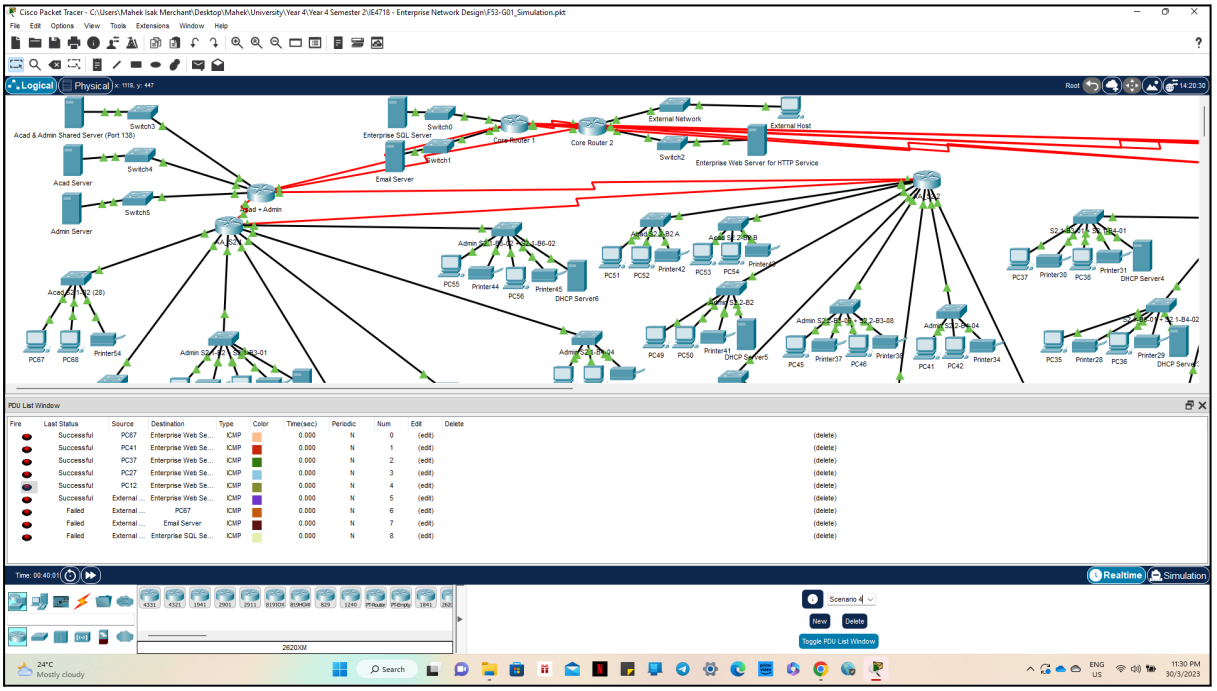


Fig 6-1. External Host

Table 6-5. Test 5

Source	Destination	Accessibility
Acad S2.1	HTTP server	Allow
Admin S2.2	HTTP server	Allow
RS S2.1	HTTP server	Allow
RS S2.2	HTTP server	Allow
Satellite Engineering Lab	HTTP server	Allow
External IP	HTTP server	Allow
External IP	Acad S2.1	Deny
External IP	Email server	Deny
External IP	SQL server	Deny

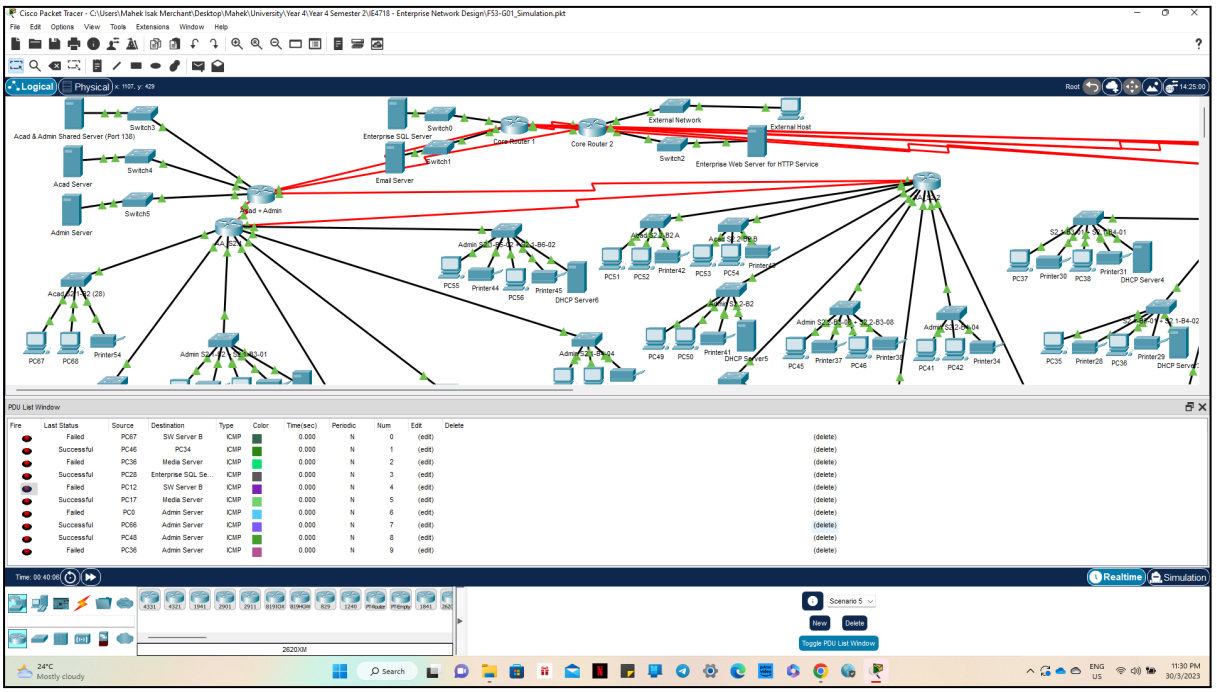


6.6 Scenario 5

Random destinations are tested for different sources.

Table 6-6. Test 6

Source	Destination	Accessibility
Acad S2.1	Software Engineering Lab B Server	Deny
Admin S2.2	RS S2.1	Allow
RS 2.1	Media Technology Lab Server	Deny
RS 2.2	SQL server	Allow
Satellite Engineering Lab	Software Engineering Lab B Server	Deny
Media Technology Lab	Media Technology Lab Server	Allow
Intelligent Robotic Lab	Admin server	Deny
Acad S2.1	Admin Server	Allow
Admin S2.2	Admin Server	Allow
RS S2.1	Admin Server	Deny



Chapter 7. Summary and conclusion

In conclusion, all project and design objectives were taken into consideration. First, top-down analysis was undertaken. During this, the logical model including structure of the system was developed before the physical model was developed. Physical network segmentation using LANs was also done.

Next, logical networks were implemented from the bottom up utilizing a three-layered hierarchical architecture made up of Core, Distribution, and Access layers. The benefits of modularity, changeability, and testing ease brought about by clear functionality at each layer allowed for the assignment of host IP addresses in a way that minimized design costs. By positioning servers equally apart and as close to user groups as possible, servers were also positioned in a way that was justifiable.

By effectively deploying ACLs to filter packets as early as possible in the network, the security of the system was thus guaranteed. We utilized Packet Tracer software in the process of testing the respective different scenarios to ensure the communications between different user groups meet the given security requirements.

Members' contribution

Cheng Kejun	Writing of report: Chapter 1,3,4,5,6, Slides
Merchant Mahek Isak	Writing of report: Chapter 5,6 Development of simulation, Slides
Sanjena Suresh	Writing of report: Chapter 2,3,4,5,7, Slides