BSCPE DEVELOPMENT OF CUST NETWORK: A CISCO PACKET TRACER APPROACH 2025

DEVELOPMENT OF CUST NETWORK:
A CISCO PACKET TRACER APPROACH

by

Muhammad Abdullah

BCPE223031

A Project Report submitted to the

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

in partial fulfillment of the requirements for the degree of

BACHELORS OF SCIENCE IN COMPUTER ENGINEERING

Faculty of Engineering

Capital University of Science & Technology,

Islamabad

January, 2025

DECLARATION

It is declared that this is an original piece of my own work, except where otherwise acknowledged in text and references. This work has not been submitted in any form for another degree or diploma at any university or other institution for tertiary education and shall not be submitted by me in future for obtaining any degree from this or any other University or Institution.

Muhammad
Abdullah
BCPE223031

January, 2025

CERTIFICATE OF APPROVAL

It is certified that the project titled "Development of a Scalable Network Model for CUST University in Cisco Packet Tracer" carried out by Muhammad Abdullah BCPE223031, under the supervision of Sir Muneeb Ahmed, Capital University of Science & Technology, Islamabad, is fully adequate, in scope and in quality, as a final year project for the degree of BS of Computer Engineering.

Supervisor: -------------------------

Sir Muneeb Ahmed

Lab Engineer

Department of Electrical Engineering

Faculty of Engineering

Capital University of Science & Technology, Islamabad

HOD: ----------------------------

Dr. Noor Mohammad Khan

Professor

Department of Electrical Engineering

Faculty of Engineering

Capital University of Science & Technology, Islamabad

ACKNOWLEDGMENT

I would like to heartly thank our supervisor for helping us through every step of this project. Through endless mentoring and guidance of the Sir Muneeb Ahmed this project was successful. We would also like to thank our faculty for teaching us sincerely so that we could be able to complete the project.

ABSTRACT

Modern universities require scalable, efficient, and secure campus networks to support academic, administrative, and research activities. However, designing such networks poses challenges, including managing traffic, ensuring security, and accommodating future growth. This project addresses these challenges by designing a robust and scalable network for the Capital University of Science and Technology (CUST). The network design was implemented in Cisco Packet Tracer, utilizing a star topology for faculty departments to centralize communication. Key features such as VLAN segmentation were used to enhance traffic isolation and security. EIGRP was configured as the routing protocol to ensure dynamic and efficient data flow between network segments. Simulations validated the performance and functionality of the design. The project successfully demonstrated a scalable and efficient campus network that ensures seamless connectivity, low latency, and high security. The implemented network design effectively meets the current demands of the university while providing room for future scalability. This project bridges the gap between theoretical network design and practical implementation by offering a comprehensive framework for campus networks. This project serves as a comprehensive model for deploying robust and adaptable campus networks in educational institutions.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS/ABBREVIATIONS

EIGRP	Enhanced Interior Gateway Routing Protocol
VLAN	Virtual Local Area Network
IPv4	Internet Protocol Version 4
CLI	Command-Line Interface
RIP	Router Information Protocol
IP	Internet Protocol

Chapter 1

INTRODUCTION

Modern institutions require a well-designed and scalable campus network to function effectively. The Capital University of Science and Technology (CUST) is facing rising need for secure, dependable, and scalable network solutions to support academic and administrative operations. This project's goal is to design and develop a strong network architecture for CUST utilizing Cisco Packet Tracer, including advanced technologies like VLANs and EIGRP to improve functionality and scalability. The report covers the project's objectives, design principles, implementation steps, and real-world applications.

.

1.1 Overview

This project aims to provide a scalable, secure, and efficient campus network for the Capital University of Science and Technology (CUST). The architecture uses Cisco Packet Tracer and a ring topology to centralize faculty communication. VLANs provide traffic separation and security, while EIGRP enables dynamic and efficient routing. The resulting framework is designed to fulfil the present and future demands of the university's network infrastructure.

.

1.2 Project Idea

The project addresses the challenge of creating a reliable and scalable university network that ensures efficient communication and robust security. By segmenting the network with VLANs and employing dynamic routing with EIGRP, the design minimizes latency and improves reliability. The network was rigorously tested through simulations in Cisco Packet Tracer to validate its performance.

1.3 Purpose of the Project

The project aims to solve common network issues such as congestion and security vulnerabilities, which often arise from outdated designs. By leveraging VLAN segmentation and EIGRP routing, it establishes a modern approach to campus networking that ensures adaptability to future growth.

1.4 Project Specifications

Key features of the project include:

FEATURE	DESCRIPTION
TOPOLOGY	Star topology for central communication across faculty networks.
ROUTING PROTOCOL	EIGRP for dynamic and efficient routing between sub-networks.
VLAN	VLAN segmentation for enhanced security and traffic isolation.
SIMULATION TOOL	Cisco Packet Tracer for design, implementation, and testing.

1.5 Applications of the Project

The network design has several practical applications:

- Secure and efficient communication between different university departments.
- Scalability to accommodate future growth and increased traffic.
- Simplified network management through static IP allocation and segmentation.
- Enhanced security through VLAN-based traffic isolation.
- Provides a model for similar implementations in other organizations.
- Project Applications should be entered with bullets.

1.6 Project Plan

The project was divided into several phases to ensure organized progress. Tasks included literature review, network design, protocol configuration, and simulation testing. A detailed timeline outlined the key milestones and ensured efficient resource utilization.

1.6.1 Project Milestones

The milestones and resource allocations for the project are shown below:

Table 2 Proposed Project Plan

Tasks	Duration	Source Person
Literature Review	Week 1	Muhammad Abdullah
Network Design (Topology, VLANs)	Week 2	Muhammad Abdullah
EIGRP Configuration	Week 3	Muhammad Abdullah
Simulation and Testing	Week 4	Muhammad Abdullah

Chapter 2

LITERATURE REVIEW

This chapter provides an overview of the foundational work in network design, technologies related to the project, and relevant studies. By reviewing existing technologies, projects, and research, this chapter establishes the context for the proposed campus network design project and highlights the gaps that this work addresses.

2.1 Background Theory

A campus network is a system that interconnects various network segments in an educational institution, enabling efficient communication and resource sharing. Key technologies in this domain include VLANs, EIGRP routing. VLANs are used to segment a network into logical units to isolate traffic, improve security, and reduce congestion. EIGRP, a dynamic routing protocol, is employed to ensure efficient and adaptive routing in large networks. These technologies are fundamental in designing scalable and secure campus networks.

2.2 Related Technologies

Several other technologies complement or extend the scope of this project, helping to create more efficient, secure, and scalable networks.

2.1.1 Related Technology: Software-Defined Networking (SDN)

Software-Defined Networking (SDN) is an emerging technology that decouples network control and data planes. This allows centralized control of network traffic, providing flexibility and scalability in managing complex networks. While SDN offers a significant advantage in dynamic and large-scale network management, its implementation complexity and cost limit its adoption in smaller, budget-conscious projects like the current one.

2.1.2 Related Technology: IPv6

IPv6 is the latest version of the Internet Protocol (IP), designed to replace IPv4 due to the exhaustion of IPv4 addresses. It offers an expanded address space and improved network efficiency, security, and scalability. While this project uses IPv4 for simplicity, future network expansions may adopt IPv6 to ensure scalability as the number of devices connected to the network grows.

2.3 Related Studies/Research

Recent research has focused on optimizing campus networks for better performance and security. Some notable areas of research include:

- Network Virtualization: Research into virtualized networks has gained traction as universities move towards cloud-based services. These technologies allow for more efficient resource allocation and management.
- Enhanced Security: Studies on securing campus networks against cyber threats have emphasized the importance of VLAN segmentation and the use of modern encryption protocols to prevent data breaches.
- IoT Integration: As campuses adopt more IoT (Internet of Things) devices, research has explored how to integrate these devices into existing networks without causing congestion or performance degradation.

2.4 Limitations of the Existing Work

While the reviewed projects and technologies have contributed significantly to campus network design, there are several limitations:

- Complexity: Implementing and managing advanced technologies such as SDN and IPv6 may not be practical for smaller institutions with limited resources.
- Scalability: Many existing solutions focus on current needs and are not future- proof, making it difficult to accommodate growing demands over time.
- Security: Despite advancements, campus networks remain vulnerable to various security threats, including unauthorized access and denial-of-service

attacks. More robust security measures are required to address these issues effectively.

2.5 Problem Statement

The hypothesis driving this project is that a well-designed campus network, utilizing VLANs, EIGRP can enhance network performance, scalability, and security for a university environment. This research will test the feasibility of this hypothesis by designing and implementing a campus network using Cisco Packet Tracer. Challenges to be addressed include network congestion, IP address conflicts, and security vulnerabilities. The research will demonstrate how these technologies, when combined, can optimize the performance of the network while ensuring scalability for future growth.

2.6 Summary

This chapter has provided a comprehensive review of the background theory, related technologies, projects, and research, as well as the limitations of existing work. The insights gained from this literature review serve to inform the design and implementation of the university network, highlighting key considerations and areas for improvement. The next chapter will delve into the specific design and implementation details of the proposed solution.

Chapter 3

PROJECT DESIGN AND IMPLEMENTATION

This chapter describes the core design and implementation process of the campus network, explaining all the methods used to achieve the desired results. The following sections detail the techniques and technologies applied, including their challenges and limitations encountered during the project.

3.1 Proposed Design Methodology

The design methodology was structured around the development of a Star Topology for the faculty networks, ensuring efficient communication and scalability for the campus. The core of the design integrates the EIGRP routing protocol for optimal path selection across the network and the VLAN technology to segment the network for enhanced performance and security. was employed for dynamic IP addressing to simplify network management. The design ensures redundancy, high availability, and minimal downtime, allowing for easy expansion as needed.

Additionally, the subnetting strategy ensured that there were sufficient IP address allocations for each department while minimizing wasted IP addresses. The choice of subnet masks was based on the number of devices in each faculty, with consideration for future scalability. The following block diagram illustrates the main building blocks of the proposed design.

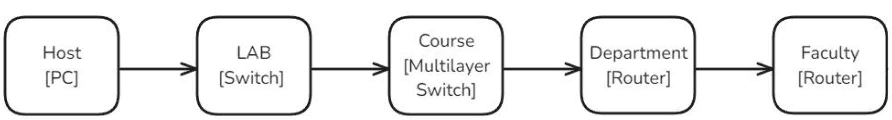

Figure 2 Block diagram of network

3.2 Analysis Procedure

Several alternatives were considered for network design, including different topologies and routing protocols. A comparison between Ring and Star topologies revealed that the Star topology was more scalable and easier to manage in a campus environment with multiple faculty departments. The decision to use EIGRP over other protocols like RIP was based on its ability to handle larger networks with more dynamic routing requirements. Additionally, the VLAN architecture was chosen to isolate traffic and improve security. Subnetting was an integral part of this decision, as it allowed for efficient allocation of IP addresses for each department. Each VLAN was assigned a unique subnet, enabling proper segmentation and isolation. The justification for these decisions is based on their ability to meet the needs for scalability, security, and ease of maintenance.

3.3 Design of the Project Hardware

The hardware design of the campus network primarily involves the selection of routers, switches, and multilayer switches that form the backbone of the network. Cisco routers and switches were chosen due to their reliability and compatibility with EIGRP and VLAN configuration. The network design incorporates redundant links between faculty switches and core routers to minimize the risk of network downtime. The hardware setup also includes access points to ensure wireless connectivity across the campus. To accommodate up to 1000+ devices while maintaining optimal performance and low latency, each faculty department was assigned its own subnet through VLAN configuration. The use of subnetting allowed for clear traffic boundaries and simplified IP management across the campus.

3.4 Design of the Project Software/Algorithm

The software design focuses on the configuration and management of EIGRP, VLAN, and on Cisco devices. The algorithm for configuring EIGRP ensures automatic route discovery and load balancing across the network. VLAN configuration is handled through a centralized management system, ensuring each department or faculty has its own isolated virtual network.

The subnetting approach ensures that devices in each VLAN receive IP addresses from the appropriate subnet without manual configuration

3.5 Implementation Procedure

The implementation of the campus network was carried out step by step. Below are the CLI commands used during each process.

3.5.1 EIGRP Configuration

```
Router>en
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router eigrp 10
Router(config-router)#network 175.65.0.0
Router(config-router)#network 175.65.32.0
Router(config-router)#network 172.161.0.0
Router(config-router)#ex
Router(config)#do wr
Building configuration...
[OK]
Router(config)#
```

Figure 3 EIGRP Configuration

3.5.2 VLAN Configuration

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name DLD
Switch(config-vlan)#ex
Switch(config)#vlan 20
Switch(config-vlan)#name ECE
Switch(config-vlan)#ex
Switch(config)#vlan 30
Switch(config-vlan)#name CAO
Switch(config-vlan)#ex
Switch(config)#
```

Figure 4 VLAN Database

```
Switch(config)#
Switch(config)#int range fa0/3-24
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#ex
Switch(config)#
```

Figure 5 VLAN Access Ports

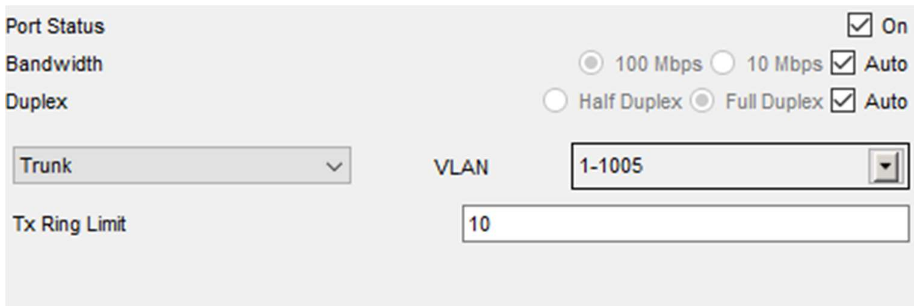

Figure 6 VLAN Trunk Ports

Figure 7 Binding VLAN to Router

3.5.3 Subnetting Configuration

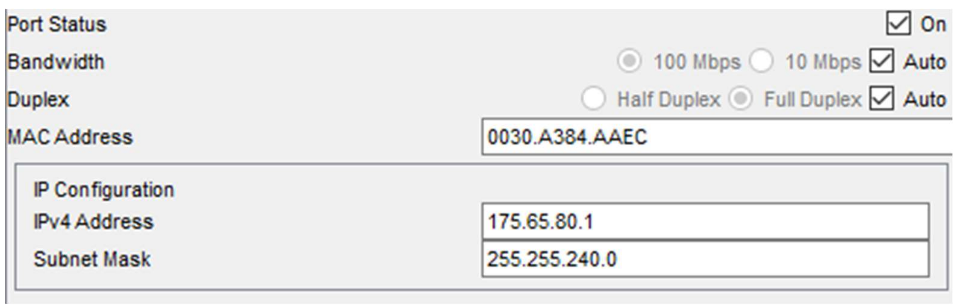

Figure 8 Assigning Subnet Network to a Router

3.5.4 Configuration

Figure 9 Implementing

3.6 Details of Simulations / Mathematical Modeling

Simulations were conducted in Cisco Packet Tracer to visualize and verify the network topology, routing behavior, and VLAN configuration. Subnetting was carefully tested in the simulation to ensure that IP address allocation within each VLAN was accurate and that inter-VLAN routing was functioning correctly. The effectiveness of the subnetting strategy was evaluated by checking the EIGRP convergence time and ensuring that all subnets were properly recognized and routed. VLAN segmentation.

3.7 Details of Final Working Prototype

The final working prototype of the campus network design was deployed on a virtualized Cisco environment in Cisco Packet Tracer.

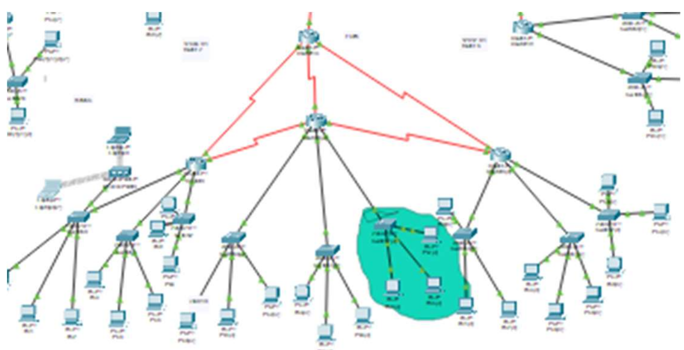

Figure 10 Computing Faculty Network

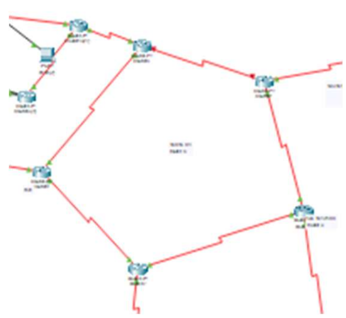

Figure 11 ring Topology

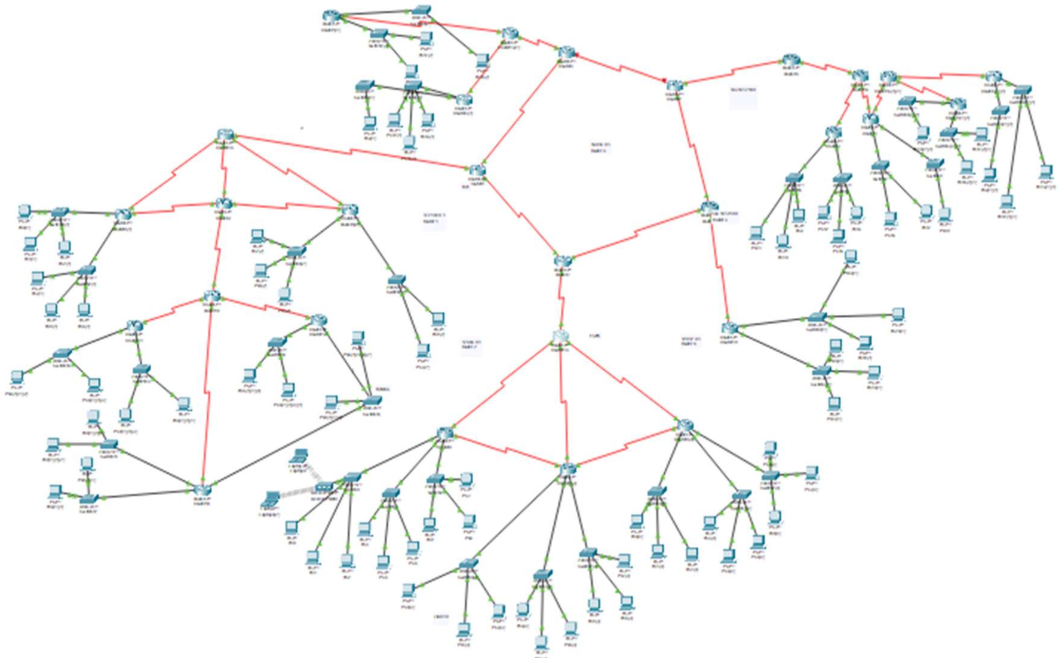

Figure 12 Entire Campus Network

3.8 Summary

This chapter outlined the design and implementation procedures followed to build the campus network using Star Topology, EIGRP, VLAN, and . Subnetting was an essential part of the design, as it ensured proper segmentation and isolation of each faculty and department's network traffic. The design was analyzed to ensure scalability, security, and ease of management. The hardware and software components were selected and configured to meet the project’s requirements, with simulations and performance tests conducted to validate the final working prototype.

Chapter 4

TOOLS AND TECHNIQUES

This chapter discusses the various tools and techniques that were essential in the design, implementation, and simulation of the campus network. The tools mentioned include software for simulation, hardware for real-world deployment, and various other techniques that supported the project from conception to completion. The following sections provide detailed insights into the tools used in each phase.

4.1 Software and Simulation Tools

This section provides details about the software and simulation tools used in the project to create, configure, and simulate the network infrastructure.

4.1.1 Cisco Packet Tracer

Cisco Packet Tracer was the key software tool used throughout the project to simulate the campus network. It allowed for the visualization of the network design, the configuration of network devices, and the testing of protocols such as EIGRP and .

4.1.2 Subnetting Calculator

A Subnetting Calculator was used to efficiently plan and allocate IP addresses across the campus network. This tool was particularly useful for determining the correct subnet masks and IP address ranges for each VLAN.

Chapter 5

CONCLUSION AND FUTURE WORK

This project successfully demonstrated the potential of simulation-based tools like Cisco Packet Tracer to design and evaluate an efficient, scalable, and secure campus network. By implementing a ring topology, static routing using EIGRP, and VLAN segmentation, the network design addressed critical requirements such as scalability, performance optimization, and traffic isolation. The integration of streamlined IP management, ensuring ease of device connectivity. While the results validate the practicality of the design, the project lays a foundation for further exploration, including real-world implementation with physical hardware, enhanced redundancy mechanisms, advanced security measures, and support for emerging technologies like IPv6 and Software-Defined Networking. Additionally, scaling the network to accommodate thousands of devices and conducting in-depth traffic analysis with tools like Wireshark would provide deeper insights into performance and reliability. For those aiming to build upon this work, leveraging real-world data, engaging with experts, and maintaining thorough documentation are strongly recommended to enhance the practicality and robustness of the design. Overall, this project provides a robust framework for modern campus network design and serves as a stepping stone for further advancements in network engineering.

References

1 EIGRP ImplementationGeeksforGeeks02June2022Available:https://www.geeksforgeeks.org/ospf-implementation/28December2024

2

3 Configuring and Verifying VLANs in CiscoGeeksforGeeks23April2024Available:https://www.geeksforgeeks.org/configuring-and-verifying-vlans-in-cisco/31December2024

A.4 Department : Civil Engineering

Table 6 Civil Engineering Subnet

LAB	Network	Department IP	Usable Host Range	Broadcast Address
1	172.161.24.0/21	172.161.8.1	172.161.8.1 - 172.161.8.254	172.161.8.255
2	172.161.24.0/21	172.161.40.1	172.161.40.1 - 172.161.40.254	172.161.40.255
3	172.161.24.0/21	172.161.56.1	172.161.56.1 - 172.161.56.254	172.161.56.255

Appendix – B: Faculty of Computing Subnetting Structure

B.1 Faculty of Computing

Table 7 Faculty of Computing Subnet

Network	Subnet Mask	Faculty IP	Usable Host Range	Broadcast Address
175.65.0.0/20	255.255.240.0	175.65.0.1	175.65.0.1 - 175.65.15.254	175.65.15.255

B.2 Department : Computer Science

Table 8 Computer Science Subnet

LAB	Network	Department IP	Usable Host Range	Broadcast Address
OOP	192.168.2.32/27	175.65.16.0	175.65.16.1 - 175.65.31.254	175.65.31.255
DS	192.168.2.64/27	175.65.32.0	175.65.32.1 - 175.65.47.254	175.65.47.255
WAD	192.168.2.96/27	175.65.48.0	175.65.48.1 - 175.65.63.254	175.65.63.255

B.3 Department : Mathematics

Table 9 Mathematic Subnet

LAB	Network	Department IP	Usable Host Range	Broadcast Address
1	192.168.2.128/27	175.65.64.0	175.65.64.1 - 175.65.79.254	175.65.79.255

B.4 Department : Software Engineering

Table 10 Software Engineering Subnet

LAB	Network	Department IP	Usable Host Range	Broadcast Address
1	192.168.2.160/27	192.168.2.161	192.168.2.162- 192.168.2.190	192.168.2.191
2	192.168.2.192/27	192.168.2.193	192.168.2.194- 192.168.2.223	192.168.2.223
3	192.168.2.224/27	192.168.2.225	192.168.2.226- 192.168.2.254	192.168.2.255

Appendix – C: Faculty of Management and Social Science Subnetting Structure

C.1 Faculty of Faculty of Management and Social Science

Table 11 Faculty of Management and Social Science Subnet

Network	Subnet Mask	Faculty IP	Usable Host Range	Broadcast Address
193.151.210.0/27	255.255.255.224	193.151.210.1	193.151.210.1 - 193.151.210.30	193.151.210.31

C.2 Department : Management Sciences

Table 12 Management Sciences Subnet

LAB	Network	Department IP	Usable Host Range	Broadcast Address
1	193.151.210.32/27	193.151.210.33	193.151.210.33 - 193.151.210.62	193.151.210.63
2	193.151.210.64/27	193.151.210.65	192.168.31.66- 192.168.31.94	193.151.210.95

C.3 Department : Psychology

Table 13 Psychology Subnet

LAB	Network	Department IP	Usable Host Range	Broadcast Address
1	193.151.210.96/27	193.151.210.97	193.151.210.98- 193.151.210.126	193.151.210.127
2	193.151.210.128/27	193.151.210.129	193.151.210.130- 193.151.210.158	193.151.210.159

C.4 Department : Accounting and Finance

Table 14 Accounting and Finance Subnet

LAB	VLAN	Network	Department IP	Usable Host Range	Broadcast Address
1	10	193.151.210.160/27	193.151.210.161	193.151.210.162- 193.151.210.190	193.151.210.191

C.5 Department : English

Table 15 English Subnet

LAB	VLAN	Network	Department IP	Usable Host Range	Broadcast Address
1	12	193.151.210.192/27	193.151.210.193	193.151.210.194-193.151.210.223	193.151.210.223
1	40	193.151.210.224/27	193.151.210.225	193.151.210.226-193.151.210.254	193.151.210.255

Appendix – D: Faculty of Health and Life Sciences Subnetting Structure

D.1 Faculty of Health and Life Sciences

Table 16 Faculty of Health and Life Sciences Subnet

Network	Subnet Mask	Faculty IP	Usable Host Range	Broadcast Address
160.16.0.0/21	255.255.248.0	160.16.0..1	160.16.0.1 - 160.16.31.254	160.16.31.255

D.2 Department : Bioinformatics

Table 17 Bioinformatics Subnet

LAB	VLAN	Network	Department IP	Usable Host Range	Broadcast Address
1	10	160.16.8.0/21	160.16.8.1	160.16.8.1 - 160.16.15.254	192.168.4.31
2	20	160.16.16.0/21	160.16.16.1	160.16.0.1 - 160.16.31.254	192.168.4.47
3	30	160.16.24.0/21	160.16.24.1	160.16.0.1 - 160.16.31.254	192.168.4.63
4	20	160.16.32.0/21	160.16.32.1	160.16.32.1 - 160.16.39.254	192.168.4.79
5	30	160.16.40.0/21	160.16.40.1	160.16.40.1 - 160.16.47.254	192.168.4.95
6	40	160.16.48.0/21	160.16.48.1	160.16.48.1 - 160.16.55.254	192.168.4.111

Appendix – E: Faculty of Pharmacy Subnetting Structure

E.1 Faculty of Pharmacy

Table 18 Faculty of Pharmacy Subnet

Network	Subnet Mask	Faculty IP	Usable Host Range	Broadcast Address
120.0.0.0/11	255.224.0.0	120.0.0.1	120.0.0.1 - 120.31.255.254	120.31.255.255

E.2 Department : Pharmacy

Table 19 Pharmacy Subnet

LAB	Network	Department IP	Usable Host Range	Broadcast Address
1	120.32.0.0/11	120.32.0.1	120.32.0.1 - 120.63.255.254	120.63.255.255
2	120.64.0.0/11	120.64.0.1	120.64.0.1 - 120.95.255.254	120.95.255.255
3	120.96.0.0/11	120.96.0.1	120.96.0.1 - 120.127.255.254	120.127.255.255