



**DEBRE BERHAN UNIVERSITY**

**COLLEGE OF COMPUTING**

**DEPARTMENT OF INFORMATION SYSTEM**

**A Project ON**

**A Local Area Network Design for Debre Berhan Polytechnic College**

**PROJECT SUBMITTED IN PARTIAL FULFILLMENT OF THE  
REQUIREMENT FOR THE AWARD OF THE DEGREE OF BACHELOR  
OF SCIENCE IN INFORMATION SYSTEM**

**SUBMITTED BY**

**NAME OF STUDENTS**

**ID NO**

1. ZELALEM ASHENAFI

3258/11

2. ABNET BASHE

3886/11

3. MEDHANIT TEGAFW

1750/11

4. SELAM ALEHEGN

1712/11

5. MELKE DESIE

1715/11

**PROJECT ADVISOR: Mr. ALEBACHEW CHICHE**

**JUNE, 2022,**

**Debre Berhan University, Debre Berhan, Ethiopia**

## DECLARATION

The project entitled A LOCAL AREA NETWORK DESIGN FOR DEBRE BERHAN POLYTECHNIC COLLEGE is submitted to the Department of Information Systems for the award of BSC in Department of Information Systems is based on our original work carried out under the guidance of Mr. Alebachew Chiche. The project has not been submitted elsewhere for the award of any degree.

The material borrowed from other source and incorporated in the project has been duly acknowledged and/or referenced.

We will be responsible and liable for plagiarism, if any, detected later on.

**Date:** \_\_\_\_\_

**Name of the students**

**Signature**

1. ZELALEM ASHENAFI

\_\_\_\_\_

2. ABNET BASHE

\_\_\_\_\_

3. MEDHANIT TEGAFAW

\_\_\_\_\_

4. SELAM ALEHEGN

\_\_\_\_\_

5. MELKE DESIE

\_\_\_\_\_

**Name of the Advisor**

**Signature**

**Date**

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

## APPROVAL FORM

This is to confirm that the project report entitled A Local area network design for Debre Berhan polytechnic college submitted to **Debre Berhan University**, College of Computing Department of Information Systems by Group one(1) is approved for submission.

-----	-----	-----
Advisor Name	Signature	Date
-----	-----	-----
Department Head Name	Signature	Date
-----	-----	-----
Examiner 1 Name	Signature	Date
-----	-----	-----
Examiner 2 Name	Signature	Date
-----	-----	-----
Examiner 3 Name	Signature	Date

## **Acknowledgement**

First of all, we would like to thank our GOD for giving all the capabilities to do everything and helped us from the start to the end.

Secondly, we would like to express our deepest gratitude to our advisor Mr. Alebachew Chiche for his support and his continuous encouragement, kindly support, quick evaluation of our work and creative advices.

We would also to thank the community of the DBPTC college especially Mr. Kefelegn Gulnt and his colleagues for their willingness for interviews and for giving us any information that are related with our project.

Finally we would like to thank our class mates, friends, family for their support and encouragement and everyone who directly or indirectly participated on this project.

# Table of Contents

DECLARATION .....	i
APPROVAL FORM .....	ii
Acknowledgement .....	iii
List of Figures .....	vii
List of Tables .....	vii
List of Abbreviation .....	viii
CHAPTER ONE .....	1
1. INTRODUCTION .....	1
1.1 Introduction .....	1
1.2 Background of the organization.....	2
1.3. Statement of the problem .....	4
1.4. Objectives.....	4
1.4.1. General objective .....	4
1.4.2. Specific objectives .....	5
1.5. Scope.....	5
1.6. Significance of the study .....	7
1.7. Beneficiary of the system.....	7
1.8. Methodology.....	7
1.9. Tools .....	9
1.10. Feasibility study .....	10
1.10.1. Operational Feasibility .....	10
1.10.2. Technical Feasibility .....	10
1.10.3. Economic Feasibility.....	10
1.10.4. Political feasibility .....	12
Chapter Two.....	13
2. Network Analysis.....	13
2.1. Description of the Current Network .....	13
2.2. The New Proposed Network.....	14
2.3 Functional Requirements.....	14

2.4 Non Functional Requirements .....	15
2.5. Network Requirements.....	16
2.5.1 User Requirements .....	16
2.5.2 Network device Requirements .....	17
2.5.3 Service Requirements .....	19
2.5.4 Standard Requirements .....	20
2.5.5 Protocol Requirements .....	20
2.5.6 Wireless LAN Requirements.....	22
Chapter Three.....	23
3. Network Architecture.....	23
3.1. Introduction .....	23
3.2. Network Topology.....	23
3.3. Technologies .....	24
3.3.1. Performance.....	24
3.3.2. Security .....	25
3.3.4. Network management .....	26
3.4. Equipment Class.....	28
3.5. Addressing.....	30
3.6. Routing.....	30
Chapter Four .....	31
4. Design phase .....	31
4.1. Introduction .....	31
4.2. Network design .....	31
4.2.1. Physical design .....	32
4.3. Data Center deign .....	34
4.4. Network Design Topology.....	38
4.5. IP addressing schema.....	40
4.6. VLAN design .....	44
4.7. Security design .....	45
4.8. Routing protocol .....	47

4.9. WLAN design .....	48
4.10. Servers.....	50
4.11. Location Specification .....	51
4.12. Vendor Selection.....	53
4.13. ISP (internet service provider) .....	55
References .....	57
Appendix I .....	58
Appendix II .....	59

## List of Figures

Figure 1: Organizational Structure of DBPTC .....	3
Figure 2 Geographical scope .....	6
Figure 3: Network Management Architecture .....	27
Figure 4: Physical network design for Library .....	32
Figure 5: Physical network design for LABs.....	33
Figure 6: Physical network design for Offices .....	33
Figure 7: Physical network design for Workshops .....	34
Figure 8: Physical design for Data center .....	36
Figure 9: Components of data center .....	37
Figure 10: Hierarchical Network Structure.....	39
Figure 11: Hierarchical Network Structure in DBPTC compound (Logical Design) .....	40
Figure 12: Logical design for IP design and sub-networks .....	43
Figure 13: Logical design for VLAN Structure .....	44
Figure 14: Security architecture of the network .....	47
Figure 15: Outdoor wireless LAN design.....	50
<i>Figure 16: Physical network design for Location specification .....</i>	<i>53</i>

## List of Tables

Table 1: Tools .....	9
Table 2: Items with their quantity and total Cost prices .....	11
Table 3: Hardware Requirements .....	17
Table 4: Software Requirements.....	18
Table 5: Sub-networks with their information.....	41
Table 6 Sample switch allocation .....	41



Table 7: VLANs with their purpose.....	45
Table 8: Location specification for Network devices .....	52
Table 9: Network devices with vendors.....	54

## **List of Abbreviation**

DBPTC: Debre Berhan Poly Technic College

DHCP: Dynamic Host Control Protocol

DNS: Domain Name Service

FTP: File Transfer Protocol

HRMS: Human Resource Management System

ICT: Information Communication Technology

IEEE: Institute of Electrical and Electronics Engineers

IOS: International Organizational Standard

IP: Internet Protocol

LAN: Local Area Network

Mbps: Megabit per second

NOC: Network operation control

OSPF: Open shortest path first

PPDIOO: Prepare, Plan, Design, Implement, Operate, and Optimize

QoS: Quality of services

SNMP: Simple Network Management Protocol

SSH: Secure Shell

TCP: Transmission Control Protocol

UPS: universal power supply

UTP: Unshielded Twisted Pair

VPN: Virtual private network

VTP: Virtual trunking protocol

Gbps: Gigabits per second

WEP: Wired equivalent privacy

WLAN: Wireless Local Area Network

# **CHAPTER ONE**

## **1. INTRODUCTION**

### **1.1 Introduction**

The computer network represents a component, especially on how it enhances the functional performance in different fields and organizations, such as companies and schools. A school's computer network performs so many functions, such as connecting students with the college, faculty, and the library. Most educational sectors today use the network to provide online education by connecting widely dispersed students with their instructors directly. For this reason, computer networks play a vital role in the education area by providing efficient communications for the college environment. However, the design of computer networks differs from one sector to another. This is a result of many factors which determine the differences. Such factors include; adaptability, integration, resilience, security, and cost.

LAN network is made up of two or more computers connected in a short distance usually at home, office buildings, or school. For designing a LAN network the most efficient way is to use the hierarchical network design approach. A hierarchical network design involves dividing the network into discrete layers. Each layer or tier in the hierarchy provides specific functions that define its role within the overall network. This helps the network designer and architect to optimize and select the right network hardware, software, and features to perform specific roles for that network layer. The benefit of dividing a flat network into smaller, more manageable blocks is that local traffic remains local. Only traffic that is destined for other networks is moved to a higher layer. This design approach includes the Core, Distribution, and Access Layers which include different services and protocols such as Datacenter, Routing, VLAN, WAN, and Security design.

As part of its strategy for innovation and growth, the Debre Berhan Ploy Technic college ICT office (DBPTC ICT) plans to build a new network with scalable modular data center on the ground floor of the B-12 building which will house the Servers, Network equipment, Storages and the Internet active element's. As such, they have to be extremely reliable and secure while being able to accommodate growth and reconfiguration.

Considering that network infrastructure is the heartbeat of any organization, DBPTC ICT Office intends to setup a campus network and data center infrastructure that will have a modern facility, built on state-of-the-art technology and that measure up to best practices in the industry. The new infrastructure shall not only support the present computing demands, but it shall also, be capable of gracefully accommodating future and emerging computing requirements of the college. It is envisioned that at the end of the design, the infrastructure would be converted into a state-of-the-art facility that is not only faster, but also highly available, fault tolerant, and safe place to store and run all the critical business applications of college.

To this end, the purpose of this project is, therefore, to design and set up a new hierarchical network and secured modular data center that protects resources, optimizes IT productivity and resource utilization, and supports growth. The proposed design will help to align network resources with DBPTC's business priorities.

## **1.2 Background of the organization**

Debre Berhan Polytechnic College (DBPTC) is an educational sector that is found in Debre Berhan city which is located 695K.M far from Regional City Bahirdar and 130 K.M far from the capital city of Ethiopia, Addis Ababa.

The College was established in 1990 E.C. with 106 male and 69 female students a total of 191 students. It had been teaching in only 4 fields of study and these are General Mechanics, Auto Mechanics, Electricity and Wood Work.

In general, The College has 57 buildings, which include classrooms, workshops, labs, and offices. Currently, it includes about 11 departments within different fields and 65 fields of training. Among these buildings, the 4 departments have Computer Laboratories.

Currently, the college is teaching 3096 students from different areas especially Debre Berhan city and other neighboring places in northern Shewa.

The College organization is divided into 10 different middle-level management departments and each department has other sub-departments and their own work divisions. It is adamantly and unrelentingly working and undertaking massive organizational activities in terms of human resource development and construction with an overview to further enhance its institutional capacity in areas of producing competent graduates, conducting problem-solving research & offering community services.

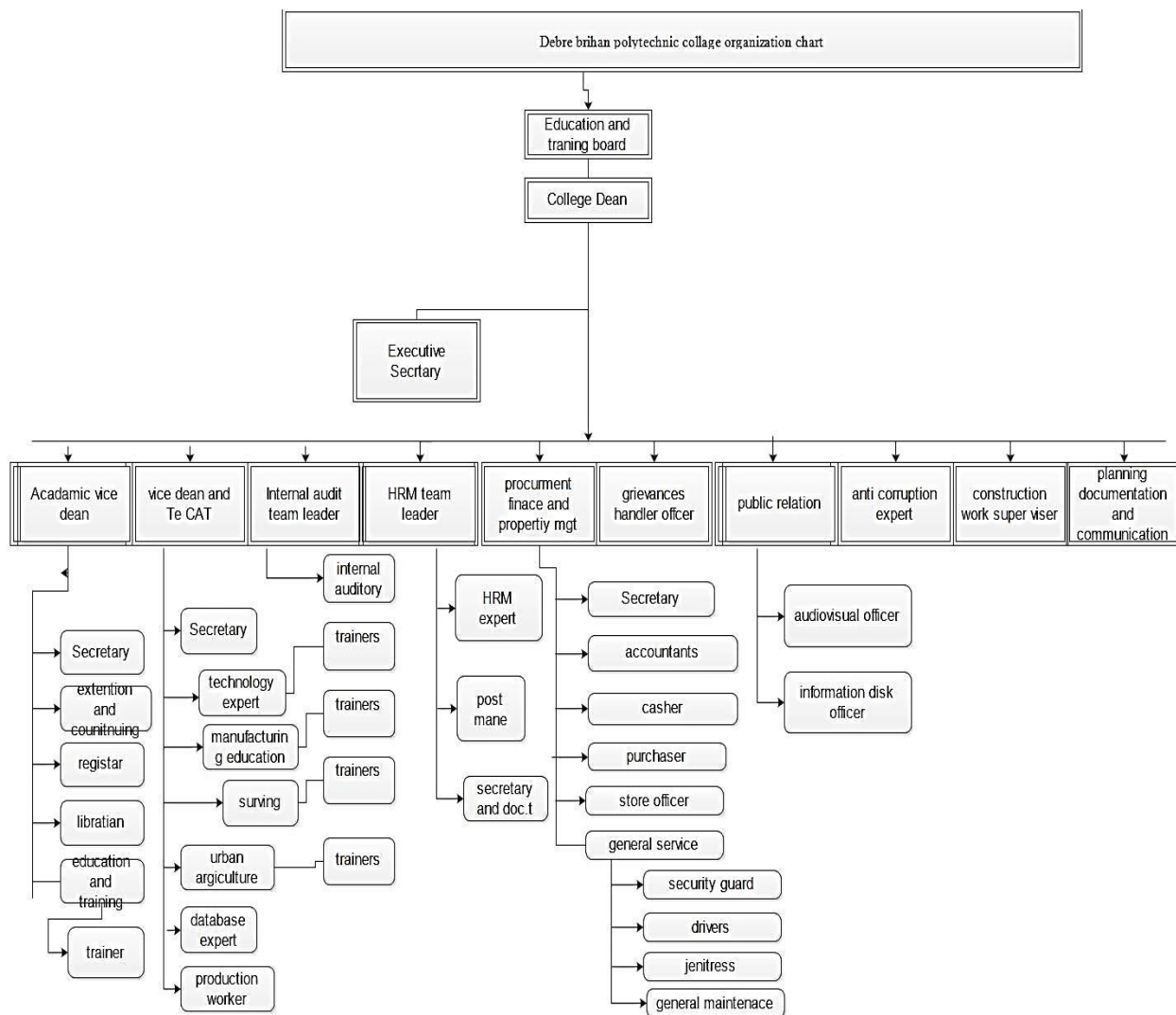


Figure 1: Organizational Structure of DBPTC

### **1.3. Statement of the problem**

The existing DBPTC network covers only the administrative building, library and the computer laboratories. There is no wireless access point around the building to enable the students to access the network using portable devices.

The limited coverage of this flat network structure causes the network not to address all class rooms and workshops, the wireless APs are only located in several buildings around the administrative and ICT department buildings, and this makes the Wi- Fi service not sufficient for all users. It has also lack of network devices and servers like database server, printer server, applications servers; this makes users unable to use resource sharing services. And the existing network has also impacts in slow response time, slow speed performance, security problem on the network traffic, higher traffic since the existing network is not sufficient

Due to the absence of data storages improper data handling is the other problem in the institution, data may be lost. Data integrity and consistency, Security, delay, online data sharing, and central administration in DBPTC is also a serious problem of the project.

The College is now expanding with many departments and the number of students and staff is now increasing year to year dramatically. So providing service for the student manually will be difficult.

As the number of students increase and in the time of very busy days, it is difficult to handle students' requests manually, students' abundant data requires many buildings to store paper data, and also it requires a continuous high amount of money each year which is above the real financial capacity of the College.

This was the reason that motivates us to propose the network design with a new reliable and available Data-Center based network.

### **1.4. Objectives**

#### **1.4.1. General objective**

The general objective of this project is to design and implement a good Local area network for Debre Berhan Poly Technic College.

### **1.4.2. Specific objectives**

The specific objectives of this project are:-

- To identify existing network problems
- To define the identified problems
- To gather the requirement from stakeholders,
- To identify the appropriate tools and devices to be used,
- To identify and select the locations where the device will be located,
- To design the network structure according to the requirement,
- To install and configure the design using simulation tools,
- To test the connectivity of the configurations.

### **1.5. Scope**

Geographically, this project will be designed to work on the compound of the DBPTC- it is located around tebase in kebele 07. The central network will cover the whole compound of the college.

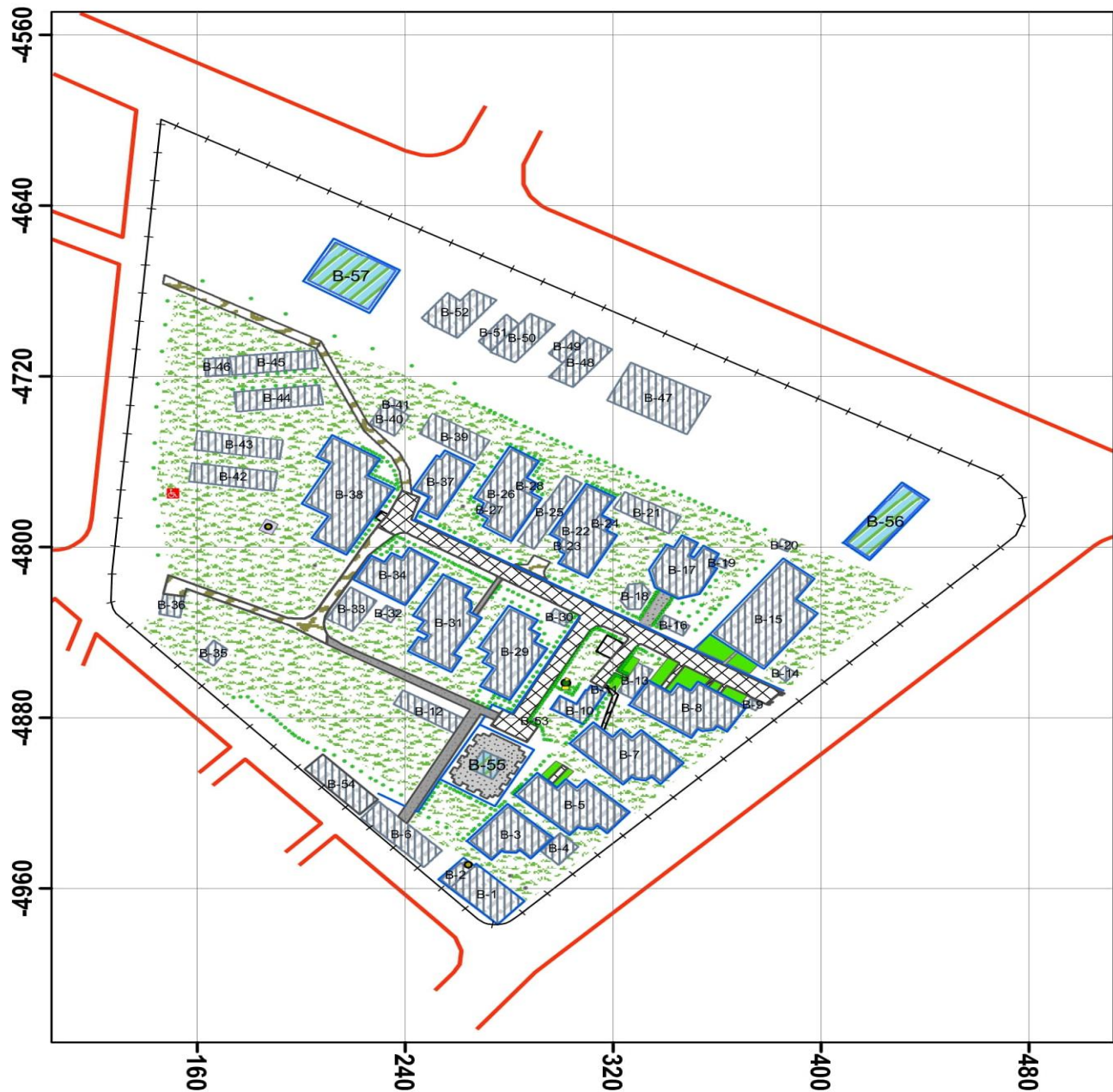


Figure 2 Geographical scope

The project implementation includes the design data center, design LAN and WLAN, design security, VLAN Configuration, and different services such as NAT, DHCP, DNS, FTP, Mail Server, IP design, and Application Servers using LAMP configuration (LINUX). This project also ensures that the new network design ability of fault tolerance, security, and high-speed connection, Supports scalability for future expansion, providing an intra-communication mechanism.

## 1.6. Significance of the study

After the implementation of the design, the college will have a structured and organized network. This implementation has a benefit for different bodies such as the organization and the end-users.

At the organization level, it is used to facilitate student registration and profile management by using its prevention method, it helps to enhance availability and avoid data loss. Financially, the new proposed network system is used to avoid financial losses due to shrinking repayment and rising costs and avoid duplication of services; it also decreases the college's expenses.

For the end-users, it has a role to save time by serving a large number of users in a minimum response time. It also gives unlimited access to students' data by any privileged user at any time from any place in the college even the same record at the same time concurrently.

## 1.7. Beneficiary of the system

This network design project is significant for the college community by facilitating the day-to-day activities and by improving the overall performance of the network and bodies who gained benefits from this network design are:-

**Students** are the first and main beneficiaries of this system, the teaching-learning process can be efficient and facilitated by utilizing the internal and worldwide resources and services of this new network infrastructure.

**Staff** can be teachers, lab and workshop assistants, and office workers, the new network makes their work and duties simpler in terms of ease connection with students and access to their student's information, result management system, and share education resources

**High-level managers** be able to control of the whole ICT infrastructure in the college they can get current status and information without moving from their offices,

And also other bodies including employees will benefit from this project in the aspect of use of internet service or get connected worldwide and information sharing.

## 1.8. Methodology

This project requires different methodologies for different tasks, as a network design project it needs different activities starting from assessing the physical and logical structure of the



compound to gathering information about the users that is included in this network structure. Usually designing a networking project is passing through six common phases. Our project is also passing along these stages. These are **PPDIOO** (prepare, plan, design, implement, operate, and optimize) phases. PPDIOO stands for Prepare, Plan, Design, Implement, Operate, and Optimize. PPDIOO is a Cisco methodology that defines the continuous life-cycle of services required for a network. The main advantage of this network methodology is to minimize the total cost of network ownership, it also increase the network availability and accelerate access to application and services.

For the design process, project is designed by using the **Hierarchical Network Design Approach**. A hierarchical network design involves dividing the network into discrete layers. Each layer, or tier, in the hierarchy provides specific functions that define its role within the overall network. This helps us to optimize and select the right network hardware, software, and features to perform specific roles for that network layer.<sup>[1]</sup>

Some methodologies are used for the data gathering process.

- **Observation:** Observation is one of our data collection methods and it is more accurate than the other methods because during observation we have observed everything available in the organization related to the network. And also this method helps us to decide in our way. There is a limited end users and network device as compare to the number of the students. Even there are some devices such as a APs and Switches. There is no standard full data center and network management mechanism.
- **Interview:** In this data collection method we have got some answers to what we before asked about local area network, wide area, and data center design by directly communicating with the system administrator and his colleagues. We have discussed with them on oral questions that are concerned with our field of study. We have interpreted and analyzed their opinion. We have also interviewed the network administrator orally.
- **Document review:** Publications and other researches that have direct relation with our project is reviewed and assessed.

## 1.9. Tools

To design and logically implement this project we used the following HW and SW tools:

Table 1: Tools

Software requirements	Hardware requirements
1. Cisco packet tracer 8.0.0	1. Desktop computer with the following Specification <ul style="list-style-type: none"><li>➤ RAM: 8GB</li><li>➤ Storage: 1TB</li><li>➤ Processor: IntelI CORE I I7 CPU 4160</li></ul>
2. Windows 10 Operating System and Linux operating system: - for design and implementation.	2. Laptop with the following Specification <ul style="list-style-type: none"><li>• RAM: 4GB</li><li>• Storage: 1TB</li><li>• Processor: IntelI CORE I I3 CPU 5005</li></ul>
3. Microsoft Visio 2013 and Wondershare Edraw 2007:-for drawing diagrams.	3. External hard disk with <ul style="list-style-type: none"><li>• Storage:1TB</li></ul>
4. Enterprise.Architect.12.0	
5. Microsoft Office 2019	

## **1.10. Feasibility study**

This project is designed by considering the current ability of the organization in terms of financial, time and resources. The following types of feasibility are analyzed according to the organization.

### **1.10.1. Operational Feasibility**

This project is operationally feasible and able to utilize, support and perform the necessary service of the network. The new design will improve the reachability of the network by increasing its speed, performance, and security. It satisfies customers' requirements identified in the requirements analysis phase of system development and performs or operates several tasks to provide a service for the user. Due to these reasons, the project is operationally feasible.

### **1.10.2. Technical Feasibility**

This project is technically feasible because it can meet performance objectives. It supports different networking technologies in the organization regarding networking devices, software applications, protocols and skilled people to administer the ICT center effectively.

The technical goals of our project are:

- Improve network capacity and performance.
- Provide sufficient network access.
- Support scalability for future expansions.
- Managing network effectively.
- Improve network security.
- Achieve effective communication and file-sharing services.

### **1.10.3. Economic Feasibility**

In the equipment selection process we have tried to consider that how we can get faster and better featured devices with the minimum amount of cost, this makes the project economically feasible. There are also some new devices and technologies that are currently owned by the institution this minimize the expenses. Economically one of the goals of this project is to make the institution beneficiary with the minimum possible cost.

Table 2: Items with their quantity and total Cost prices

No	Item	Quantity	Price
1.	Desktop Computers (dell 3020)	350	4,375,000
2.	Printers	4	124,000
3.	Cisco Switch /Distribution switch	4	5,899,124
4.	Cisco Router (core)	2	1,651,457
5.	Access switches	35	6,340,673.5
6.	Aruba (AP)	10	164000
7.	Server(Dell PowerEdge R840)	5	6,000,000
8.	48U Data Center Server Rack Cabinet	1	58700
9.	Biometrics (Finger Print)	3	20250
10.	Liebert-gxt-mt-plus-ups	1	352,500
11.	Cisco Firewall	1	929,750
12.	18U Cabinet	4	133,002.36
13.	Cat 6 UTP Cable	150roll	2,250,000
14.	cable trunket	750	300,000
15.	5000VA UPS	1	283,800

16.	18 inch PVC Pipe	500	550000
17.	Fire Extinguisher	2	4500
18.	Split Type air Conditioner	2	567,600
19.	Standby Diesel Generator	1	769337.2
20.	RJ 45 connector	1000	6000
21.	Fiber cable	130m	130,000
22.	Maintenance Toolkit	2	24,818
23.	Network Toolkit	4	13,728
24.	Female Port (Network)	500	10,730
	Total		30,958,970.06

#### **1.10.4. Political feasibility**

Due to the reason that the organization is a governmental organization, the government will benefit from this project in terms of minimizing the cost of the existing system, giving service to the customer effectively and a structured organizational data handling.

## **Chapter Two**

### **2. Network Analysis**

#### **2.1. Description of the Current Network**

Currently, DBPTC has a network connected with the Internet Service Provider (ISP) through copper cable network. It covers the administrative building/offices, computer labs partially and the library. In the main computer lab users can access wired as well as wireless network. There is no any dedicated data center for the network. The network is just for internet access service which is not manageable and structured.

The current network supports slow Internet access. Users have complained about occasional downtime and slow response times when accessing the network, especially at peak access times. At a minimum, DBPTC wishes to correct these issues through an upgrade to their system.

The existing network uses copper cable with cat 5 and older version of switch D-Link DGS-1024D model. They use DSL with 4 ports and 10 mbps bandwidth. The one port of DSL goes to a switch with 24 port located in the main Lab and they extend it to the neighboring offices and labs. The other port of the DSL goes to Distance office switch. The other two ports go to the dean office for two offices.

The current network structure in DBPTC has a flat connection among different buildings in a separate and unorganized manner; the network connection that is working on the compound is mainly used for printer connection due to the reason that there is a lack of enough new technology printers in the compound. This connection has also been used for online examination in an insecure way by using a personal computer as a server in the network; this has a problem with performance, security and speed. There are about 54 connected devices in the flat network connection and 12 other devices without even any connection. This flat network also consists of different low-level network devices and these are switches (dlink and 3com) with a 10MB connection. This makes the management and teaching-learning process insecure and inefficient.

## **2.2. The New Proposed Network**

The new network design tends to solve the problem faced by the college. The new system is a hierarchical data center-based network, Which is a data center-based network structure, in which the server is located in a central location “Datacenter” and other network devices are located in different levels of structures up to the client computer; where users share and access network resources. The dedicated computer controls the level of access that users have for resources. The server operating system is designed to handle the load when multiple client computers access server-based resources. This network implementation will have such benefits. The college will be able to manage the data of users easily, it also makes both hardware and software resources sharing process simple, and the network of the college secure by applying both detective(firewalls) and preventive security(backup critical information) controls.

This project provides guidelines and best practices for IP addressing and design for the device, selection of routing protocol based on the organization network topology and server farm access layer design. The network design has taken into consideration for IP address allocation, dynamic routing, and building data center.

## **2.3 Functional Requirements**

Functional requirement explains and describes the interaction between the network system and the users or in general with the environment. The network consists of the following the functional requirements:

- Allowing the users to access web services for browsing
- Allowing the users to access FTP, VOIP and e-mail services
- Allowing the users to access DHCP and DNS services
- Digital library, student registration system, finance system, online examination system and other local web services will be accessed quickly with better bandwidth
- Allows users to share files
- Allow to access fast file service from the file server
- Allow the staff members who have laptop computers use network access in office, cafeteria and green areas.
- Fast and efficient network connection

- Allowing system administrators to manage, control and maintain the network easily

## 2.4 Non Functional Requirements

The non-functional requirements deals with the quality of the network needed to be developed from different evaluation point of view like the response time of the network to a given user queries, and these requirements do not directly affect the performance of the network but they are nonetheless important.

**Availability:** The new proposed project makes the network available for the college community to access the service at any time and the network can provide services when they want to access it. The network is available 24 hours to provide a service to assure that the network uses some techniques and these are: Device redundancy and path redundancy.

**Performance:** Since our project focuses on a server-based network system, it has a growing value of data accessed by many users concurrently. It is the speed at which content is delivered to users and how responsive the system is. Processing time should take less than one second, over a reasonably common internet connection, speeds, the server should respond to client requests in less than one second.

**Redundancy:** In time of a particular device failure the network should continue its service for the user this can be assured by redundancy, in this mechanism each high level network devices has not only one path to transfer packets, the devices will be connected with each other, this makes the network on-work in time of failure of a network device.

**Scalability:** A network design should be implemented with consideration of a future change in the network without the interference of the existing network. This network design project is scalable in terms of adding more campus boundaries, service and user requirements to the network and also this network study is scalable in terms of subnet addressing when it adds a new component and service the network is simply extended.

**Security:** This Network design makes the local area network and data center secure; it can detect and prevent different attacks by using different detection and prevention techniques. There is some local area network security mechanism like protocols configuration, security policy, filtering and ACL (access control list). The network must support advanced security features such as Firewall, protocols, security policy, anti-virus, filtering, Application Detection, Email



security, DMZ (Demilitarize Zones) and Anti-Spam, and it provides all-around security protection to safeguard the efficient running of data center and local area network.

## **2.5. Network Requirements**

Network Requirement involves identifying initial network requirements based on goals, facilities, user needs, and so on. This section involves characterizing sites and assessing any existing networks and performing a gap analysis to determine whether the existing system infrastructure, sites, and the operational environment can support the proposed system. Network Requirement includes the following different sub-requirements.

### **2.5.1 User Requirements**

The network design should fulfill several needs of the user- that can be expanded to include everyone involved in the system, such as network and system administrators and management. The system should adapt to users and their environments provide quick and reliable information access and transfer and offer quality service to the user.

The institution consists different bodies such as students, teachers, office workers and managerial bodies; the network is implemented according to this organizational structure. For different member of the college, there are different VLANs configured so that different departments will have logically separated networks this is important to organize the network according to the organization's structure.

This indicates the following general requirements:

**Timeliness** is a requirement that the user can access, transfer, or modify information within a tolerable time frame.

**Reliability** is a requirement for consistently available service. Not only must the user be able to have access to system resources a very high percentage of the time, but the level of service to the user (in terms of application usage or information delivery) must be consistent.

**Adaptability** is the ability of the system to adapt to users' changing needs. Some examples of this are distance-independence and mobility. As users rely more and more on the network, they are becoming coupled to logical services and decoupled from physical servers. This decoupling

means that users do not have to care where servers are located, as long as they can get the services they need.

**Security** is a requirement to guarantee the confidentiality, integrity, and authenticity of a user's information and physical resources, as well as access to user and system resources.

**Scalability**- for future expansion of the network, making the network scalable is one of the requirements that should be fulfilled.

**Response time** is the time between the entry of a command or keystroke and the host system's execution of the command or delivery of a response. This should be possibly minimum to achieve the network users faster access needs.

## 2.5.2 Network device Requirements

We have selected and specified network devices since they are supported and widely accepted throughout the world, this includes the hardware and software requirements of the new network design; these equipment are basic and new equipment that are required to implement a hierarchical network design in the institution, which ranges from the end users PC to high capacity servers.

### 2.3.2.1. Hardware Requirements

Table 3: Hardware Requirements

No	Item
1.	Desktop Computers (dell 3020)
2.	Printers
3.	Cisco Switch /Distribution switch
4.	Cisco Router (core)
5.	Access switches

6.	Access Points
7.	Servers
8.	Firewall
9.	Fiber cable

#### 2.3.2.2. Software Requirements

The basic Software and applications used in this design are summarized in the below table:

**Table 4: Software Requirements**

No	Item	Versions
1	Windows 10	21H2
2	Windows Server	2019
3	Apache HTTP Server.	2.4.46
4	FortiGate	NGFW
5	FileZilla Server	3.56.2
6	Cisco IOS	15.9M

Beyond these basic applications there can be also other software which can be deployed and installed on the new network infrastructure, this can be divided in three major categories based on their requirement in terms of capacity, availability and interactivity, these applications makes the institution's educational and other activities facilitated.

### **Mission-critical application**

An application is mission-critical when it is essential to the operation. Mission-critical applications should not experience any downtime when end users are likely to utilize them.

These are:

- SIMS(student information management system)
- Staff Profile Management System
- HRMS
- Security control systems

### **Rate critical applications**

In terms of capacity, some applications require a predictable, bounded, or high degree of capacity. Such applications, termed here rate-critical applications, include voice, non-buffered video, and some tele-service applications (applications that provide a subset of voice, video, and data together to be delivered concurrently to groups of people at various locations.

- Video conferencing
- VoIP
- FTP over TCP

### **Real-time and interactive applications**

Real-time applications are those that have a strict timing relationship between source and destination, with one or more timers set for the receipt of information at the destination. <sup>[2]</sup> Information received after the timers expire at the destination is considered worthless and is dropped. The best example of this type of application is an online digital examination system.

### **2.5.3 Service Requirements**

**Internet service:** - it is a required service to provide internet access to the campus community to access information and resources over a network

**Ftp:** - it is also a required service for the campus community to send, receive and access large number of size files via the campus network.

**Email service:** - this Email service will also be required by DBPTC community to get email service.

**Printer sharing service:** - it is also a required service to share a common printer for different office

**Intra-office communication service:** - it is also a required service to share information between intra-office via online, gives ability to connect and interact with the outside environment.

**Voice over IP service:** - it is also a required service to make a call in the campus office by using IP telephones which use the network for connection.

**Video conference:** service for communicating users at different places in the compound or beyond through the video conference Application.

**Online student information management service:** - service to check or see the student's results through Portals, information management systems.

**Online repository service:** - service to store the institution's research, projects and other papers, Generally these services will be required in this network design for the campus community to provide service to the university community through the campus network.

## **2.5.4 Standard Requirements**

The networking standards ensure the interoperability of networking technologies by defining the rules of communication among networked devices. Networking standards exist to help ensure products of different vendors can work together in a network without the risk of incompatibility. Wireless devices need standards to communicate with other devices, this known as IEEE 802.11. 802.11 have different standards. Among these standards, the proposed network structure will use the IEEE 802.11a standards to support speeds of up to 54 Mbps in the 5 GHz band. Since the 2.4 GHz frequency band is heavily used by many users and appliances, moving to the 5 GHz band gives the advantage of less interferences, it also reduce the signal penetration through walls and foliage compared to 802.11b.

## **2.5.5 Protocol Requirements**

- **Routing protocols:** - it is used to route the network and communicate router with each other, which means it chooses the best and shortest path to deliver packets to the intended destination. It also has a function of distributing information that enables them to select

routes between any two nodes on a computer network from the routing protocols definition.

- **Security protocols:** - Network security protocols are primarily designed for this network design to prevent any unauthorized user, application, service or device from accessing network data by applying different security protocols those protocols are Secure File Transfer Protocol (SFTP), Secure Hypertext Transfer Protocol (HTTPS), and Secure Socket Layer (SSL) and secure socket shell (SSH).
- **VLAN protocols:** - a **VLAN trunking protocol** is a type of virtual LAN protocol that is used to propagate the definition of Virtual Local Area Networks (VLAN) on the whole local area network. Using VTP Switch advertises the following on its trunk ports are:- Management domain, Configuration revision number and Known VLANs and their specific parameters
- **DHCP** (dynamic host configuration protocols):- it is widely used in LAN environments to dynamically assign host IP addresses from a centralized server, which significantly reduces the overhead of administration of IP addresses. DHCP also helps conserve the limited IP address space because IP addresses no longer need to be permanently assigned to hosts
- **IP (internet protocols):**-This protocol also will require assigning specific IP addresses for each and every network device to communicate through the whole network structure.
- **DNS (domain name service):**-This protocol is used to resolve the college's user queries using the domain namespace and resource records it maintains in its zone database files and these servers maintain the databases that store resource records and information about the domain namespace structure as well as used to resolve IP address with the domain name.
- **SMTP (simple mail transfer protocols):**- this protocol will configure on a server to provide mail service to the college's community, so this network design also configures these protocols to the campus network to provide email service.
- **Ftp (file transfer protocols):**-This protocol is used to access a directory and sub-directories so the college community can connect to this server with an FTP client. File transfer protocols configuration on the network creates better intra-office communication

it enables user to share files remotely without using other removable hard drives for data sharing purpose.

### **2.5.6 Wireless LAN Requirements**

A WLAN transmits information over radio waves. Data is sent in packets. The packets contain layers with labels and instructions that, along with the unique MAC (Media Access Control) addresses assigned to endpoints, enable routing to intended locations.

Identifying which services and applications the WLAN must support is a key to building a robust, relevant, scalable and sustainable architecture. It is strongly urged to consider the several elements such as type of application being utilized, total bandwidth requirements, throughput requirements and security of end devices.

The essential hardware network device which is required for wireless network is the Access point. An access point (AP) is a device that creates a wireless local area network (WLAN). Access points are essential components of a wireless network's infrastructure. They project a Wi-Fi signal to a specific area,

## Chapter Three

### 3. Network Architecture

#### 3.1. Introduction

The network architecture guides the technical design of the network by applying sets of high-level design principles. Such high-level design principles act upon the building blocks of the network to develop overall structure and function. This section includes the relationships within and between major architectural components of the network, such as addressing and routing, network management, performance, and security.

#### 3.2. Network Topology

The choice of a topology for a network is influenced by several factors, the most important being the size and scale of the network as well as cost. However, long-term factors including configuration management, monitoring, and general performance also need to be considered. The topology for this LAN network is selected by considering network operational and maintenance costs, Increase network performance, optimal network health by the effective allocation of resources, and troubleshoot errors faster.

To get multiple functions from multiple topologies this infrastructure is designed by using the Mesh-Star hybrid network topology, this makes the network redundant in the high-level hierarchies, simple and center based in the lower (access) Layers.

Among several Structural topologies, the most common and well efficient is Star Topology which is used in the lower-level layer of the network structure. A star topology is the one in which each peripheral node is connected to a central hub or switch. It is probably the most commonly used network topology for LAN because it is considered the easiest topology to design and implement.

In this hybrid topology, the other topology used is the mesh topology; Mesh topology is a type of networking where all nodes cooperate to distribute data amongst each other. The Mesh system which is applied in the higher layers usually relies on a *routing table*, which tells every node how to communicate with the access point, and how a node should direct traffic that is trying to go somewhere. The routing table assumes that there is no direct communication anywhere in the



network except by nodes that have a route to the access point. This helps to make the network infrastructure redundant and available in time of failure of a network device or a cable.

### 3.3. Technologies

Building a local network mainly depends on the network technologies that it uses. Network technologies enable the network to have a capability of access different service for users easily and in a better performance, these technologies can be identified by several aspects of networking.

#### 3.3.1. Performance

Performance of a network pertains to the measure of service quality of a network as perceived by the user. There are different ways to measure the performance of a network, depending upon the nature and design of the network. The characteristics that measure the performance of a network are Bandwidth, Throughput, and Latency (Delay).

This network design project assures the network performance by using some techniques which means that there are some mechanisms to improve the network performance through VLAN (Broadcast domain limitation), link aggregation or redundancy, physical topology design and network device redundancy.

The following are devices that are used to enhance the performance of the network:

**A. Fiber Optic cable:** A fiber optic cable is a network cable that contains strands of glass fibers inside an insulated casing. They're designed for long-distance, high-performance data networking, and telecommunications. Compared to wired cables, fiber optic cables provide higher bandwidth and transmit data over longer distances. It supports a higher capacity. The amount of network bandwidth a fiber cable can carry easily exceeds that of a copper cable with a similar thickness. Fiber cables rated at 10 Gbps, 40 Gbps, and 100 Gbps are standard.

**B. Gigabit Ethernet (GbE):** a transmission technology based on the Ethernet frame format and protocol used in local area networks (LANs) provides a data rate of 1 billion bits per second, or 1 gigabit (GB). Gigabit Ethernet networks can function as half-duplex networks for shared media or as Ethernet switches with a switched full-duplex network.

**C. Wireless LAN:** uses high-frequency radio signals, infrared beams, or lasers to speak between the workstations, file servers, or hubs. Wireless LAN is formed by connecting different devices through wireless communication to form an area network. WLAN follows a typical named IEEE 802.11. WLAN gives a high data transfer rate. It uses a star during which all nodes send/receive data through access points. It works better in small LAN areas. Especially in offices no extra cables are required and arranging a gathering is additionally easy. It has a transfer rate of 1-10 Mbps. Wireless LAN uses security that incorporates WEP or WPZ. It also uses infrared technology if required.

**D. Link Aggregation:** - network performance can be improved through combining multiple network connections in parallel in order to increase throughput beyond a single connection could sustain and to provide redundancy in case one of the link should fail.

### **3.3.2. Security**

Network Security is vital in protecting client data and information, keeping shared data secure and ensuring reliable access and network performance as well as protection from cyber threats. A well-designed network security solution reduces overhead expenses and safeguards organizations from costly losses that occur from a data breach or other security incident.

#### **A. Firewall**

Firewalls control incoming and outgoing traffic on networks, with predetermined security rules. Firewalls keep out unfriendly traffic. Network Security relies heavily on Firewalls, and especially Next-Generation Firewalls, which focus on blocking malware and application-layer attacks.

Among the different types of hardware firewalls, the Packet-filtering firewalls type is installed on the new server. Packet-filtering firewalls create a checkpoint at a traffic router or switch. The firewall performs a simple check of the data packets coming through the router inspecting information such as the destination and origination IP address, packet type, port number, and other surface-level information without opening up the packet to inspect its contents. If the information packet doesn't pass the inspection, it is dropped.

The good thing about these firewalls is that they aren't very resource-intensive. This means they don't have a huge impact on system performance and are relatively simple.

## **B. Intrusion Prevention Systems (IPS)**

IPS technologies can detect or prevent network security attacks such as brute force attacks, Denial of Service (DoS) attacks and exploits of known vulnerabilities. A vulnerability is a weakness for instance in a software system and an exploit is an attack that leverages that vulnerability to gain control of that system. When an exploit is announced, there is often a window of opportunity for attackers to exploit that vulnerability before the security patch is applied. An Intrusion Prevention System is used in these cases to quickly block these attacks.

## **C. Physical security controls**

Physical security of a data center comprises various kinds of built-in safety and security features to protect the premises and thereby the equipment that stores critical data. For the safety and security of the premises, factors ranging from location selection to authenticated access of the personnel into the data center should be considered, monitored, and audited vigorously. These are the specific elements of physical security controls, especially in the data center room:

- closed-circuit television (CCTV) camera surveillance with video retention as per the college policy
- Fire protection systems with double interlock. On actuation of both the detector and sprinkler, water is released into the pipe. To protect the data and information technology (IT) equipment, fire suppression shall be with a zoned dry-pipe sprinkler.
- Cable network through a raised floor, which avoids overhead cabling, reduces the heat load in the room and is aesthetically appealing.
- Protect all access via electronic Access Control Systems (ACS). These systems include fingerprint readers, Two-factor authentication with access cards and passwords.

### **3.3.4. Network management**

Network management is the process of administering, managing, and operating a data network, using a network management system. Modern network management systems use software and hardware to constantly collect and analyze data and push out configuration changes for improving performance, reliability, and security.

The system manages network devices such as switches, routers, and access points; it typically uses a centralized server to collect data from network elements.

**Simple Network Management Protocol (SNMP)** services are commonly used to identify problems and alert the appropriate IT manager. These tools also report and record issues that IT managers can analyze for trends, which can yield important insights into longer-term issues that can be addressed to improve performance. This provides network devices (routers, printers, servers, etc.) with a common language for sharing information with a network management system.

The purpose of this technology is to continually monitor and manage the health of network devices across an organization. Managing the health of network devices is necessary to ensure all applications and services which, employees and customers are using are working properly.

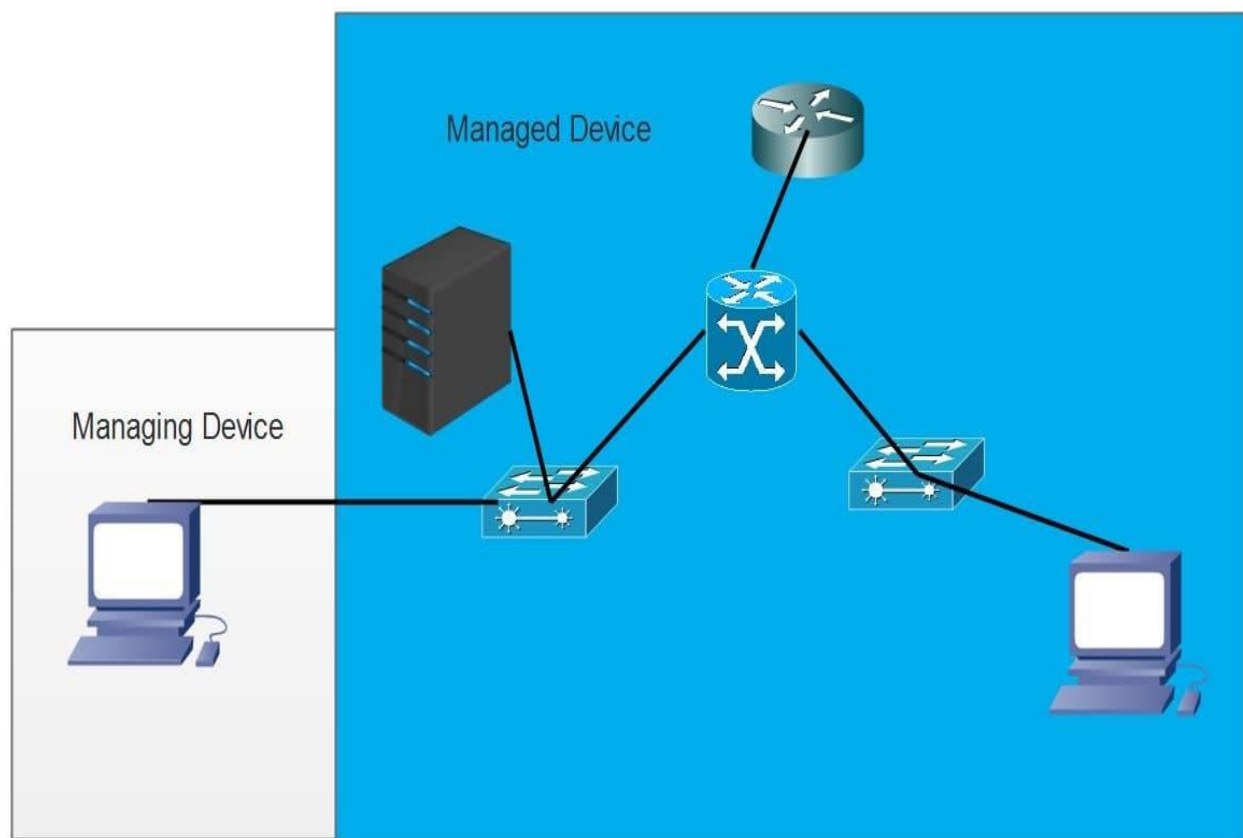


Figure 3: Network Management Architecture

### 3.4. Equipment Class

Network devices are intended and designed to have different features and functions, these functions can be a general function that should be included in all equipment classes, there are especially high-class equipment, and these equipment are expensive in cost and advanced type of network devices. For this network design, several factors are considered to select each network device. The general factors that are considered are Cost, speed and types of ports, and support for different services.

Cost is typically one of the most important factors when selecting equipment. The cost of a switch or router is determined by its capacity and features. The device capacity includes the number and types of ports available and the backplane speed. Other factors that impact the cost are network management capabilities, embedded security technologies, and optional advanced switching technologies. The expense of cable runs required to connect every device on the network must also be considered.

The other main factor is Speed and Types of Ports/Interfaces, Choosing the number and type of ports on a router or switch is a critical decision. Questions to be asked include: “Do we order just enough ports for today's needs, or do we consider growth requirements?”, “Do we require a mixture of UTP speeds?”, and “Do we require both UTP and fiber ports?”

Depending on the version of the operating system, a network device can support certain features and services, such as: Security, QoS, VoIP, Layer 3 switching, NAT, DHCP.

There are also specific equipment class features that are included in different equipment classes, below are the different network devices and their features that are considered to select for this network infrastructure.

#### Switch

- **Mix-and-Match Switch Types:** should be compatible with different other types of switches in terms of ports and model of the devices
- **Integrated Wireless LAN Controller:** should deliver improved operating efficiency and WLAN security, mobility, and ease of use for business-critical wireless LANs
- **Smart Multicast:** greater efficiency for multicast applications such as video.

- **Network Security:** should support a comprehensive set of security features for connectivity and access control, including ACLs, authentication, port-level security, and identity-based network services
- **IPv6 Support:** should support IPv6 routing in hardware for maximum performance. As network devices grow and the need for larger addressing and higher security becomes critical, the switch will be ready to meet the requirement.

## Router

The general functions that must be fulfilled on core layer routers are security, voice, high availability, IP Routing and Multicast, Quality of Service (QoS), IP Mobility, and Multiprotocol Label Switching (MPLS), VPNs, and embedded management. There are also other device dependent future which are:

- **Services Integration:** offer increased levels of services integration with voice, video, security, wireless, mobility
- **High performance with integrated services:** powered by high-performance multi-core processors that can support the growing demands of high-speed WAN connections
- **Energy efficiency:** provides energy-saving features that include intelligent power management, High-efficiency power supplies.
- **Network Agility:** should offer increased capacity and performance as the network needs to expand.
- **Wireless and Mobility Services:** enable deployment of secure, manageable wireless LANs (WLANs) optimized for remote sites and branch offices, including fast secure mobility, survivable authentication, and simplified management.
- **Integrated Gigabit Ethernet Ports:** should include all onboard WAN ports are 10/100/1000 Gigabit Ethernet WAN routed ports.
- **Innovative Universal-Serial-Bus (USB)-Based Console Access:** A USB console port offers management connectivity for devices without a serial port such as modern laptop computers.

### **3.5. Addressing**

The fundamental goal of an IP addressing scheme is to ensure network devices are uniquely addressed. IP Address Schemes are a fundamental part of any network's security architecture and should support network separation and segregation. There are some techniques to assist in separating and segregating network elements. It is also useful to consider how to segregate and control network traffic through defined network perimeters and boundaries, and defined network traffic rules.

Due to the capacity of users this network uses the class b network that ranges from 128 to 191, which has 16 bits for each address (network address and host address). This class is used in networks that are relatively medium sized number of users. The network address is also divided to 5 sub-networks for manageability purposes.

### **3.6. Routing**

A routing protocol specifies how routers communicate with each other, distributing information that enables them to select routes between any two nodes on a computer network. Among the different routing protocols (EIGRP, OSPF, RIP) this network design uses the OSPF routing protocol, this protocol is selected for some reasons. It has faster convergence and is more efficient in using bandwidth; therefore, it can reduce its packet loss. OSPF has a higher throughput compared to other protocols. The main advantage of the OSPF (Open Shortest Path first) is that it handles the error detection by itself and it uses multicast addressing for routing in a broadcast domain.

## **Chapter Four**

### **4. Design phase**

#### **4.1. Introduction**

This phase involves designing the network according to the initial requirements determined in the plan phase, incorporating any additional data gathered during network analysis.

Logical network design is a virtual implementation of the real system. It is the shadow of real facts in the networking service. It includes the physical arrangement of network devices and their logical interconnection. This section covers the network design for the DBPTC network. The network design is designed based on the hierarchical network architecture with the datacenter approach. This approach is used so that the network meets current business and technical requirements and incorporates specifications to support availability, reliability, security, scalability, and performance. This design specification provides the basis for the implementation activities.

#### **4.2. Network design**

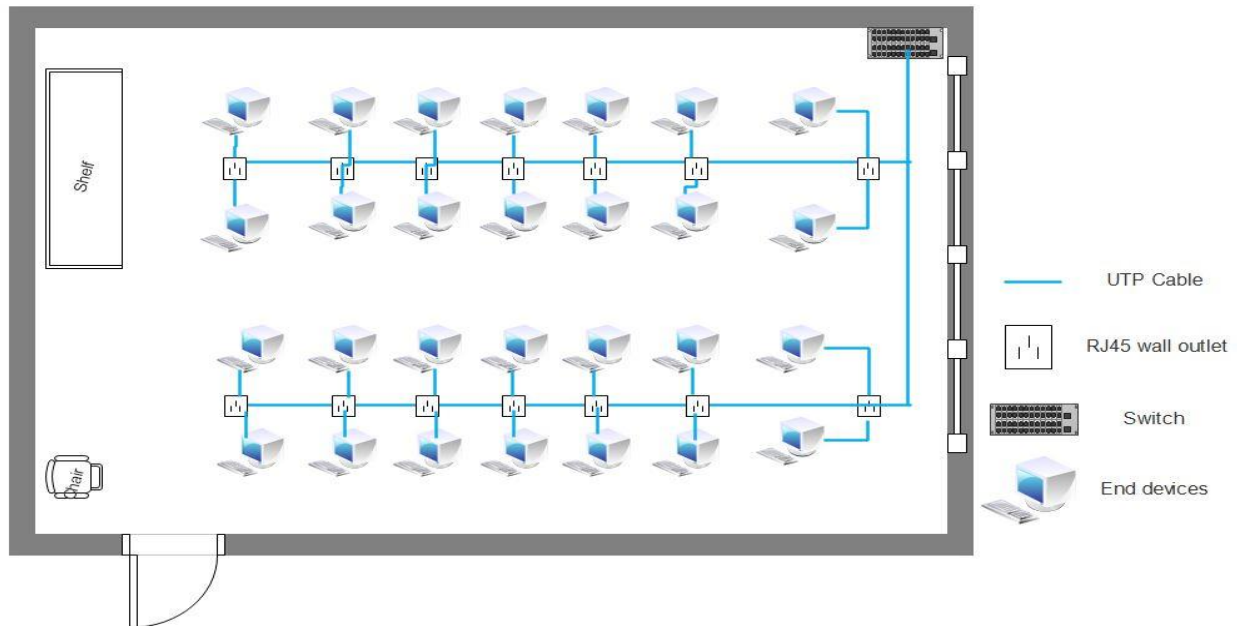
The whole network design is usually represented as a network diagram that serves as the blueprint for implementing the network physically. Typically, network design includes the following:

- The internal structure of a Network on different types
- Logical map of the network to be designed in the college environment
- Cabling structure
- Quantity, type and location of network devices (router, switches, servers)
- IP addressing structure
- Network security architecture and overall network security processes



### 4.2.1. Physical design

The physical design includes the physical device and the cable connection between them, it also includes elements like workstations, servers, routers, and switches while the lines between these elements represent cable connections, below are a sample of different type of floors which are found in the college with their physical network topology.



#### Figure 4: Physical network design for Library

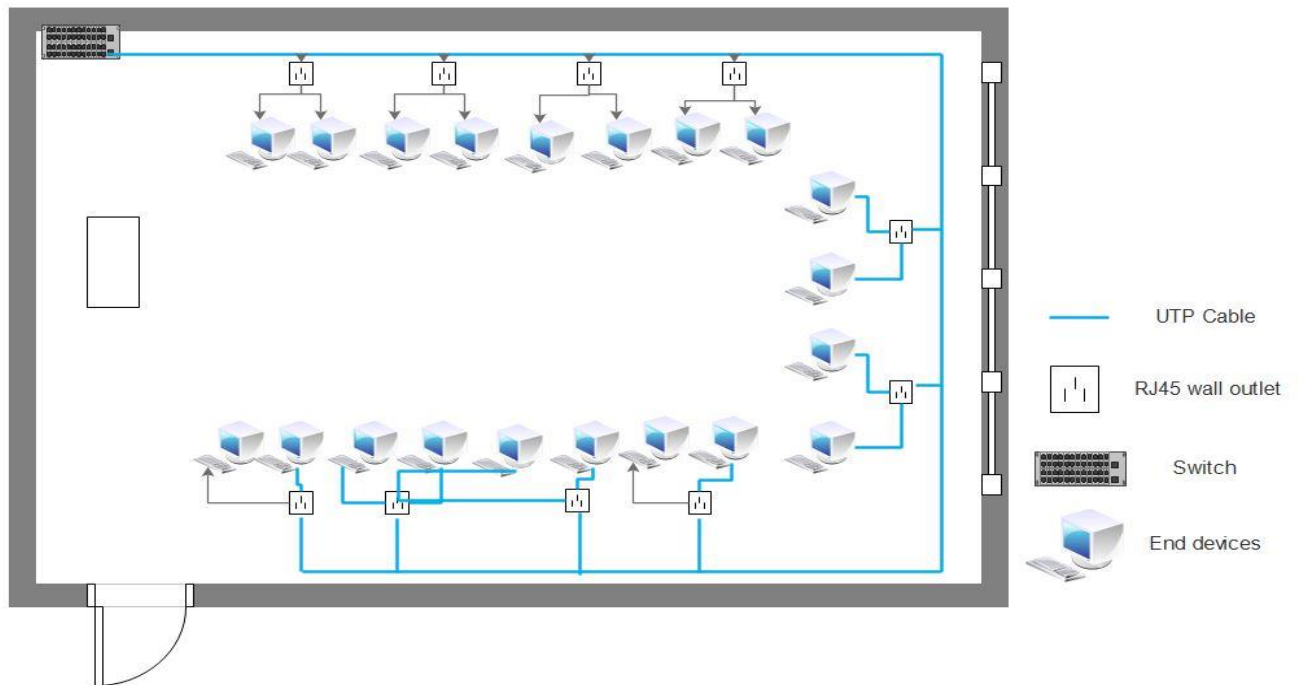


Figure 5: Physical network design for LABs



Figure 6: Physical network design for Offices

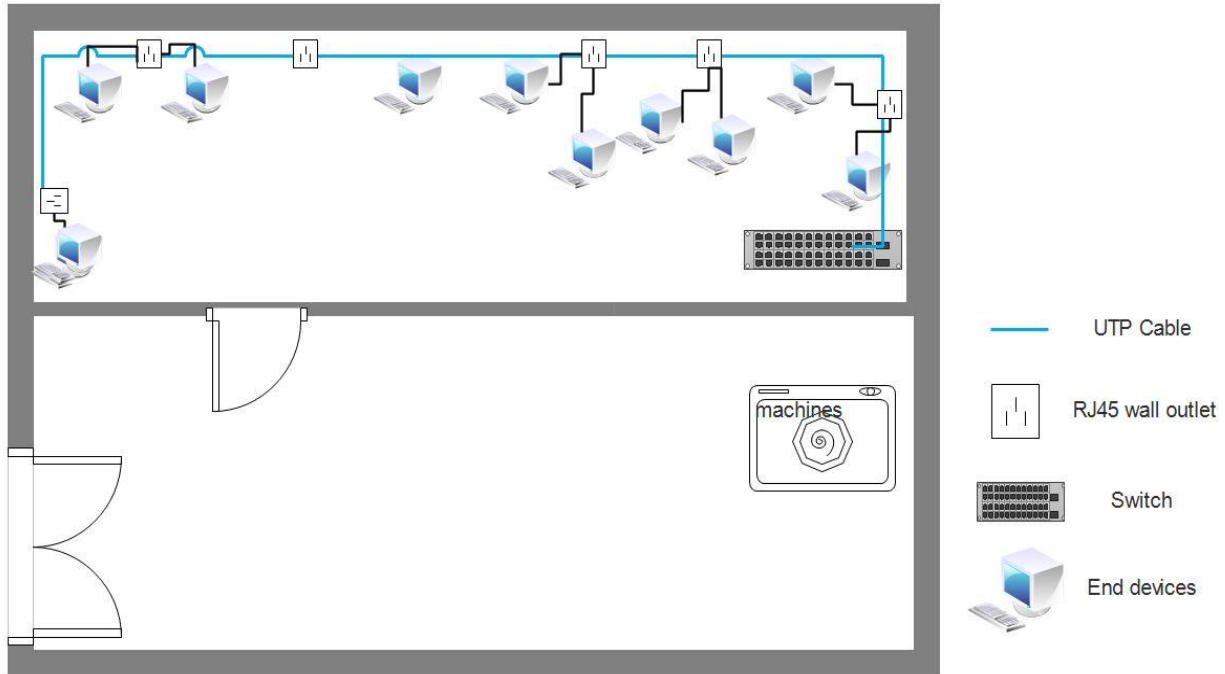


Figure 7: Physical network design for Workshops

### 4.3. Data Center design

A data center consists of hardware such as server racks and power distribution units, software such as server operating systems and network monitoring tools. The responsibilities of a data center are to provide computational power, network of computers, storage devices, cooling system and applications that are essential to aid an enterprise business <sup>[3]</sup>. Data center is an integrated environment with all kinds of necessary subsystems or modules. Modular design allows creating highly complex data center system from smaller and more manageable modules. These small modules are easier to be defined and can be easily managed. The installed technologies used in this concept are modular anywhere it is possible.

Above all, the following technologies and components are concerned:

- Racks
- Network connectivity infrastructure
- Security measures and appliances
- Monitoring structures

- Modular UPS
- In-row cooling unit
- Hot aisle containment

Through this concept, it is possible for staged construction by installing just a part of the data center to meet the current needs and expanding smoothly for future needs. Another effect would be the possibility to reach higher efficiency at partial loading by means of shutting down unnecessary modules.

The necessary modules which must be included in the data center infrastructure are:

- **Security**

Physical security is necessary to be built up for data center protection. It should be able to prevent unauthorized people entering to the Data Center. It comprises various kinds of built-in safety and security features to protect the premises and thereby the equipment that stores critical data. For the safety and security of the premises, factors ranging from location selection to authenticated access of the personnel into the data center should be considered, monitored, and audited vigorously.

- **Flexible Expansion**

In the cloud computing era, data centers should be able to expand flexibly as business and requirements grows. Scalability of the data center is the flexibility to construct and expand using simple, repeatable processes and components that can easily adjust to handle increased traffic or new devices without impacting the functioning of business operations, workflows or enterprise applications.

- **Low Total Cost of Ownership**

As energy being more and more expensive, power consumption of data center becomes the biggest part of operation expense. How to reduce power consumption should be considered during data center design. Conserving energy by using power saving equipment is one of the common mechanisms to minimize power usages. When purchasing new servers it is recommended to look for products that include variable speed fans as opposed to a standard constant speed fan for the internal cooling component. With variable speed fans it is possible to deliver sufficient cooling while running slower, thus consuming less energy.

Most data center equipment uses internal or rack mounted alternating current/direct current (AC-DC) power supplies. Using higher efficiency power supplies will directly lower a data center's power bills and indirectly reduce cooling system cost and rack overheating issues.

## Architecture Design

The conceptual architecture design of the proposed data center site is shown below.

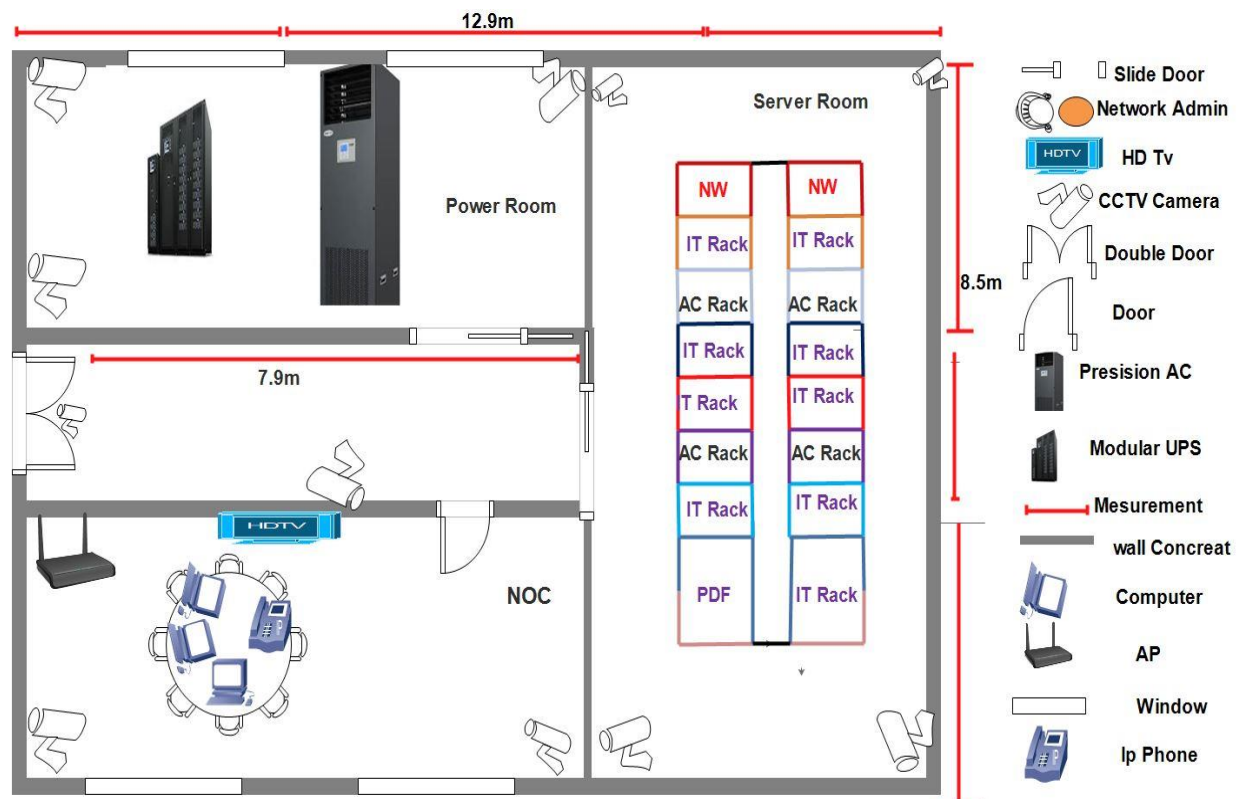


Figure 8: Physical design for Data center

## Data Center Layout Plan

The above picture shows the layout of the main equipment in the data center. The data center is divided into 3 rooms the NOC, Power room and data center room. The NOC room consists of IP phone, 65 inch UFHD LCD TVs and Aps. The power room consists mainly precision AC and Modular UPS. In the Data Center room there are two containments, the first containment consists

of 8 Racks with 6 IT Racks and 2 In Row AC Racks, the Second Containment consists of also 8 Racks with 2 Network Racks, 2 In Row AC Racks and 6 IT Racks.

The Data center building process also take consideration about the Cabinet System, Interior Decoration, Flooring, Ceiling, Wall painting, Wall Skirting, Light and Emergency Light, Door, Blocking of openings and windows, Aisle Containment Structure and other aspects to make the data center at its highest functionality.

The following figure shows the basic modular high level data center view.

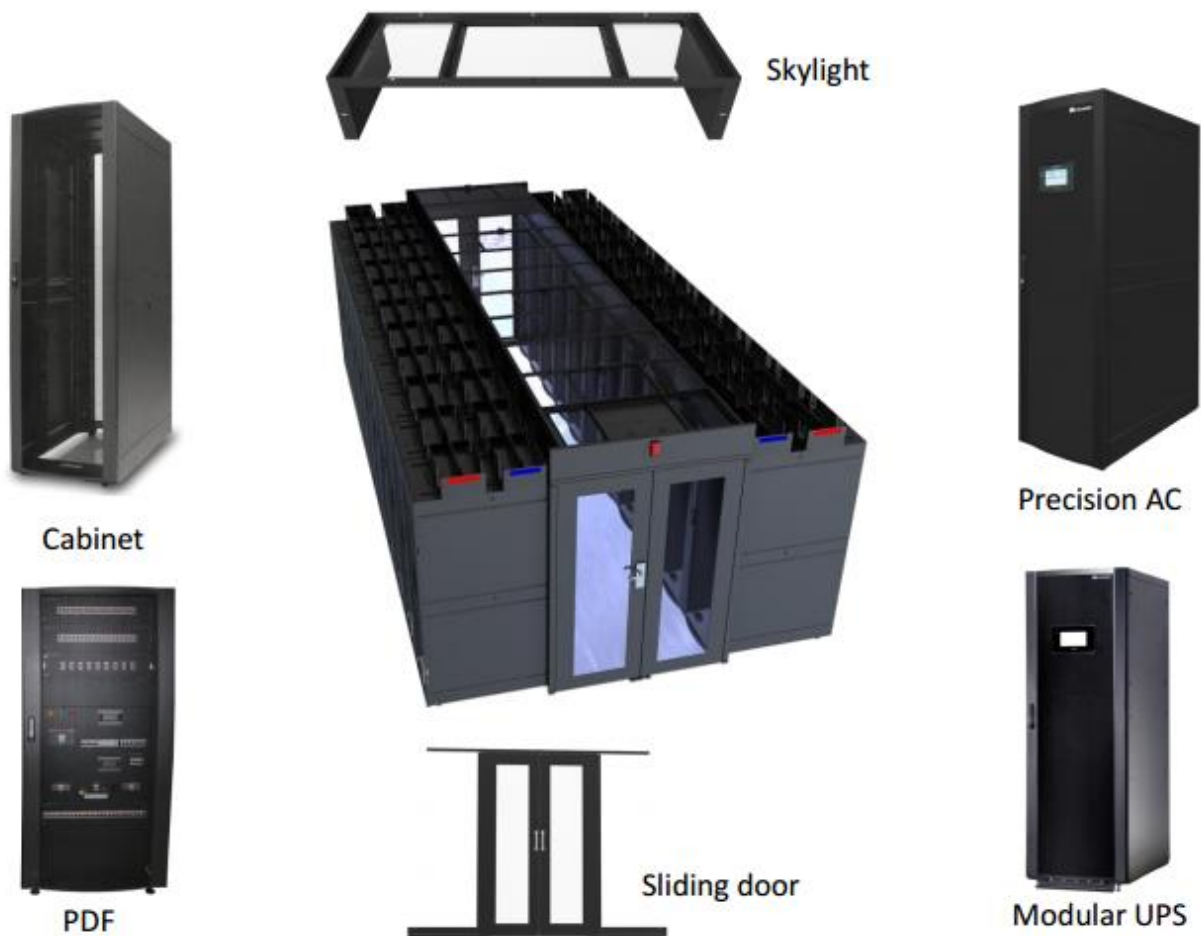


Figure 9: Components of data center

## 4.4. Network Design Topology

### Hierarchical network design

Hierarchical network design is a network design approach that has three-tier architecture. Most of the time hierarchical network designs are called top-down network designs because of that their architecture flows down from the narrower core to the wider access layers. In networking, a hierarchical design is used to group devices into multiple networks. The networks are organized in a layered approach. The hierarchical design model has three basic layers

**Core layer:** The Core layer provides a high-speed connection between the access layer, distribution and the data server and edge distribution. Redundancy is implemented to ensure a highly available and reliable backbone. The core layer includes one or more links to the devices to support the internet, virtual private networks (VPN), extranet, and WAN access.

This layer includes

Technologies used at the core layer include the following:

- Routers or multilayer switches that combine routing and switching in the same devices
- Redundancy and load balancing
- High-speed and aggregate links

**Distribution layer:** The distribution layer provides access between workgroups and the Core layer. Routing is implemented in this layer. This layer controls access to services by implementing filters or access lists. Redundant switches and redundant links to both the access and backbone are also implemented on this layer. The following are critical functions implemented on this layer:

- Filtering and managing traffic flows.
- Enforcing access control policies.
- Summarizing routes before advertising the routes to the Core.
- Isolating the core from access layer failures or disruptions.
- Routing between access layer VLANs.

**Access layer:** The Access layer, located within a campus building, aggregates end-users from different workgroups and provides uplinks to the building distribution layer. This contains all the devices to allow authorized users in the building to access the network. This includes end-user devices, such as workstations as well as devices to interconnect the end-users to the services they require. This layer provides important services, such as broadcast suppression, protocol filtering, network access, IP multicast, and quality of service. Due to this, it can connect IP telephones, video cameras and videoconferencing systems. <sup>[4]</sup>

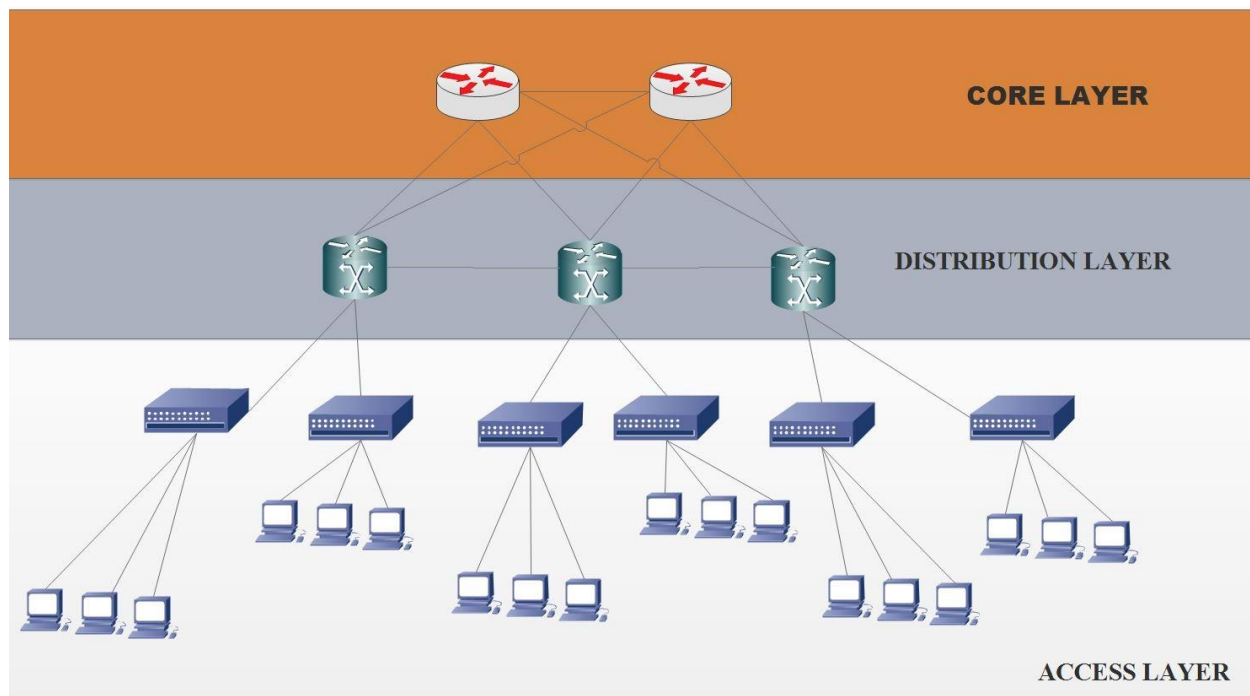


Figure 10: Hierarchical Network Structure



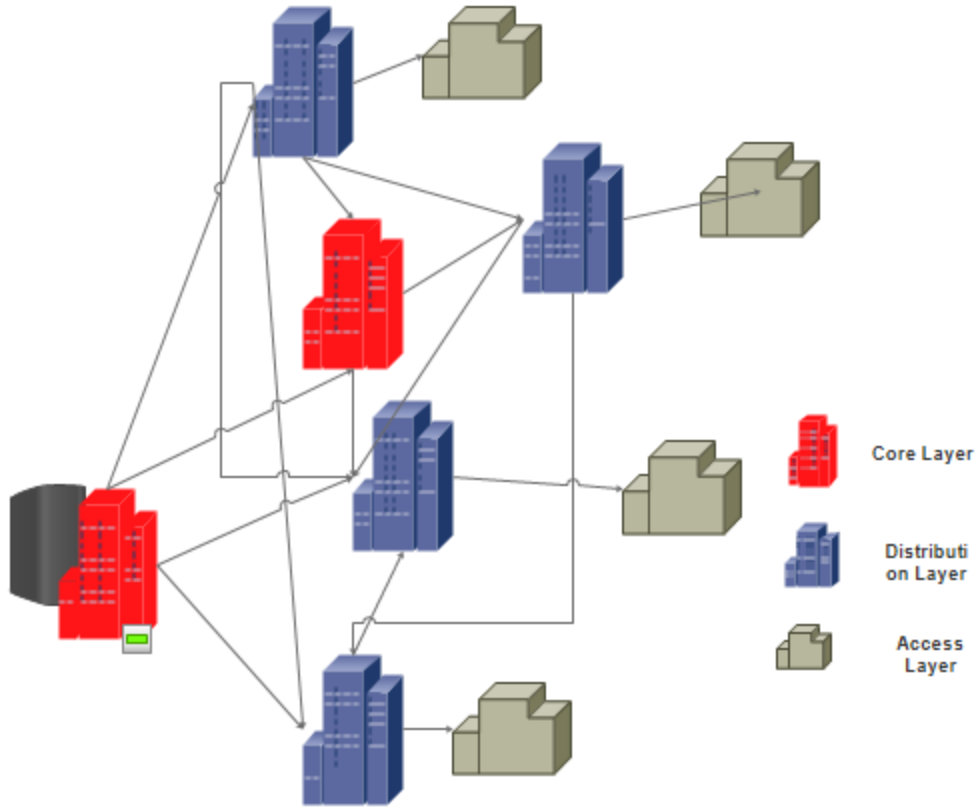


Figure 11: Hierarchical Network Structure in DBPTC compound (Logical Design)

## 4.5. IP addressing schema

By considering the number of users determined from the requirement analysis we have used the following class B network. Before the subnetting process, the network address that is used by this campus network is 175.10.0.0. This address is divided and sub-netted to several sub-networks and VLANs and distributed and assigned to each network device and equipment in the college compound.

The IP address is divided according to the placement of the buildings in the compound and the organizational structure of the college the network is divided in to 5 networks, each network is working on places where the buildings are densely placed in one environment. The total number of interfaces on the router that are connected are also taken to consideration.

Table 5: Sub-networks with their information

Net. Add	Valid Host Range	Broadcast Address	Subnet mask	CI DR	No of hosts
175.10.0.0	175.10.0.1 – 175.10.15.254	175.10.15.255	255.255.240.0	20	4094
175.10.16.0	175.10.16.1 – 175.10.19.254	175.10.19.255	255.255.252.0	22	1022
175.10.20.0	175.10.20.1 – 175.10.23.254	175.10.23.255	255.255.252.0	22	1022
175.10.24.0	175.10.24.1 – 175.10.25.254	175.10.25.255	255.255.254.0	23	510
175.10.26.0	175.10.26.1 – 175.10.26.2	175.10.26.3	255.255.240.252	30	2

## Switch allocation

Sample switch allocation for B-23 building: Switch name: ASL1 IP address: 175.10.16.0/22

Table 6 Sample switch allocation

Interface /sub interface	speed	VLAN
Fastethernet0/1	100mbps	Student_vlan
Fastethernet0/2	100mbps	Student_vlan
Fastethernet0/3	100mbps	Student_vlan
Fastethernet0/4	100mbps	Student_vlan
Fastethernet0/5	100mbps	Student_vlan
Fastethernet0/6	100mbps	Student_vlan
Fastethernet0/7	100mbps	Student_vlan
Fastethernet0/8	100mbps	Office_vlan
Fastethernet0/9	100mbps	Office_vlan
Fastethernet0/10	100mbps	Office_vlan
Fastethernet0/11	100mbps	Office_vlan
Fastethernet0/12	100mbps	Office_vlan

Fastethernet0/13	100mbs	Office_vlan
Fastethernet0/14	100mbs	Office_vlan
Fastethernet0/15	100mbs	Office_vlan
Fastethernet0/16	100mbs	Student_vlan
Fastethernet0/17	100mbs	Student_vlan
Fastethernet0/18	100mbs	Student_vlan
Fastethernet0/19	100mbs	Student_vlan
Fastethernet0/20	100mbs	Student_vlan
Fastethernet0/21	100mbs	Student_vlan
Fastethernet0/22	100mbs	Student_vlan
Fastethernet0/23	100mbs	Student_vlan
Fastethernet0/24	100mbs	Student_vlan
Fastethernet0/25	100mbs	Student_vlan
Fastethernet0/26	100mbs	Student_vlan
Fastethernet0/27	100mbs	Student_vlan
Fastethernet0/28	100mbs	Student_vlan
Fastethernet0/29	100mbs	Student_vlan
Fastethernet0/30	100mbs	Student_vlan
Fastethernet0/31	100mbs	Student_vlan
Fastethernet0/32	100mbs	Student_vlan
Fastethernet0/33	100mbs	Student_vlan
Fastethernet0/34	100mbs	Student_vlan
Fastethernet0/35	100mbs	Student_vlan
Fastethernet0/36	100mbs	Student_vlan
Fastethernet0/37	100mbs	Student_vlan
Fastethernet0/38	100mbs	Student_vlan
Fastethernet0/39	100mbs	Student_vlan
Fastethernet0/40	100mbs	Student_vlan
Fastethernet0/41	100mbs	Student_vlan
Fastethernet0/42	100mbs	Student_vlan

Fastethernet0/43	100mbps	Student_vlan
Fastethernet0/44	100mbps	Student_vlan
Fastethernet0/45	100mbps	Student_vlan
Fastethernet0/46	100mbps	Student_vlan
Fastethernet0/47	100mbps	-
Fastethernet0/48	100mbps	-

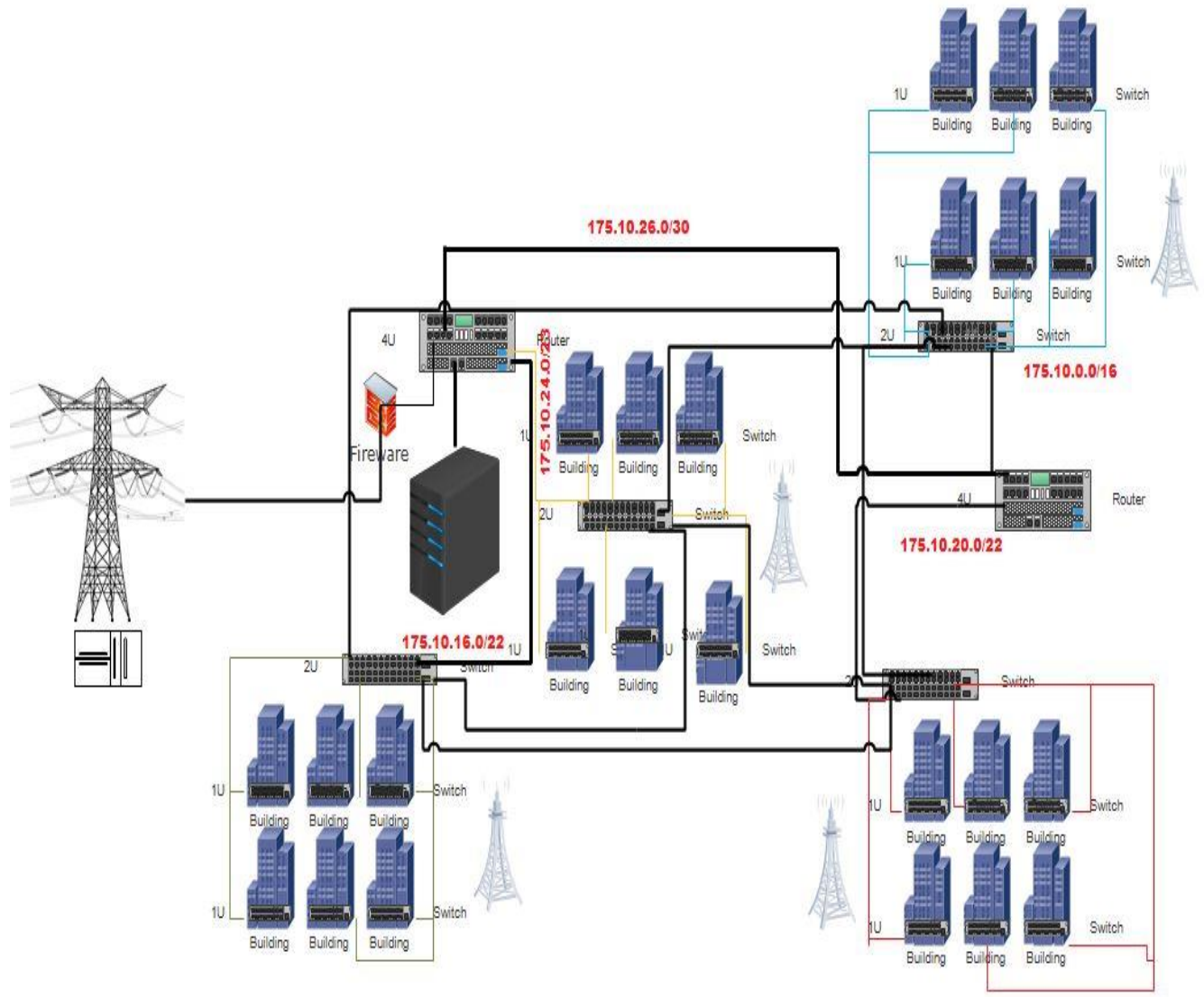
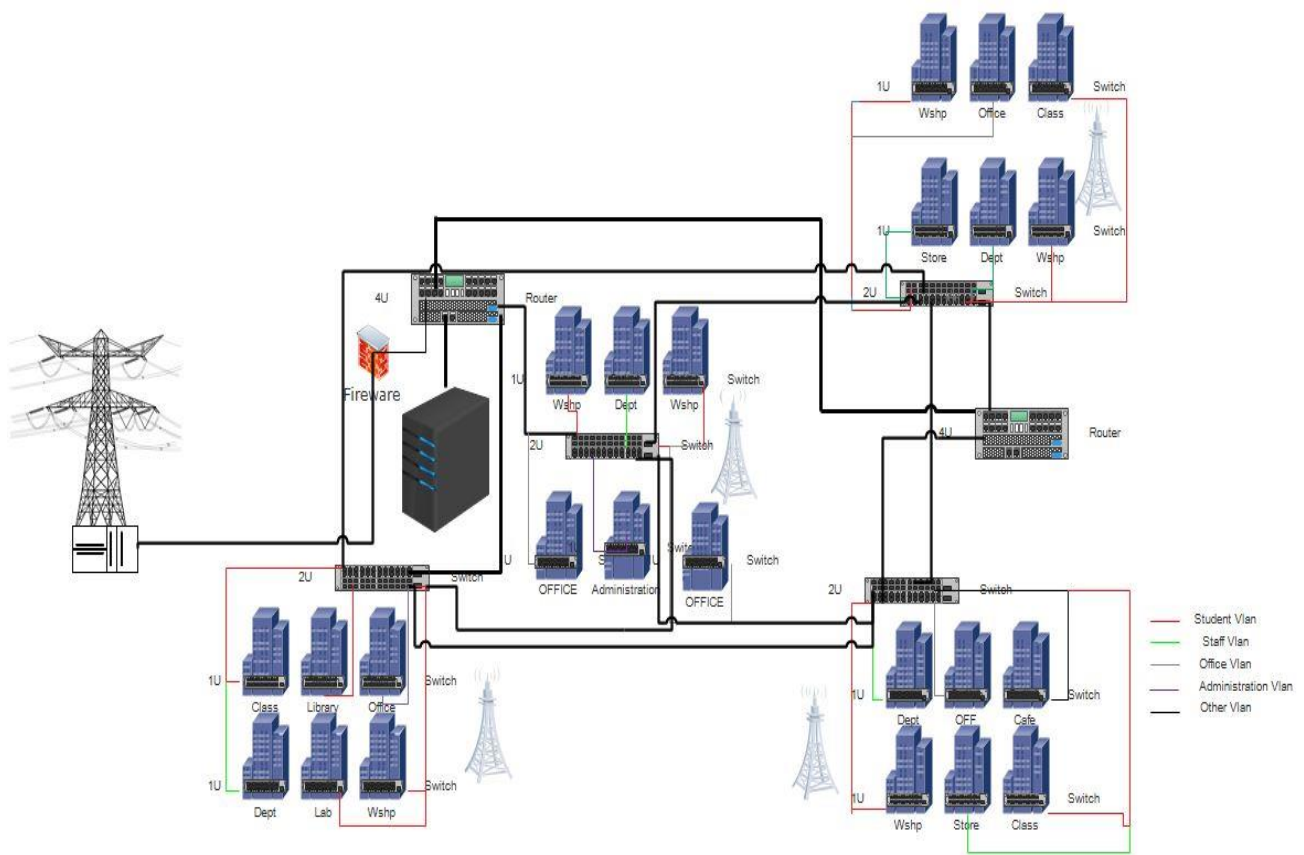


Figure 12: Logical design for IP design and sub-networks

## 4.6. VLAN design

VLANs can be used to create broadcast domains that eliminate the need for expensive routers. Periodically, sensitive data may be broadcast on a network. In such cases, placing only those users who can have access to that data on a VLAN can reduce the chances of an outsider gaining access to the data.

The VLAN is divided according to the managerial and departmental structure of the college; this helps the network structure to be manageable and simple, the network is logically divided into 5 VLANs. Each group contains about 2000 hosts. These groups of VLANs are Managerial, Office, Staff, Students, and Others. This logical separation of the network has an important role in securing sensitive information which has to be hidden from the rest user of the network, it is also used to control network traffic, and ease administration.



**Table 7: VLANs with their purpose**

VLAN ID	VLAN Name	Purpose
VLAN-10	Student_VLAN	To control and manage devices that are used by students which are found in (LABs, classes, Workshops, and Library)
VLAN-20	Staff_VLAN	To control and manage devices which are used by Teachers and Lab assistants found in (Department and Stores)
VLAN-30	Office_VLAN	To control and manage devices that are used to work office tasks in offices
VLAN-40	Mangerial_VLAN	To control and manage devices exclusively in managerial and administration offices
VLAN-50	Others_VLAN	For different miscellaneous purposes such as cafeteria, guests

#### **4.7. Security design**

Implementing a security control system on networks is vital to make the network secure and protect data and information on the network. The security design must take into consideration supporting different security dimensions. And these can be Access control, Authentication, Non-repudiation, Data confidentiality, Communication Security, Data integrity, availability, and privacy. The security design in this project includes security standards that are currently effective and efficient. The network is designed to have a strong firewall that prevents any outside connections not explicitly authorized by the college, mandatory authentication to access any workstation and isolation of the VLAN for organizational streams.

In this project we also use different security mechanisms to ensure safe security of DBPTC local area network such as protocols configuration, security policy, filtering, and ACL (access control list) security protocols will apply on the network device those protocols include:-

- **SSH:** allows the administrators to have a remote administration outside the local network
- **Access control list:** - is configured on network devices with packet filtering capabilities such as routers and firewalls and it is used to filter the network traffic and allow and deny networks to access information from the data server.
- **HTTPS:-** protocol that is used to access the HTTP service securely.
- **MAC address filtering:** - that used to filter Mac for specific port when a person requests a service to the network the port must identify before connecting to the network so because of this MAC address the network security will assure and Protect against IP spoofing and flooding.
- **Firewall:** - the most necessary security method in which it filters the incoming and outgoing traffic of the LAN network.
- **NAT:** Configured in the border router which has one interface in the local (inside) network and one interface in the global (outside) network.
- **DMZ:** a perimeter network that protects and adds an extra layer of security to an organization's internal local-area network from untrusted traffic.

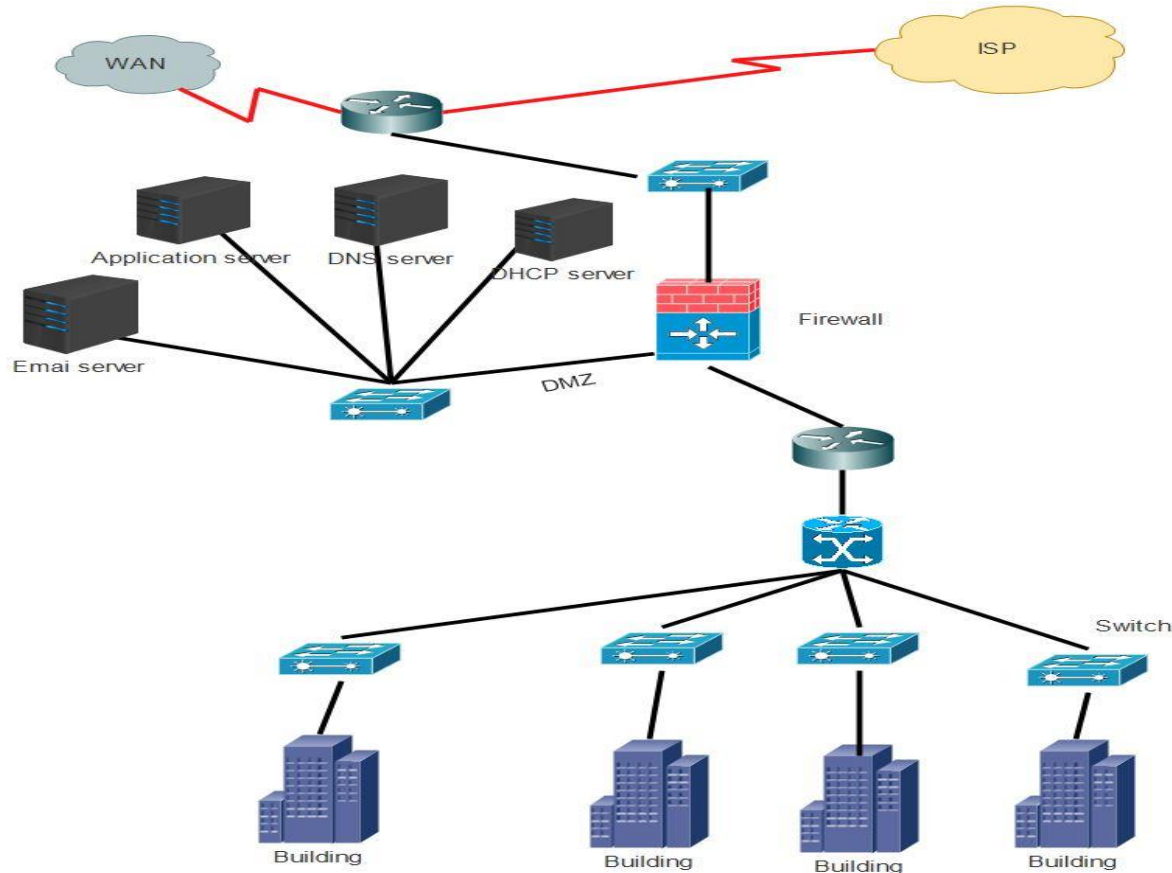


Figure 14: Security architecture of the network

## 4.8. Routing protocol

Transmission Control Protocol (TCP) and other protocols work with the data on network devices, and then it's sent to the IP module, where the data packets are bundled into IP packets and sent over the network. To reach the destination on the other side of the network, the data packets must pass through several routers. The work these routers do is called routing.

Each of the intermediate routers reads the destination IP address of each received packet. Based on this information, the router sends the packets in the appropriate direction. Each router has a routing table where information about neighboring routers (nodes) is stored.

This information includes the cost (in terms of network requirements and resources) of forwarding a packet in the direction of that neighboring node. Information from this table is used



to decide the most efficient node to use or the best route on which to send the data packets. Each packet can be sent in a different direction, but all eventually get routed to the same destination machine.

On reaching the destination, the packets are consumed by the network device, where the IP module reassembles the packets and sends the resulting data to the TCP service for further processing.

The selected Routing protocol for this network is the OSPF routing protocol. When it is configured, it listens to its neighbors in the networks, and it gathers all the link state data available. This data is then used to make a topology map that contains all available paths in the network. This database is saved for use, and we call it Link State Database.

Once the Link State Database is made, it is used to calculate the shortest path to subnets/networks using an algorithm known as Shortest Path First, developed by Edsger W Dijkstra. OSPF creates 3 tables:

- **Routing Table:** It contains currently working best paths that will be used to forward traffic between two neighbors.
- **Neighbor Table:** This contains all discovered Open Short Path First neighbors.
- **Topology Table:** This one contains the entire road map of the network. This road map includes all the available Open Short Path First routers and keeps calculated data about best and alternative paths.

## 4.9. WLAN design

Designing a reliable, secure and available wireless network requires considering many factors. A primary issue to be considered is capacity, in which the ability of the WLAN to provide reliable and available connectivity to clients in the coverage area. The placement of the wireless network devices is also another factor that affects the availability of the wireless network service.

In the new network design the wireless network will have access point positioning within 100 meter difference to next access point mean 1 access point will cover more than 4 building in different direction and also will position or place in different area according to the network usage of in that area. According to this information the outdoor wireless devices are distributed to 5 destinations which have high number of users. These destinations are around the Administrator

building, Electricity Department, The library building, New ICT classroom, the café. There are also indoor wireless devices which serve the users in the offices, labs and library. For continuous availability of connection throughout the compound 10 % overlaps from each access point is considered. The selected wireless access points have a coverage radius of 50m.

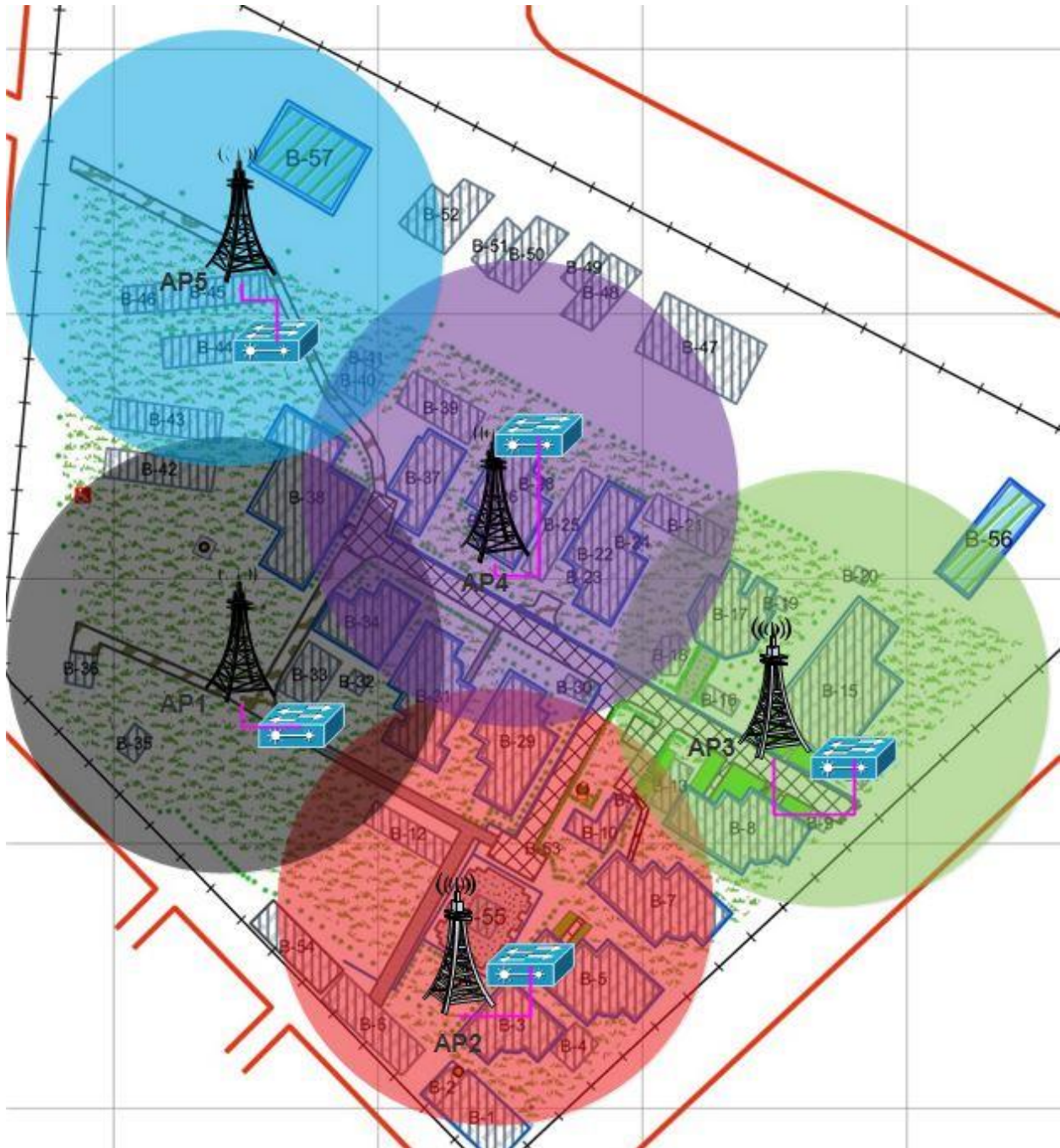


Figure 15: Outdoor wireless LAN design

## 4.10. Servers

The servers in the design can be taken as the brain for the network structure. Every network transmission will be passed by this network this has a benefit for:

- **Optimization:** Server hardware is designed to serve requests from clients quickly.

- **Centralization:** Files are in one location for easy administration.
- **Security:** Multiple levels of permissions can prevent users from damaging the files.
- **Redundancy and backup:** Data can be stored in redundant/disuse ways, making it easy to restore in case of problems.

There are servers with different functionalities to make the network usable in terms of different services. Most of these servers are located on the core layer of the network, this helps to make the service available in the whole network infrastructure.

**Proxy Server:** A proxy server uses to perform a function on behalf of other computers. It is located between the server and the clients.

**File Server:** to store the basic and sensitive information in the organization, and distributes files over the network to workstations. And as a standard, this server uses the FTP protocol to share resources throughout the network.

**DNS Server:** for managing the names of Web sites and other Internet domains. It masks the name of the website with its corresponding IP address.

**Web server:** delivery of web pages on the request to clients using the Hypertext Transfer Protocol (HTTP). It is the main server that makes users able to access websites and web apps.

**DHCP server:** Each computer that is connected to the network needs an IP address. The dynamic Host Configuration Protocol (DHCP) server will be connected to the switch device to connect many computers. The DHCP will distribute the IP address to each computer.

## 4.11. Location Specification

Identifying the location of each network device is a vital task to make the cable installation process simple and faster,

In this hierarchical network design, the data center which consists of the servers and core layer routers is located in the B-12 building; this building is selected for the data center because it was previously dedicated for the data center by the college's IT professionals. In the core layer there are 2 main routers in which each routers' two interfaces are connected with 4 distribution switches, these devices distribute the network to their nearby access layer switches, the access layer switches are devices which are directly connected with the end devices such as computers,

IP phones and printers. This table summarizes where is the network device located and how are they connected.

Below is the list of the Routers and switches with their corresponding building location,

**Table 8: Location specification for Network devices**

Network device types	Device name	Location
Core Layer Routers	Router1	Building B12
	Router2	Building B27
Distribution Layer Switches	DLS1	Building B3
	DLS2	Building B17
	DLS3	Building B29
	DLS4	Building B37
Access Layer Switches	ALS1- ALS35	On Every Main building (2u or 1u)
Access Points	AP1	Around building B5
	AP2	Around building B21
	AP3	Around building B29
	AP4	Around building B31

The next figure shows the locations where each components of the network, starting from the datacenter up to low level access layers, is located. It also illustrates how the devices are connected with their parent nodes.





#### 4.12. Vendor Selection

This section includes each network device that is used in the design and its manufacturers and suppliers. The vendors are identified by considering the specifications of the devices and selecting the models according to the network requirement of the infrastructure.

**Table 9: Network devices with vendors**

No	Network Device type	Vendor selected	Specifications
1	Server	Dell PowerEdge R840(Blade server)	<ul style="list-style-type: none"> <li>➤ Supports up to four Intel Xeon Scalable processors, 6 TB max memory, 200TB</li> </ul>
2	Firewall	Cisco ASA 5545-X Firewall	<ul style="list-style-type: none"> <li>➤ is next-generation firewalls that combine the most widely deployed stateful inspection firewall in the industry with a comprehensive suite of next-generation network security services</li> <li>➤ For comprehensive security without compromise.</li> </ul>
3	Core Layer Router	Cisco Router ISR 900	<ul style="list-style-type: none"> <li>➤ Combine Internet access, comprehensive security, and wireless services (LTE Advanced 3.0, Wireless WAN and Wireless LAN).</li> </ul>
4	Distribution Layer Switch	Cisco Catalyst 9300X Fiber	<ul style="list-style-type: none"> <li>➤ Stackable, Layers 2 and 3, 1 Tbps</li> <li>➤ 12 or 24 ports of 25G/10G/1G fiber</li> <li>➤ Modular uplinks: 100G/40G, 25G/10G/1G</li> </ul>
5	Access Layer switch	Cisco Catalyst 9500 Series	<ul style="list-style-type: none"> <li>➤ Stackable, Layers 2 and 3, 6.4 Tbps</li> <li>➤ Up to 4 x 400G/28 x 100G, 48 x 100G, 96 x 40G and 192 x 50G/25G/10G/1G ports</li> </ul>

			➤ Designed for Cisco DNA and SD-Access
6	Access Point	Aruba AP22 R4W02A	➤ Fast 802.11ax, 2X2:2 ➤ Wi-Fi Certified 6™ (Wi-Fi 6) ➤ Smart Mesh Wi-Fi support ➤ Built-in Wi-Fi router/gateway functionality
7	UTP Cable	HUAWEI	-
8	Fiber Cable	OFS	-

### 4.13. ISP (internet service provider)

Apparently, there are two main ISP companies that are currently working on giving internet service to the people these two companies are Ethio Telecom and Safaricom Ethiopia these two are currently competing by offering different options and by upgrading the current technology but it is preferable to use the earlier company which is Ethio Telecom. We prefer this company because of the different advantages it has compared to Safaricom Ethiopia.

The advantages are:

1. Ethio Telecom is a governmentally owned company so this increases its accountability and its supply faster and better service since The College is also a government institution.
2. Resources can be easily accessed in such government companies any kind of resource (internal, external) have better access possibilities to government companies than privately-owned companies.
3. Such government companies have better communication and connection with worldwide companies and get better credibility than privately-owned companies.
4. The privately-owned company like Safaricom Ethiopia takes Main lines from Ethio telecom and distributes them to their customers because of resource scarcity so Ethio telecom has its own lines and it has a better capacity, speed, consistency, and guarantee.



5. Other than these advantages Ethio telecom has better experience in this field of network and has many years of working time and people accompanied with it.







## References

- [1] - <https://www.ciscopress.com/articles/article.asp?p=2202410&seqNum=4>
  - [2] - James D. McCabe. (2003). *Network Analysis, Architecture and Design, Second Edition (The Morgan Kaufmann Series in Networking)*
  - [3] - Scott D. Lowe, (2016), *Building a Modern Data Center Principles and Strategies of Design*, Okatie Village Site 103-157, USA.
  - [4] - John Tiso (2012), *Designing Cisco Network service Architectures*, Third Edition, Cisco Press
- Steven T. Karris, 2009, *Networks: Design and Management*,

## **Appendix I**

1. When was the College established?
2. With how many students did the college started?
3. How many fields of trainings were provided?
4. What is the number of students currently?
5. How many departments and field of training are provided currently?
6. What is existing network infrastructure in the college?
7. How many network connected and not connected devices are found in the college
8. What are the drawbacks of the existing system?
9. What is your expectation from a new Local network design?
10. What services should be provided from the new proposed network design?

## Appendix II

Symbols	Description
	Servers
	Distribution Switch
	Router
	Access layer switch
	Access point
	ISP tower