University of Mumbai

Design and Implementation of End to End Secured Campus Area Network

Submitted at the end of semester VII in partial fulfillment of requirements For the degree of

Bachelors in Technology

by

Harsh Panchal
Roll No: 1813033

Kaushal Patil
Roll No: 1813038

Shubh Dedhia
Roll No: 1813040

Rohit Shah
Roll No: 1813042

Guide

Dr. Kiran Ajetrao

Department of Electronics and Telecommunication Engineering
K. J. Somaiya College of Engineering, Mumbai-77
(Autonomous College Affiliated to University of Mumbai)

Batch 2018 -2022

K. J. Somaiya College of Engineering, Mumbai-77

(Autonomous College Affiliated to University of Mumbai)

Certificate

This is to certify that the dissertation report entitled **Design and Implementation of End to End Secured Campus Area Network** submitted by Harsh Panchal, Kaushal Patil, Shubh Dedhia and Rohit Shah at the end of semester VII of LY B. Tech is a bonafide record for partial fulfilment of requirements for the degree of Bachelors in Technology in Electronics and Telecommunication Engineering of University of Mumbai.

27/12/2021

Guide/Examiner1

RADeshpande

Expert/Examiner2

Date: 27/12/2021

Place: Mumbai-77

K. J. Somaiya College of Engineering, Mumbai-77

(Autonomous College Affiliated to University of Mumbai)

Certificate of Approval of Examiners

We certify that this dissertation report entitled is bonafide record of project work done by Harsh Panchal, Kaushal Patil, Shubh Dedhia and Rohit Shah during semester VII. This project work is submitted at the end of semester VII in partial fulfilment of requirements for the degree of Bachelors in Technology in Electronics and Telecommunication Engineering of University of Mumbai.

27/12/2021

Guide/Examiner1

Expert/Examiner2

Date: 27/12/2021

Place: Mumbai-77

K. J. Somaiya College of Engineering, Mumbai-77

(Autonomous College Affiliated to University of Mumbai)

DECLARATION

We declare that this written report submission represents the work done based on our and / or others ideas with adequately cited and referenced the original source. We also declare that we have adhered to all principles of intellectual property, academic honesty and integrity as we have not misinterpreted or fabricated or falsified any idea/data/fact/source/original work/ matter in my submission.

We understand that any violation of the above will be cause for disciplinary action by the college and may evoke the penal action from the sources which have not been properly cited or from whom proper permission is not sought.

Signature of the Student **1813033** **Roll No.**	**Signature of the Student** **1813038** **Roll No.**
Signature of the Student **1813040** **Roll No.**	**Signature of the Student** **1813042** **Roll No.**

Date:

Place: Mumbai-77

Abstract

The importance of networks security and services at higher education institutions has never been higher than it is now. Users and institutions are demanding more and more network services and the exchange of more potentially sensitive information within these services. Firstly, in campus there is definite requirement of the network access. Doing work at one place by professors and sharing it at another place either to faculty members and students becomes quite difficult. As doing tasks on one PC, a professor might have to visit different classes and labs due to various reasons. Similarly a student working on a project might have to access a particular project document in multiple labs and classes. Head of Department has to visit various rooms and classes in a particular day. It would be very tedious job to carry laptop everywhere. There might be a situation when a user wants to share a particular data with more than one user. There can also be a situation when a particular message/ information need to be shared with the entire university. So this research work proposes a novel approach to communicate among various users that are present at different sites at the same time. So university network system is being proposed which would help departments to share information among faculty members and students. Proposed approach takes the help BUS topology model to explore concepts like VLANs, InterVLANs, OSPFs, ACLs, Redundancy and implementing firewall for internal and external security of network with the help of Cisco Packet Tracer to make the network more secured. This project looks into developing **End to End Secured Campus Area Network.**

Key words**:** ACLs (Access Control Lists), Addressing Table (AT), Cisco Packet Tracer (CPT), Domain name System (DNS), File Transfer Protocol (FTP), Open Shortest Path First (OSPF), Simple Mail Transfer Protocol, SSH (Secure Shell), Virtual LAN (VLAN).

List of Figures

List of Tables:

Chapter 1

1. Introduction

This chapter presents the introduction of the Design and Implementation of End to End Secured Campus Area Network. It contains the background of the technology utilized in the project topic, the motivation behind choosing this project and also the scope and overview of the developed project.

1.1 Background:

Network is important for a society from very ancient age. A good network (fast, efficient and leakage proof) play vital role in establishment of any government, research organization, or business establishment. In the age of Information Technology, ancient information network converted into computer network which is very fast and easily manageable. Similar to ancient era computer network security threat is always a serious issue and is very crucial. A campus network is an autonomous network under the management of university campus or within a local geographic area such as a business park, a government institution, a research centre, or a medical centre. While the network may be managed by a single entity, it may be used by different organizations. The campus network has matured and grown more complex than ever. Often, a campus network provides and access path into a larger network, such as a metropolitan area network or the Internet. To build a stable, safe, efficient, convenient wireless campus network has become the inevitable trend of development and construction of campus network.

Main purpose of a computer network is to facilitate the users to communicate among themselves and share resources with other users. A Campus network is an important part of campus life and network security is essential for a campus. The College Network Architecture is about designing a network topology that is a LAN (Local Area Network) for a College in which various computers of different departments are set up so that they can interact and communicate with each other by interchanging data. Campus network faces challenges to address core issues of security which are governed by network architecture. Secured network protects an institution from security attacks associated with network. Network security will prevent the college network from different types of threats and attacks. In this project, a tested and secure network design is implemented based on the practical requirements and this proposed network infrastructure is realizable with adaptable infrastructure.

1.2 Motivation:

The core motivation behind developing this project is to maximize security on campus in the era of ever increasing data and various threats and attacks associated to it. As college data is very crucial when it comes to any level of the campus network so to prevent any privacy breach of any entity a secured network is very much necessary. Also to prevent malicious attacks which has potential to hamper the life of a student or faculty. With the Pandemic, things going virtual and studying/working from home has become the new normal, the security aspect must go hand in hand to ensure smooth functioning of life on virtual campus.

1.3 Scope of the Project:

The scope of the project begins from the research on various attacks that can happen in campus area network, the methods and logic to prevent such attacks, and then the implementation of these specific preventive measures. The campus area network has two main benefits.

- **Much Secured:** Unlike other types of networks, Campus Area Network is maintained and managed by one entity, which in most cases is the campus IT department. Network administrators can easily monitor, regulate, and allow access to the network. The team also installs firewalls between CAN and internet providers to prevent unauthorized access. They may also use proxy servers to limit internet ports or websites that users can access.

- **High Speed:** Communication within CAN takes place through a local network. Therefore, data transfer speed within the network is uninterrupted and remains higher than the typical internet speed. With this, users can share large files quickly. For instance, it can take several hours to upload a long video successfully when connected to the internet.However, transferring such videos over CAN takes a few minutes.

1.4 Overview of the Project:

The project is implemented on a platform called Cisco Packet tracer. This is a visual simulation tool with the aim to create network topology from. This project aims to design Campus network topology using Bus Topology. Campus consists of Data centre, Network Admin office, Boy's & Girls Hostel, Reception area, 5 Departments and Library. As every entity is in different network we created virtual LANs in which with the help of inter-VLAN routing we can communicate with different networks. The server consists of 4 servers viz. DNS, HTTP, SMTP, FTP. The DNS is used to create domain of the campus. HTTP is for webpage access to end users, SMTP is for Email service. FTP is a way to download, upload, and transfer files from one location to another on the internet and between computer systems. We used SSH on network admin‘s Switch & Router to take access remotely.

We will use OSPFs, ACLs to restrict, permit, or deny traffic which is essential for security of Network and will implement firewall for internal and external security of network. As this project matures, for security of the network the final step will be to identify the threats which can happen in a campus area network and analyze them.

1.5 Organization of the Report:

The report is structured in 5 chapters where, chapter 1 consists of existing campus security problems and we believe creating a network model for campus. Chapter 2 i.e., literature review consists of a brief summary of study of different secured campus area networks, problems and their use cases. Chapter 3 consisting of Problem Statement, Network Topology, Network Devices used, Flowchart, Addressing table of developed network. Chapter 4 comprises of the implementation and working of campus area network. Chapter 5 consists of Conclusions and future work that can be implemented to the project.

Chapter 2

2. Literature Review

This chapter presents a brief about the literature review of the project implemented and overview of the references from which the literature review has been composed.

In Design and Implementation of University Network [1] This paper focuses on network design using bus topology which will be used for an entire university and every user of the network will be interlinked with each other. Research work proposes a novel approach to communicate among various users that are present at different sites at the same time. Departments will share information among faculty members and students where the whole university works on a single network which includes various facilities such as transmitting messages, accessing data on any physical computer within the network, accessing same speed in various geographical areas within university network. Proposed approach takes the help of sharing common network domain by DNS and applies heterogeneous BUS topology model to explore various concepts like topology design, creating dynamic host configuration protocol, sub net masking, DNS and VLAN within a single network with the help of Cisco Packet Tracer to make the network more secured and cost effective.

In Campus Network Security and Management [2] This paper focuses on the designing of the campus area network using star topology and the project comprises of the different Departments of a Campus spread in different buildings. Multiple Routing protocols have been used in different branches and all the departments can communicate with other different departments through the redistribution among different Routing Protocols. It has a DHCP server for assigning the IP Addresses to the Hosts in the building as well as a DHCP server has been used in the other Buildings as well. The Internet Service Provider has been used for Communication of the Buildings of Campus with the Data Centre & Internet through ISP, using the Frame Relay Switching Technology available for Wide Area Network. Routing Protocol EIGRP, Static Routing & its concepts including the Default Routing as well has been applied. The different Routing Protocols are running and which has been synchronized to work with Frame Relay Switching Technology.

In Security Problems in Campus Problems and its solutions [3] This paper focuses on the importance of network security and services at higher education institutions. Users and institutions are demanding more and more network services and the exchange of more potentially sensitive information within these services. Firstly, in campus there is definite requirement of the network access and building campus network has become crucial. The campus network has a number of tasks such as teaching, research, management and communication with the outside. Therefore, the issue of network security has become a priority to campus network management. Obviously, the current Internet is convenient but at the same time it is unsafe. While using network services in campus area network it can be more easily attacked. This paper represents the current security status of the campus network, analyze security threats to campus network and describe the strategies to maintain robust network system.

In Design and Implementation of a Secure Campus Network [4] This paper focuses on network attacks. There are various types of attacks such as Passive Attack, Active Attack, Distributed Attack, Insider Attack, Close-in Attack, Phishing Attack, Hijack attack, Spoof attack, Buffer overflow, exploit attack, Password attack. Denial of service (DoS) is a interruption of service either as a result of the system is destroyed, or as a result of it's quickly out of stock. ARP spoofing could be a style of attack during which a malicious actor sends falsified ARP (Address Resolution Protocol) messages over Local Area Network (LAN). This ends up in the linking of associate attacker's mackintosh (MAC) (address with IPaddress) of a server on the network.

- **Objectives of the Project:**
    - Literature Survey of Project.
    - Design of Secured Robust Campus Area Network.
    - Creation of VLANs, InterVLAN's Communication and SSH.
    - Creation of SSH, OSPFs, ACLs and implementing firewall for internal and external security of network.
    - For security of the network, we will identify the threats which can happen in a campus area network and analyze them.
    - Validation of Small network using Hardware Setup.

Chapter 3

3. Project Design

This chapter presents the details about the design of the project. A basic introduction is given which is followed by the problem statement. It also provides the Network topology, flowchart and addressing table of the project developed.

3.1 Introduction:

In this project we created campus area network topology using cisco packet tracer. We used bus topology to design the campus network. Campus consists of Data centre, Network Admin office, Boys & Girls hostel, Reception area, 5 departments and library. As every entity is in different network we created virtual LANs in which with the help of inter VLAN routing we can communicate with different networks. The server consists of 4 servers viz. DNS, HTTP, SMTP, and FTP.

3.2 Problem Statement:

Campus network faces the security challenges which are influenced by network infrastructure. To maintain data privacy and campus integrity the campus network needs to have secure network design to protect from different types of threats and attacks. The aim of this project is to build a secured campus network design, which can defend against specified attacks.

3.3 Network Topology:

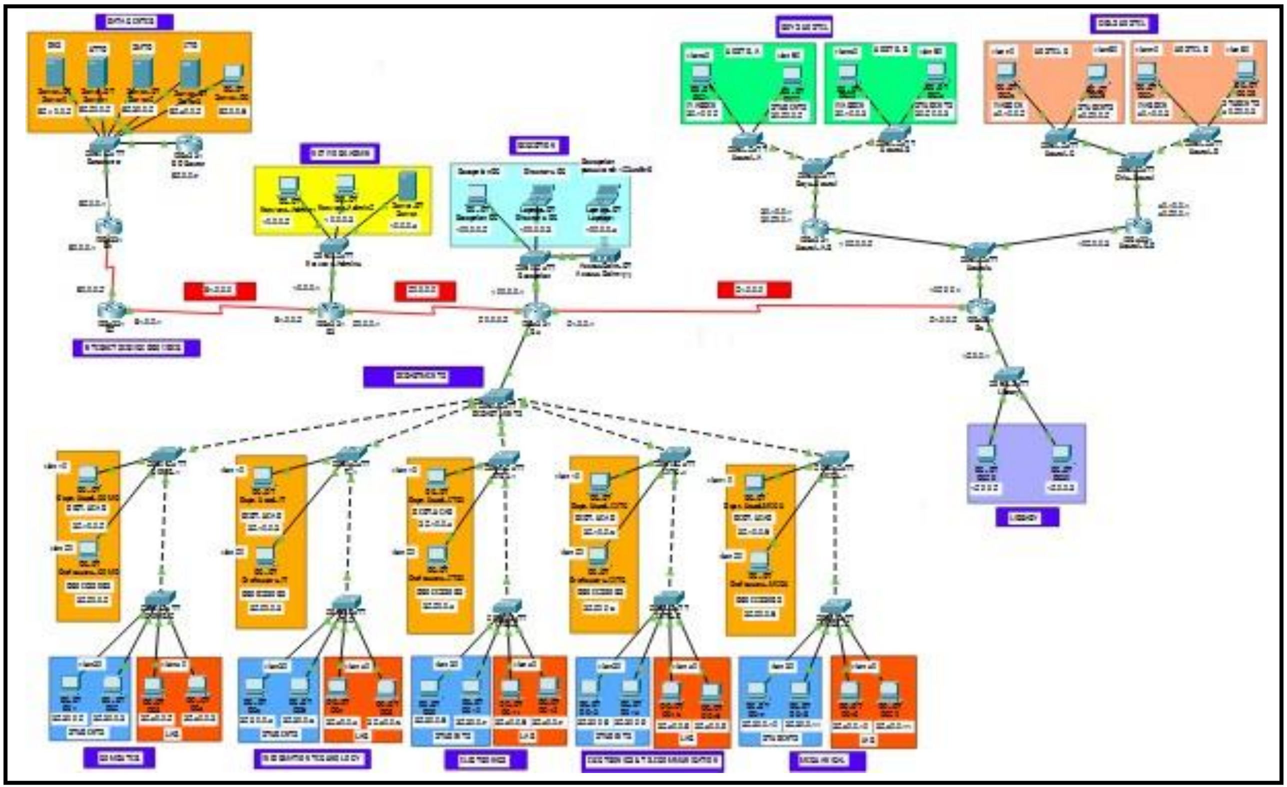


Figure no. 3.3: Network Topology

3.4 Network Devices Specifications:

1. 2960 Series Switches:

Figure no. 3.4.1: 2960 Series Switches

- **Purpose:**
  A switch is a device that operates at the Data Link layer of the OSI model—Layer 2. It takes in packets being sent by devices that are connected to its physical ports and sends them out again, but only through the ports that lead to the devices the packets are intended to reach.

Item Name	Cisco Catalyst 2960 Series Switches
Uplink Interfaces	2 dual-purpose (10/100/1000 or SFP) ports
Ports	24 x Ethernet 10/100 PoE ports
Throughput	6.5 Mpps
Dimension	1.73 x 17.5 x 9.3 in.
Cost	INR 29000

Table no. 3.4.1: 2960 Series Switches Specifications

2. Router 4331:

Figure no. 3.4.2: Router 4331

- **Purpose:**

  Routers 4331 use LAN Ethernet ports to connect to a modem and access the ISP, running a cable between a computer to the router then the router to the Ethernet port. Even though the line is connected to one central computer, the router easily allows sharing of the connection to any device that is connected to the network.

Item Name	Cisco ISR 4331 Integrated Services Router
Ports	1 x 10/100/1000 Mb/s Gigabit Ethernet RJ451 x 10/100/1000 Mb/s Gigabit SFP 1 x 10/100/1000 Mb/s Gigabit Combo Ethernet/SFP1 x Ethernet RJ45 (Console) 1 x Ethernet RJ45 1 x Mini-USB 1 x 480 Mb/s USB Type-A
Throughput	100 B/s
Dimensions	23.1 x 23 x 6.9 in
Cost	INR 461606

Table no. 3.4.2: Router 4331 Specifications

3. Access Point-Pt:

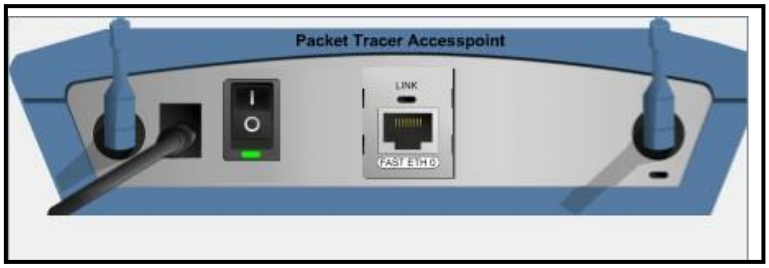


Figure no. 3.4.3 Access Point-Pt

- **Purpose:**

  A Wireless Access Point (WAP) is a networking device that allows wireless-capable devices to connect to a wired network. Instead of using wires and cables to connect every computer or device in the network, installing WAPs is a more convenient, more secure, and cost-efficient alternative

Connectors	Cable bay (left to right) Power connector (for plug-in ACpower module); RJ-45 connector for 10BASE-T or 100BASE-T Ethernet connections; upside down RJ-45 connector for serial connections.
Dimensions	7.53 x 7.53 x 1.31 in
Indicators	Tri-color Status LED indicator on the top panel and two bi-color LED indicators (radio and Ethernet) in the cable bay.
Input Voltage	48 VDC
Input Power	12.95 W

Table no. 3.4.3: Access Point-Pt Specifications

4. PC:

Figure no. 3.4.4: PC

- **Purpose:**

PC‘s are the end devices which are generally used to access services provided by the network.

Ports	PT-HOST-NM-1AM PT-HOST-NM-1CE PT-HOST-NM-1CFE PT-HOST-NM-1CGE PT-HOST-NM-1FFE PT-HOST-NM-1FGE PT-HOST-NM-1W PT-HOST-NM-1W-A PT-HOST-NM-1W-AC PT-HOST-NM-3G/4G PT-HOST-NM-COVER PT-HEADPHONE PT-MICROPHONE
Cost	INR 25000

Table no. 3.4.4: PC Specifications

5. Laptop:

Figure no. 3.4.5: Laptop

- **Purpose:**

  Laptops are the end devices which are generally used to access services provided by the network.

Ports	PT-LAPTOP-NM-1AM PT-LAPTOP-NM-1CE PT-LAPTOP-NM-1CFE PT-LAPTOP-NM-1CGE PT-LAPTOP-NM-1FFE PT-LAPTOP-NM-1FGE PT-LAPTOP-NM-1W PT-LAPTOP-NM-1W-A PT-LAPTOP-NM-1W-AC PT-LAPTOP-NM-3G/4G PT-LAPTOP-NM-COVER PT-HEADPHONE PT-MICROPHONE
Cost	INR 50000

Table no. 3.4.5: Laptop Specifications

6. **Server :**

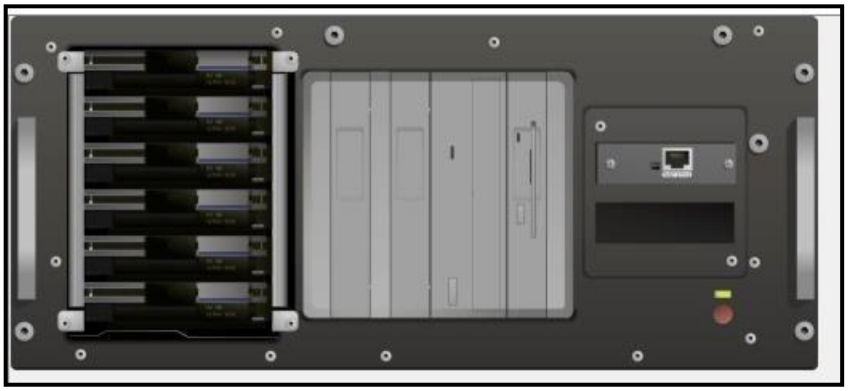


Figure no. 3.4.6: Server

- **Purpose:**

  A server is a device or program dedicated to providing services to other programs, referred to as clients‘ It may serve data to systems on a local area network (LAN) or a wide area network (WAN) over the Internet.

Ports	PT-HOST-NM-1CE PT-HOST-NM-1CFE PT-HOST-NM-1CGE PT-HOST-NM-1FFE PT-HOST-NM-1FGE PT-HOST-NM-1W PT-HOST-NM-1W-A PT-HOST-NM-1W-AC PT-HOST-NM-3G/4G PT-HOST-NM-COVER
Cost	INR 80000

Table no. 3.4.6 Server Specifications

3.5 Flow Chart:

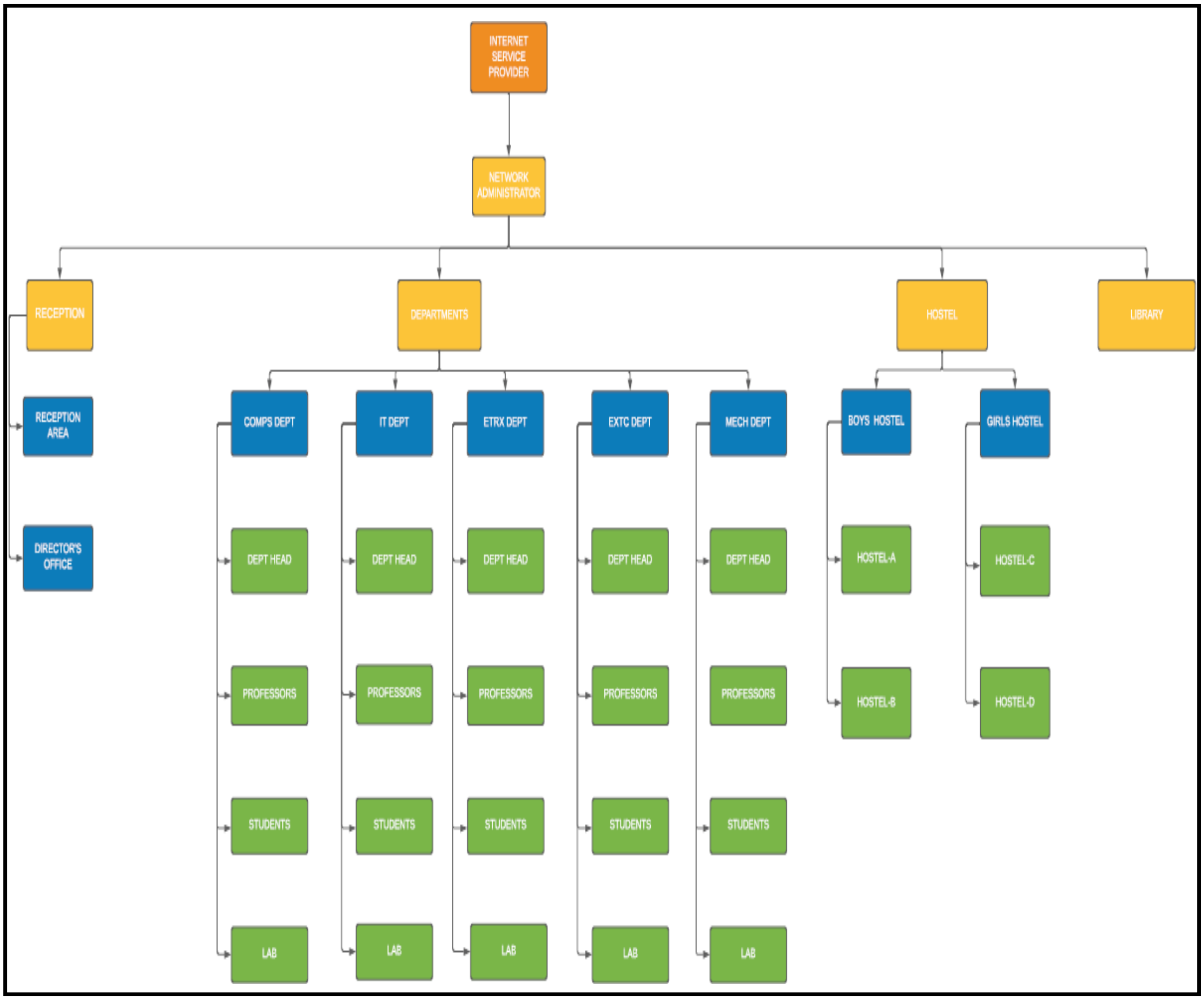


Figure no. 3.5 Flowchart

3.6 Network Description:

1. Data Centre / Server room

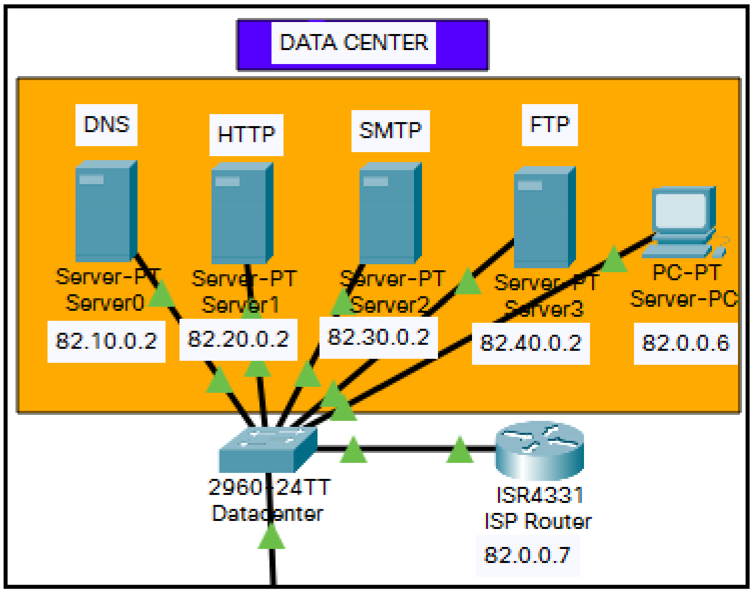


Figure no. 3.6.1: Data Centre

The server room has 4 servers. i.e. DNS,HTTP,SMTP, FTP. It also has a PC to access the servers. It is the heart of the campus. All the data of the entire campus is stored in server room.

Addressing Table:

Hostname	**IP address**	**Subnet Mask**	**Default gateway**
Server 0	82.10.0.2	255.255.0.0	82.10.0.1
Server 1	82.20.0.2	255.255.0.0	82.20.0.1
Server 2	82.30.0.2	255.255.0.0	82.30.0.1
Server 3	82.40.0.2	255.255.0.0	82.40.0.1
Server-PC	82.0.0.2	255.0.0.0	82.0.0.1
ISP Router	82.0.0.7	255.0.0.0	82.0.0.1

Table no. 3.6.1: Data Centre AT Specifications

2. Network Admin

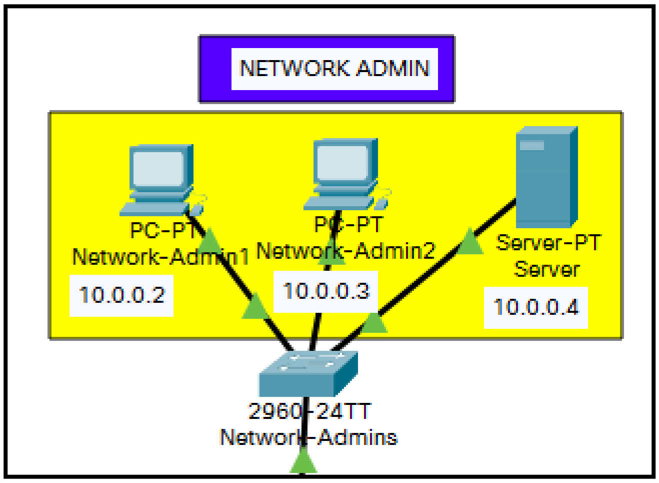


Figure no. 3.6.2: Network Admin

The role of the network administrator is to monitor and troubleshoot the network.

Addressing Table:

Hostname	IP address	Subnet Mask	Default gateway
Network-Admin1	10.0.0.2	255.0.0.0	10.0.0.1
Network-Admin2	10.0.0.3	255.0.0.0	10.0.0.1
Server	10.0.0.4	255.0.0.0	10.0.0.1

Table no. 3.6.2: Network Admin AT Specifications

3. Reception:

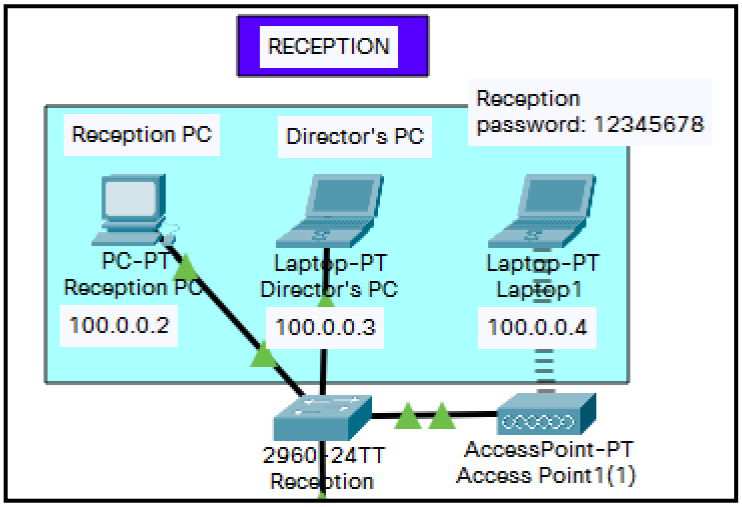


Figure no. 3.6.3: Reception

The reception has a PC of itself and a director‘s Laptop and an access point. The access point is used to wirelessly connect devices to the college network. It operates on multi band. A 2.4Ghz and 5 Ghz band.

Addressing Table

Hostname	IP address	Subnet Mask	Default gateway
Reception PC	100.0.0.2	255.0.0.0	100.0.0.1
Director's PC	100.0.0.3	255.0.0.0	100.0.0.1
Laptop 1	100.0.0.4	255.0.0.0	100.0.0.1

Table no. 3.6.3: Reception AT Specifications

4. Boys Hostel

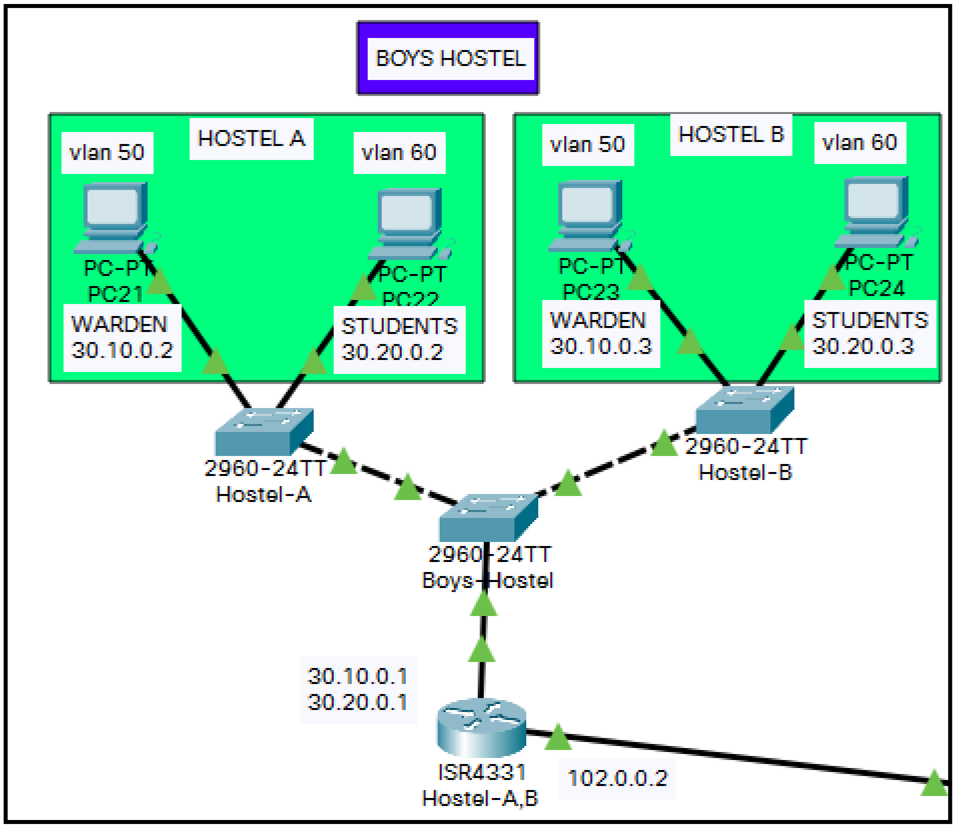


Figure no. 3.6.4: Boys Hostel

The whole Hostel consists of 4 buildings. 2 for boy's hostel and 2 for Girls hostel. Each Building has a warden and End devices for students.

Addressing Table

Hostname	IP address	Subnet Mask	Default gateway
PC21	30.10.0.2	255.255.0.0	30.10.0.1
PC22	30.20.0.2	255.255.0.0	30.20.0.1
PC23	30.10.0.3	255.255.0.0	30.10.0.1
PC24	30.20.0.3	255.255.0.0	30.20.0.1

Table no. 3.6.4: Boys Hostel AT Specifications

5. Girls Hostel

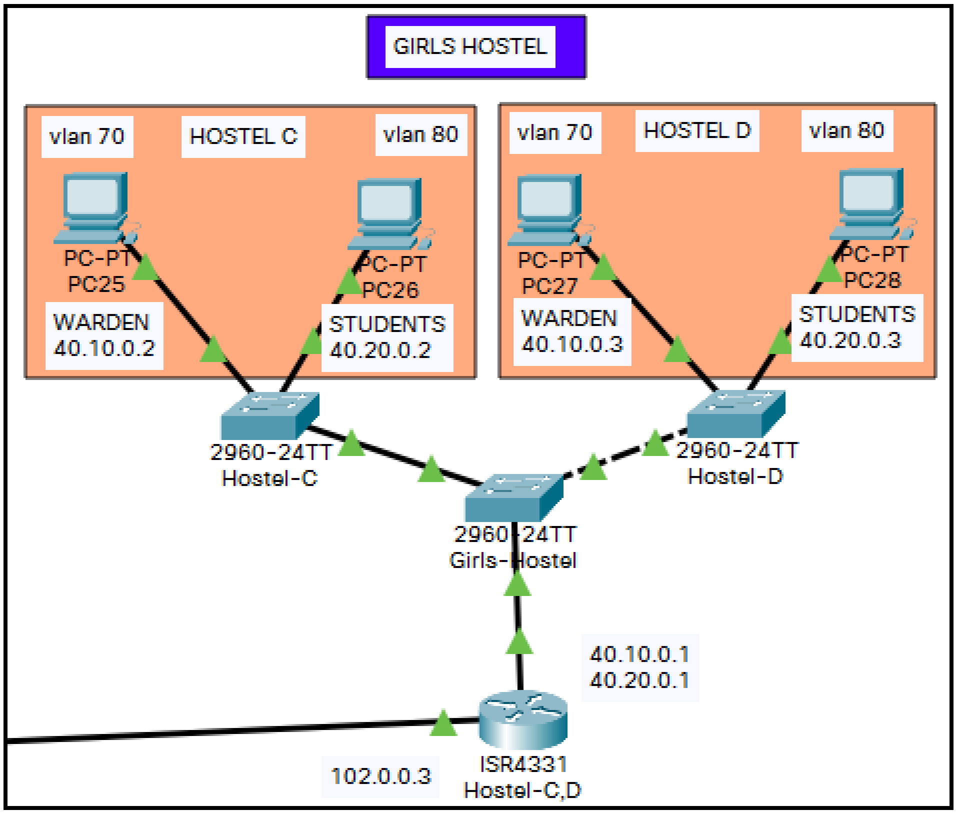


Figure no. 3.6.5: Girls Hostel

Addressing Table

Hostname	**IP address**	**Subnet Mask**	**Default gateway**
PC25	40.10.0.2	255.255.0.0	40.10.0.1
PC26	40.20.0.2	255.255.0.0	40.20.0.1
PC27	40.10.0.3	255.255.0.0	40.10.0.1
PC28	40.20.0.3	255.255.0.0	40.20.0.1

Table no. 3.6.5: Girls Hostel AT Specifications

6. Library

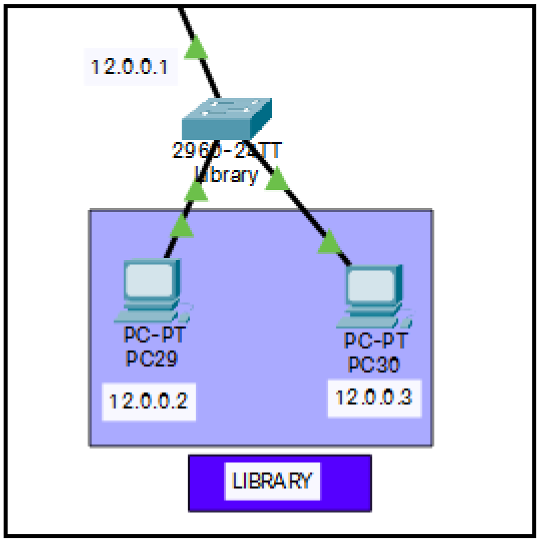


Figure no. 3.6.6: Library

Addressing Table

Hostname	IP address	Subnet Mask	Default gateway
PC29	12.0.0.2	255.0.0.0	12.0.0.1
PC30	12.0.0.3	255.0.0.0	12.0.0.1

Table no. 3.6.6: Library AT Specifications

7. Departments

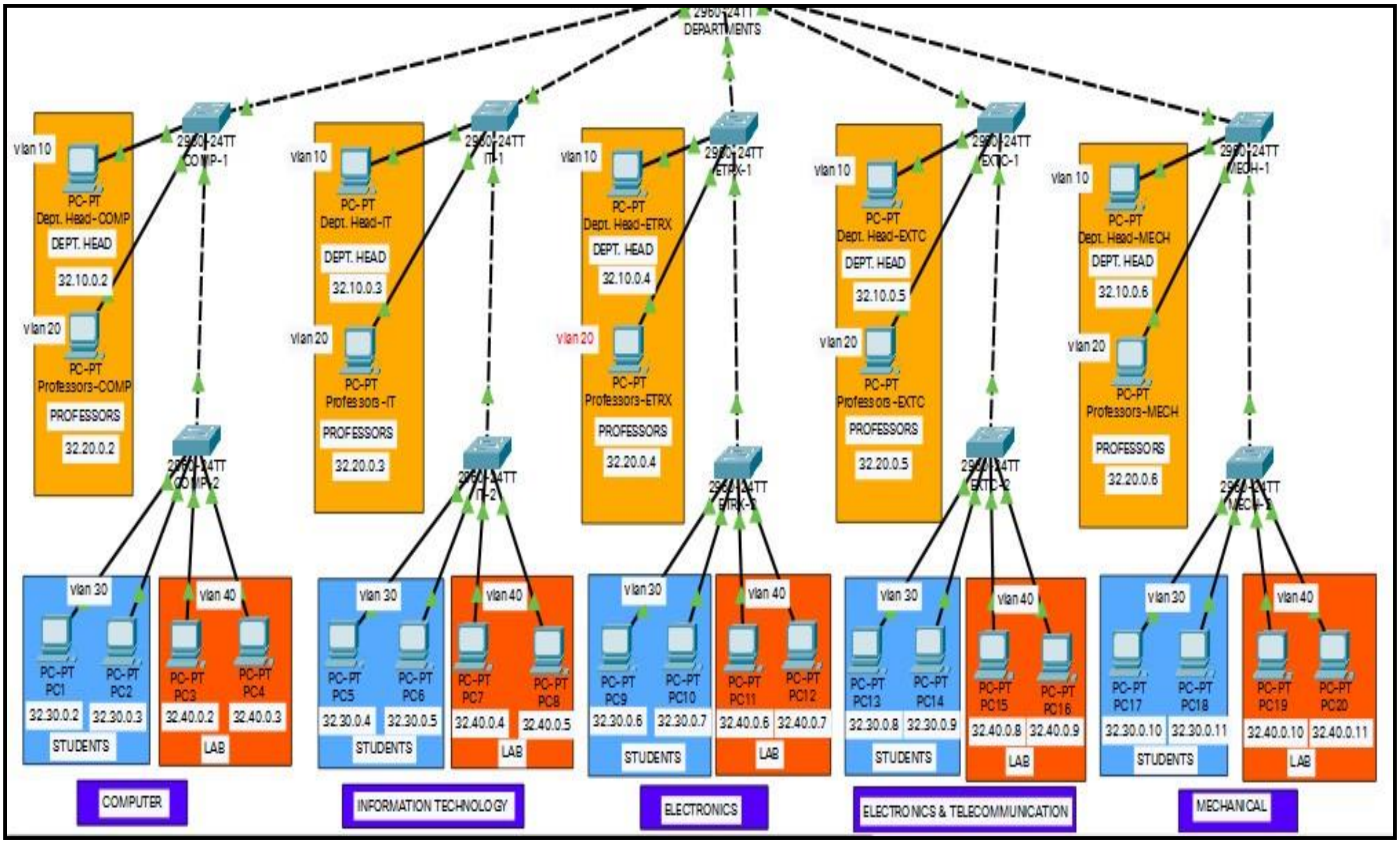


Figure no. 3.6.7: Departments

7.1 Computer Department

Addressing Table

Hostname	IP address	Subnet mask	Default gateway
Dept. head COMP	32.10.0.2	255.255.0.0	32.10.0.1
Professors- COMP	32.20.0.2	255.255.0.0	32.20.0.1
PC1	32.30.0.2	255.255.0.0	32.30.0.1
PC2	32.30.0.3	255.255.0.0	32.30.0.1
PC3	32.40.0.2	255.255.0.0	32.40.0.1
PC4	32.40.0.3	255.255.0.0	32.40.0.1

Table no. 3.6.7.1: Comp Department AT Specifications

7.2 IT Department

Addressing Table

Hostname	IP address	Subnet mask	Default gateway
Dept. head IT	32.10.0.3	255.255.0.0	32.10.0.1
Professors- IT	32.20.0.3	255.255.0.0	32.20.0.1
PC5	32.30.0.4	255.255.0.0	32.30.0.1
PC6	32.30.0.5	255.255.0.0	32.30.0.1
PC7	32.40.0.4	255.255.0.0	32.40.0.1
PC8	32.40.0.5	255.255.0.0	32.40.0.1

Table no. 3.6.7.2: IT Department AT Specifications

7.3 ETRX Department

Addressing Table

Hostname	IP address	Subnet mask	Default gateway
Dept. head ETRX	32.10.0.4	255.255.0.0	32.10.0.1
Professors- ETRX	32.20.0.4	255.255.0.0	32.20.0.1
PC9	32.30.0.6	255.255.0.0	32.30.0.1
PC10	32.30.0.7	255.255.0.0	32.30.0.1
PC11	32.40.0.6	255.255.0.0	32.40.0.1
PC12	32.40.0.7	255.255.0.0	32.40.0.1

Table no. 3.6.7.3: ETRX Department AT Specifications

7.4 EXTC Department

Addressing Table

Hostname	IP address	Subnet mask	Default gateway
Dept. head EXTC	32.10.0.5	255.255.0.0	32.10.0.1
Professors-EXTC	32.20.0.5	255.255.0.0	32.20.0.1
PC13	32.30.0.8	255.255.0.0	32.30.0.1
PC14	32.30.0.9	255.255.0.0	32.30.0.1
PC15	32.40.0.8	255.255.0.0	32.40.0.1
PC16	32.40.0.9	255.255.0.0	32.40.0.1

Table no. 3.6.7.4: EXTC Department AT Specifications

7.5 MECH Department

Addressing Table

Hostname	IP address	Subnet mask	Default gateway
Dept. head MECH	32.10.0.6	255.255.0.0	32.10.0.1
Professors-MECH	32.20.0.6	255.255.0.0	32.20.0.1
PC17	32.30.0.10	255.255.0.0	32.30.0.1
PC18	32.30.0.11	255.255.0.0	32.30.0.1
PC19	32.40.0.10	255.255.0.0	32.40.0.1
PC20	32.40.0.11	255.255.0.0	32.40.0.1

Table no. 3.6.7.5: MECH Department AT Specifications

Chapter 4

Implementation and Experimentation

This chapter presents the details about the project implementation and working of the model developed. The software requirements for the project are given along with the snapshots of created VLANs, SSH and Results are also given.

4.1 Software Requirements:

1. **Cisco Packet Tracer:**

- Packet Tracer is a cross-platform visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks.
- The software allows users to simulate the configuration of Cisco routers and switches using a simulated command line interface.
- It can be run on Linux, Microsoft Windows, and macOS.
- It allows users to create simulated network topologies by dragging and dropping routers, switches and various other types of network devices. A physical connection between devices is represented by a 'cable' item. Packet Tracer supports an array of simulated Application Layer protocols, as well as basic routing with RIP, OSPF, EIGRP, BGP.

4.2 Methodology:

4.2.1 VLANs:

- *Virtual LAN (VLAN)* is a concept in which we can divide the devices logically on layer 2 (data link layer). Generally, layer 3 devices divide broadcast domain but broadcast domain can be divided by switches using the concept of VLAN.
- A broadcast domain is a network segment in which if a device broadcast a packet then all the devices in the same broadcast domain will receive it.
- The devices in the same broadcast domain will receive all the broadcast packets but it is limited to switches only as routers don‘t forward out the broadcast packet.
- To forward out the packets to different VLAN (from one VLAN to another) or broadcast domain, interVLAN routing is needed. Through VLAN, different small-size sub-networks are created which are comparatively easy to handle.

VLAN ranges:

- VLAN 0, 4095: These are reserved VLAN which cannot be seen or used.
- VLAN 1: It is the default VLAN of switches. By default, all switch ports are in VLAN. This VLAN can‘t be deleted or edit but can be used.
- VLAN 2-1001: This is a normal VLAN range. We can create, edit and delete these VLAN.
- VLAN 1002-1005: These are CISCO defaults for fddi and token rings. These VLAN can‘t be deleted.
- VLAN 1006-4094: This is the extended range of Vlan.

Example:

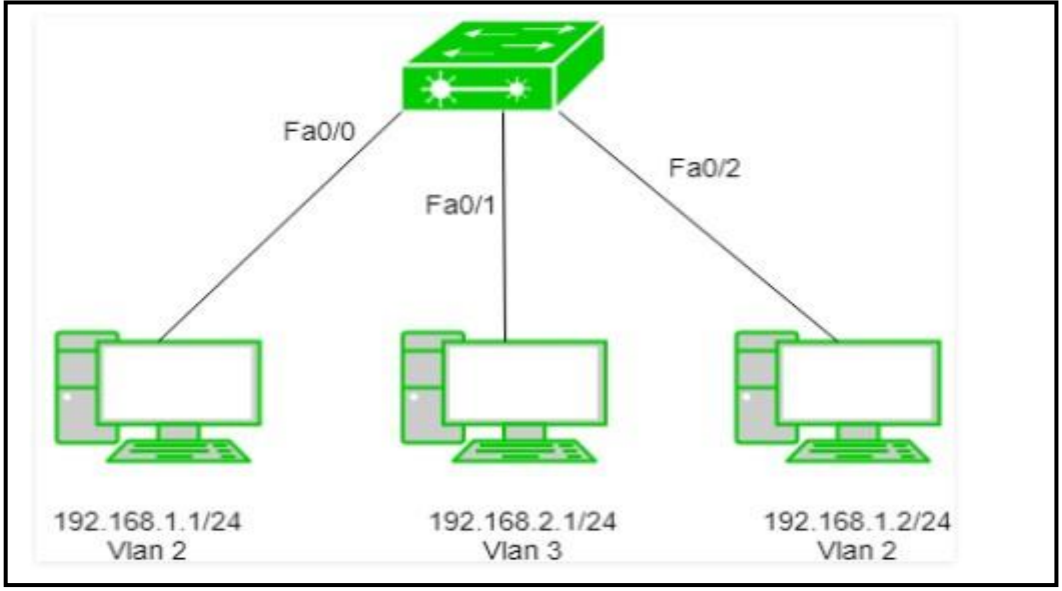


Figure no. 4.2.1: VLANs

Types of connections in VLAN:

1. **Trunk Link –**
   All connected devices to a trunk link must be VLAN-aware. All frames on this should have a special header attached to it called tagged frames.
2. **Access link –**
   It connects VLAN-unaware devices to a VLAN-aware bridge. All frames on the access link must be untagged.
3. **Hybrid link –**
   It is a combination of the Trunk link and Access link. Here both VLAN-unaware and VLAN-aware devices are attached and it can have both tagged and untagged frames.

4.2.2 InterVLAN Routing (Router on a stick Method):

- Inter VLAN routing is a process in which we make different virtual LANs communicate with each other irrespective of where the VLANs are present (on same switch or different switch).
- It can be achieved through a layer-3 device i.e. Router or layer-3 Switch. When the Inter VLAN Routing is done through Router it is known as Router on a stick.

4.2.3 SSH:

- It is a cryptographic network protocol that is used for transferring encrypted data over network.
- It allows you to connect to a server, or multiple servers, without having you to remember or enter your password for each system that is to login remotely from one system into another.
- It always comes in key pair:
    1. **Public key** – Everyone can see it, no need to protect it. (for encryption function)
    2. **Private key** – Stays in computer, must be protected. (for decryption function)
- Key pairs can be of the following types:
    1. **User Key –** If public key and private key remain with the user.
    2. **Host Key –** If public key and private key are on a remote system.
    3. **Session key –** Used when large amount of data is to be transmitted.
- We used RSA Encryption method in our topology

4.3 Model working:

4.3.1 Department Configuration:

- Created VLANs for Dept. Head, Professors, Students and lab for 5 Departments.

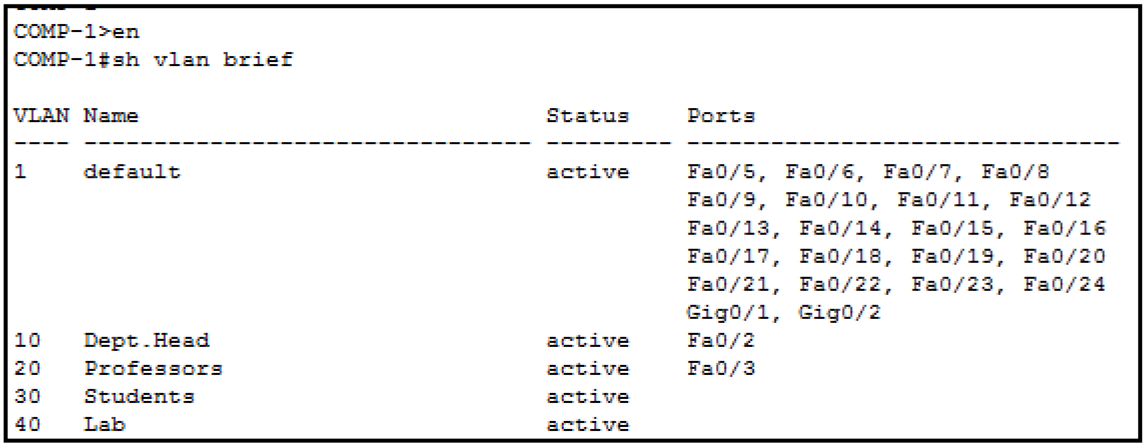
Hostname	Ports	Assignment	Network
COMP-1	fa0/2	VLAN 10	32.10.0.0
COMP-1	fa0/3	VLAN 20	32.20.0.0
COMP-2	fa0/1-2	VLAN 30	32.30.0.0
COMP-2	fa0/3-4	VLAN 40	32.40.0.0

Table no. 4.3.1: COMP VLANs

- Created trunking ports on Department switch.
- Same process is done for other departments.

Example of Computer Department:

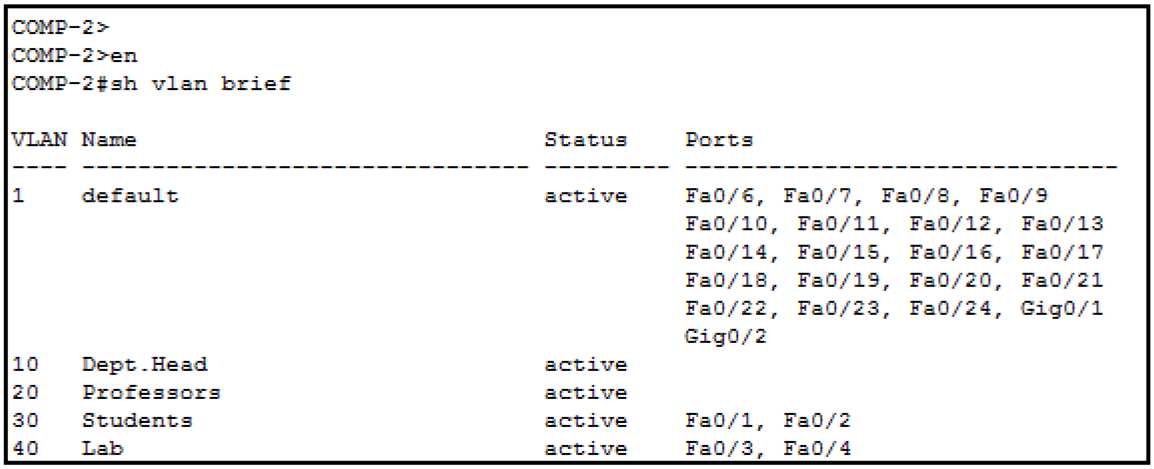
1) COMP-1 Switch:



```
COMP-1>en
COMP-1#sh vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
10   Dept.Head                        active    Fa0/2
20   Professors                       active    Fa0/3
30   Students                         active
40   Lab                              active
```

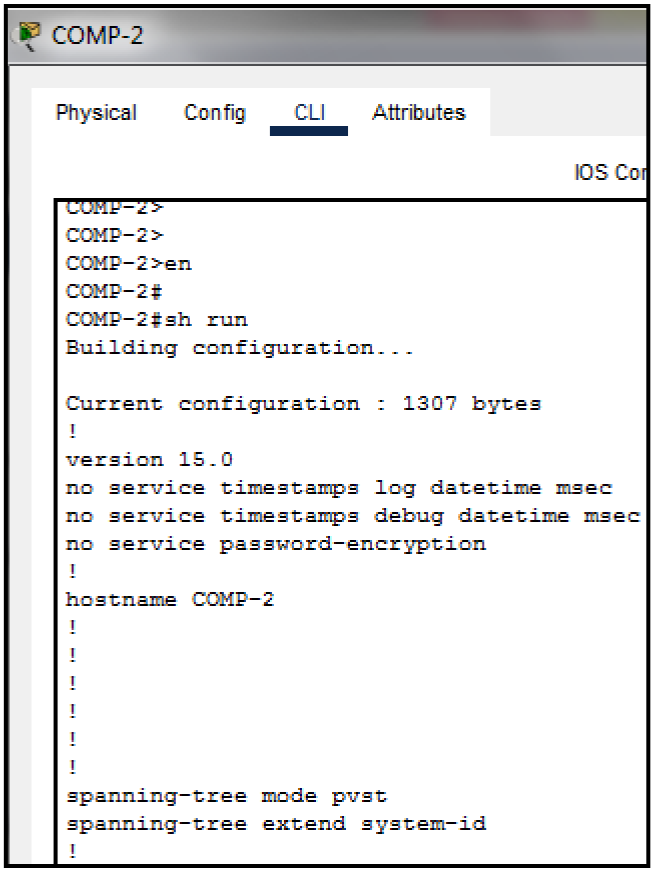
Figure no. 4.3.1.1: COMP-1 Switch

2) COMP-2 Switch:



```
COMP-2>
COMP-2>en
COMP-2#sh vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gig0/1
                                                Gig0/2
10   Dept.Head                        active
20   Professors                       active
30   Students                         active    Fa0/1, Fa0/2
40   Lab                              active    Fa0/3, Fa0/4
```

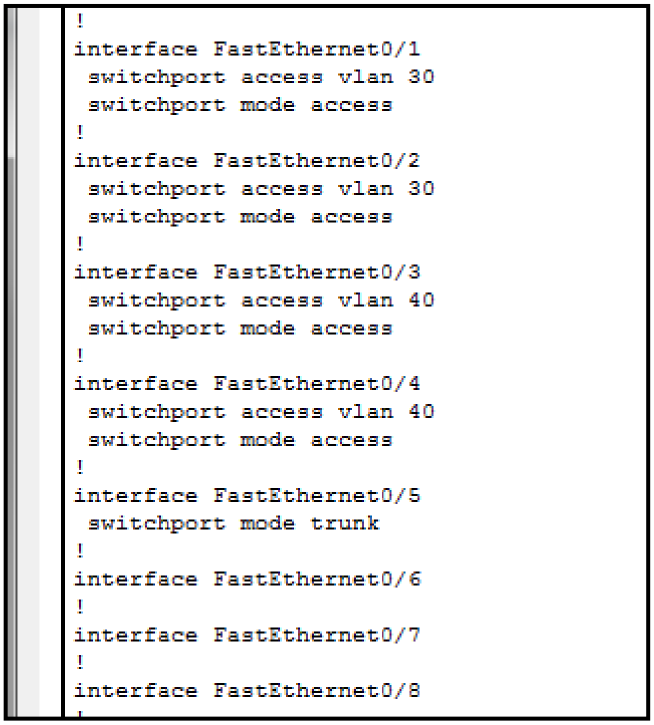
Figure no. 4.3.1.2: COMP-2 Switch



```
COMP-2>
COMP-2>
COMP-2>en
COMP-2#
COMP-2#sh run
Building configuration...

Current configuration : 1307 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname COMP-2
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
```

Figure no. 4.3.1.3: COMP-2 Switch

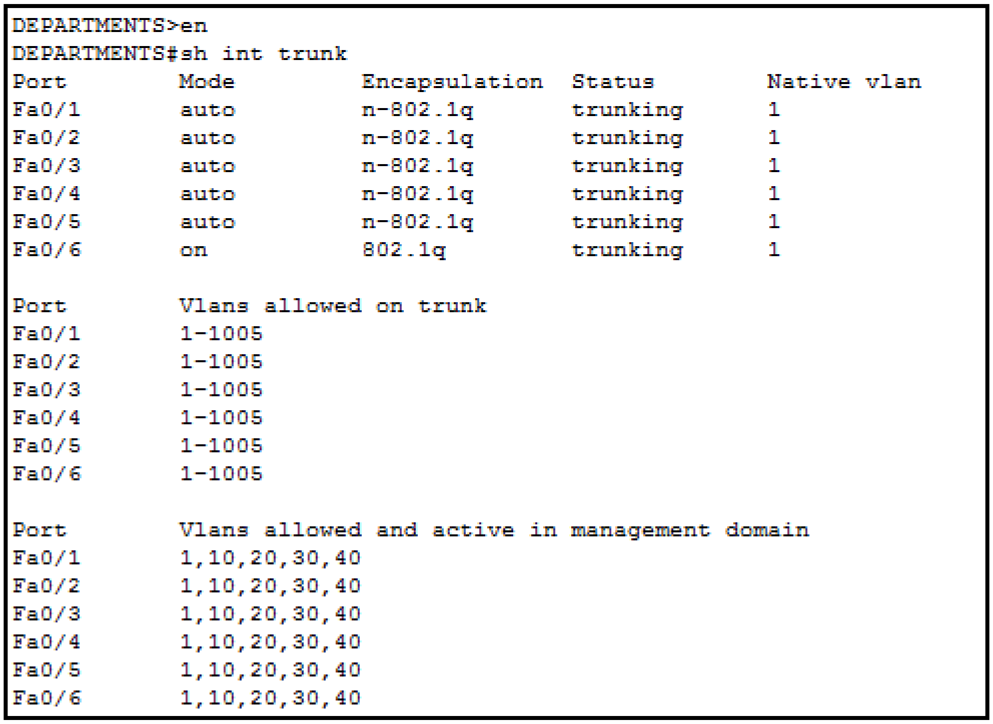
3) COMP-2 Switch (VLAN Configuration):



```
!
interface FastEthernet0/1
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 40
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 40
 switchport mode access
!
interface FastEthernet0/5
 switchport mode trunk
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
```

Figure no. 4.3.1.4: COMP-2 Switch (VLAN Configuration)

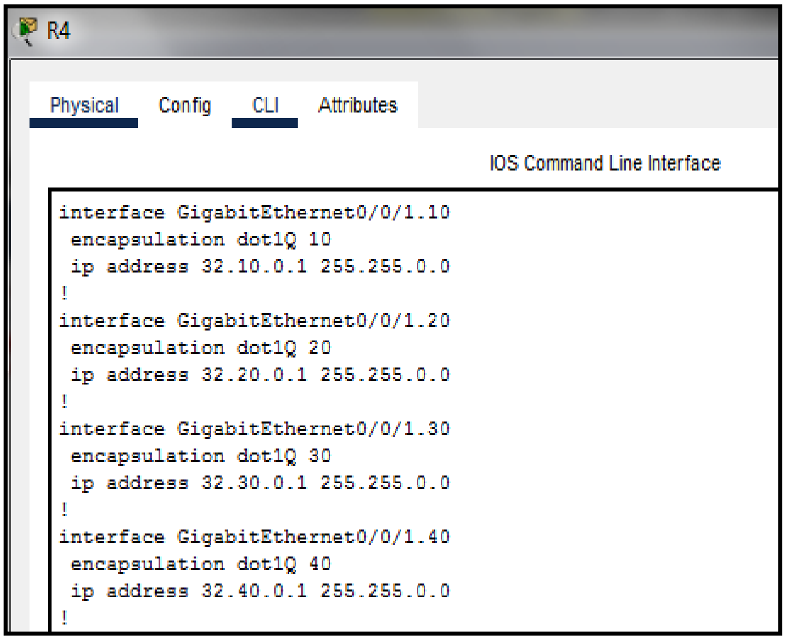
4) Departments Switch:



```
DEPARTMENTS>en
DEPARTMENTS#sh int trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       auto         n-802.1q       trunking      1
Fa0/2       auto         n-802.1q       trunking      1
Fa0/3       auto         n-802.1q       trunking      1
Fa0/4       auto         n-802.1q       trunking      1
Fa0/5       auto         n-802.1q       trunking      1
Fa0/6       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-1005
Fa0/2       1-1005
Fa0/3       1-1005
Fa0/4       1-1005
Fa0/5       1-1005
Fa0/6       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1,10,20,30,40
Fa0/2       1,10,20,30,40
Fa0/3       1,10,20,30,40
Fa0/4       1,10,20,30,40
Fa0/5       1,10,20,30,40
Fa0/6       1,10,20,30,40
```

Figure no. 4.3.1.5: Department Switch

5) Router R4: (InterVLAN Routing)



```
interface GigabitEthernet0/0/1.10
 encapsulation dot1Q 10
 ip address 32.10.0.1 255.255.0.0
!
interface GigabitEthernet0/0/1.20
 encapsulation dot1Q 20
 ip address 32.20.0.1 255.255.0.0
!
interface GigabitEthernet0/0/1.30
 encapsulation dot1Q 30
 ip address 32.30.0.1 255.255.0.0
!
interface GigabitEthernet0/0/1.40
 encapsulation dot1Q 40
 ip address 32.40.0.1 255.255.0.0
!
```

Figure no. 4.3.1.6: Router R4 (InterVLAN Routing)

4.3.2 Hostels (Boys Hostel) & (Girls Hostel) Configuration

1. **Boys Hostel (Hostel-A,B)**

- Created VLANs for Warden and students for Hostel A, B

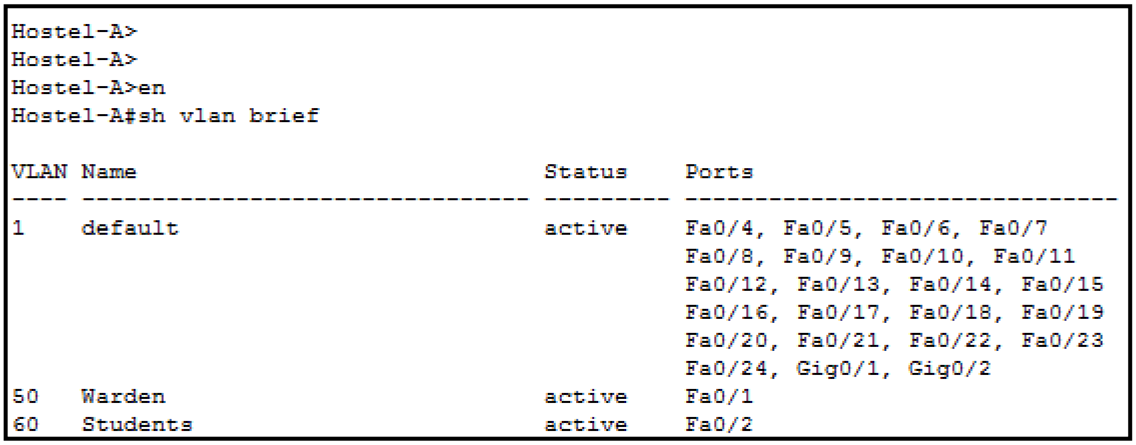
Hostname	Ports	Assignment	Network
PC-21(Warden)	fa0/1	VLAN 50	30.10.0.0
PC-22 (Students)	fa0/2	VLAN 60	30.20.0.0

Table no. 4.3.2.1: Boys Hostel VLANs

- Created trunking ports on Hostel-A,B switch
- Same process is done for Hostel-B

Example of Hostel-A:

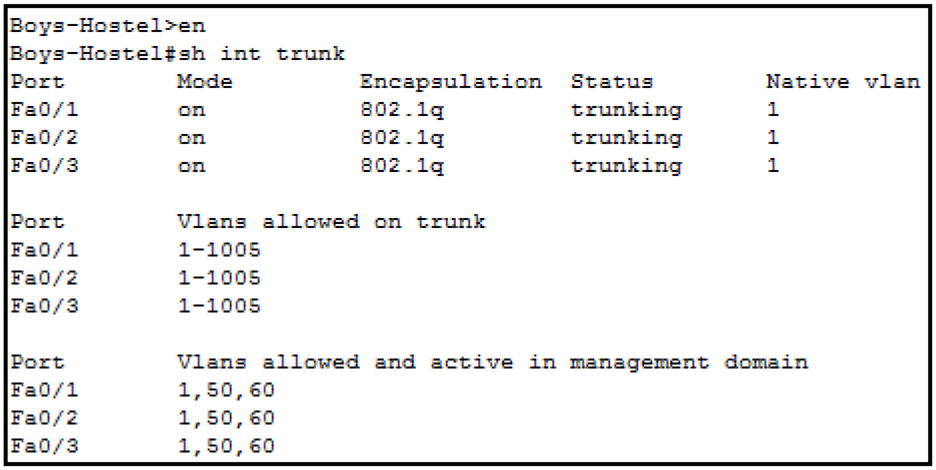
1) Hostel-A Switch



```
Hostel-A>
Hostel-A>
Hostel-A>en
Hostel-A#sh vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/4, Fa0/5, Fa0/6, Fa0/7
                                                Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Fa0/24, Gig0/1, Gig0/2
50   Warden                           active    Fa0/1
60   Students                         active    Fa0/2
```

Figure no. 4.3.2.1: Hostel-A Switch

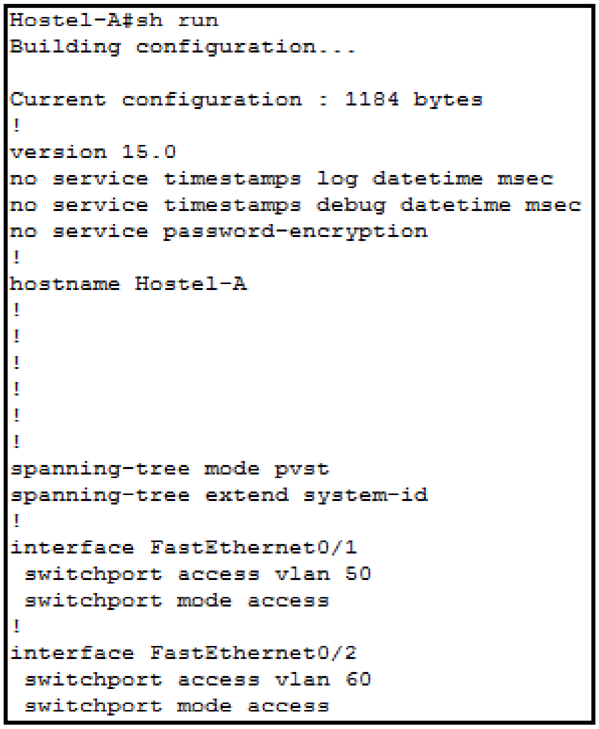
2) Boys-Hostel Switch



```
Boys-Hostel>en
Boys-Hostel#sh int trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      1
Fa0/2       on           802.1q         trunking      1
Fa0/3       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-1005
Fa0/2       1-1005
Fa0/3       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1,50,60
Fa0/2       1,50,60
Fa0/3       1,50,60
```

Figure no. 4.3.2.2: Boys-Hostel Switch

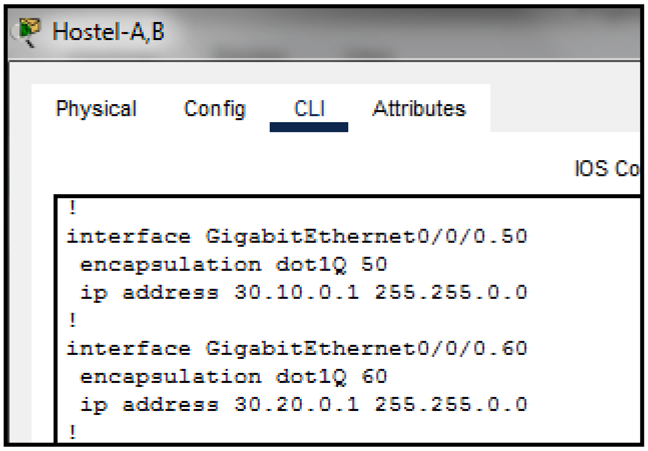
3) Hostel-A Switch



```
Hostel-A#sh run
Building configuration...

Current configuration : 1184 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Hostel-A
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport access vlan 50
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 60
 switchport mode access
```

Figure no. 4.3.2.3: Hostel-A (VLAN Configuration)

4) Router Hostel-A,B



```
!
interface GigabitEthernet0/0/0.50
 encapsulation dot1Q 50
 ip address 30.10.0.1 255.255.0.0
!
interface GigabitEthernet0/0/0.60
 encapsulation dot1Q 60
 ip address 30.20.0.1 255.255.0.0
!
```

Figure no. 4.3.2.4: Router Hostel-A,B (Intervlan Routing)

2. Girls Hostel (Hostel-C,D)

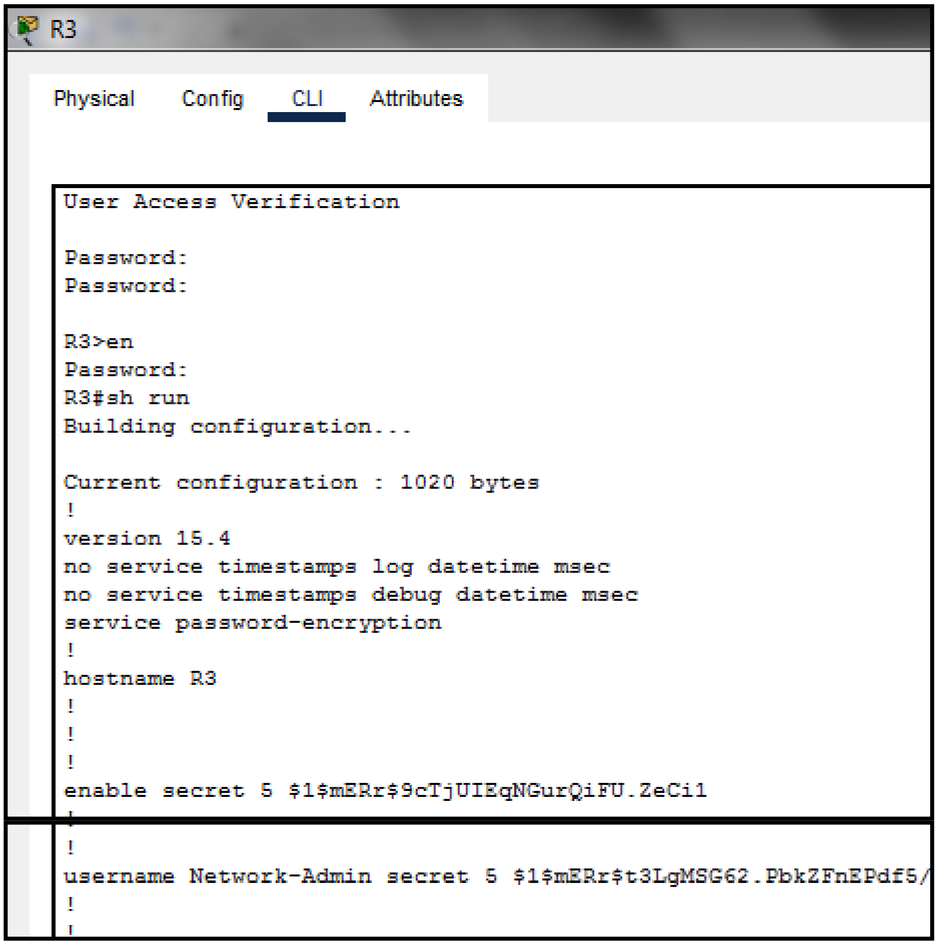
- Created VLANs for Warden and students for Hostel C, D

Hostname	Ports	Assignment	Network
PC-25(Warden)	fa0/1	VLAN 70	40.10.0.0
PC-26 (Students)	fa0/2	VLAN 80	40.20.0.0

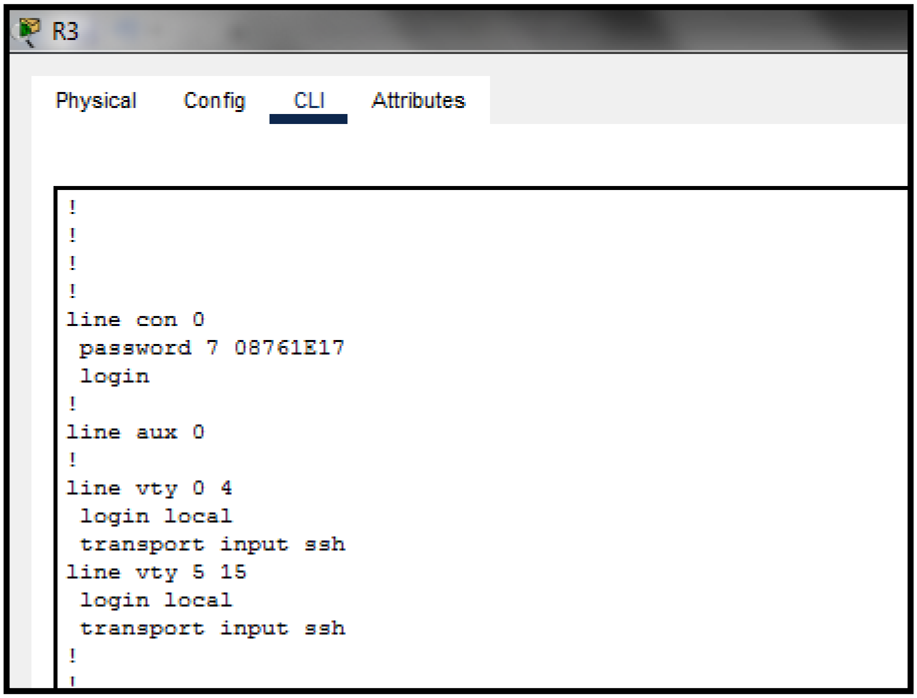
Table no. 4.3.2.2: Girls Hostel VLANs

- Same process is done for Hostel-C,D as done for Hostel-A

4.3.3 SSH Configuration:



```
User Access Verification

Password:
Password:

R3>en
Password:
R3#sh run
Building configuration...

Current configuration : 1020 bytes
!
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname R3
!
!
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
!
username Network-Admin secret 5 $1$mERr$t3LgMSG62.PbkZFnEPdf5/
!
!
```



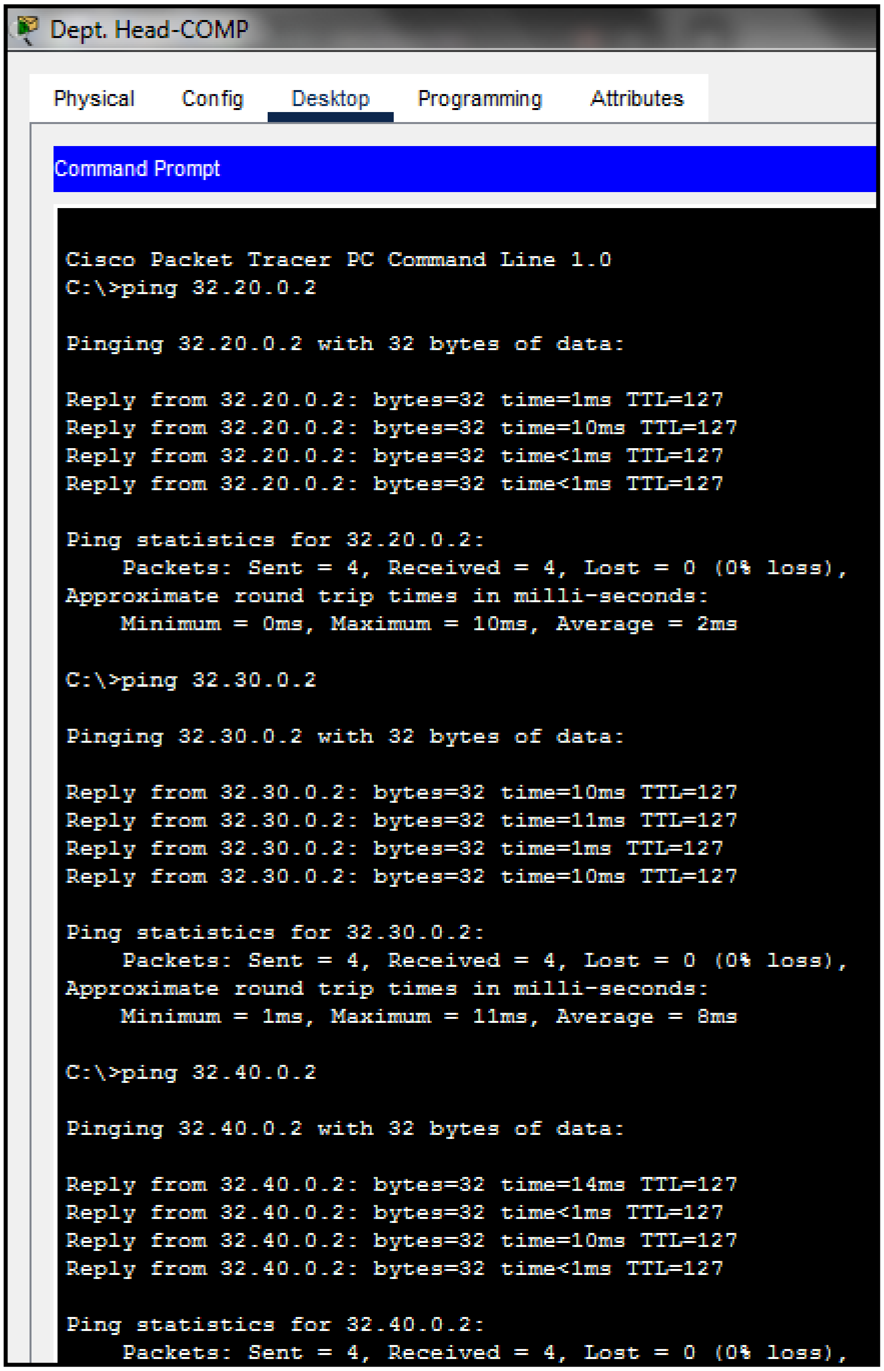
```
!
!
!
!
line con 0
 password 7 08761E17
 login
!
line aux 0
!
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
!
```

Figure no. 4.3.3: SSH Configuration

4.4 Results:

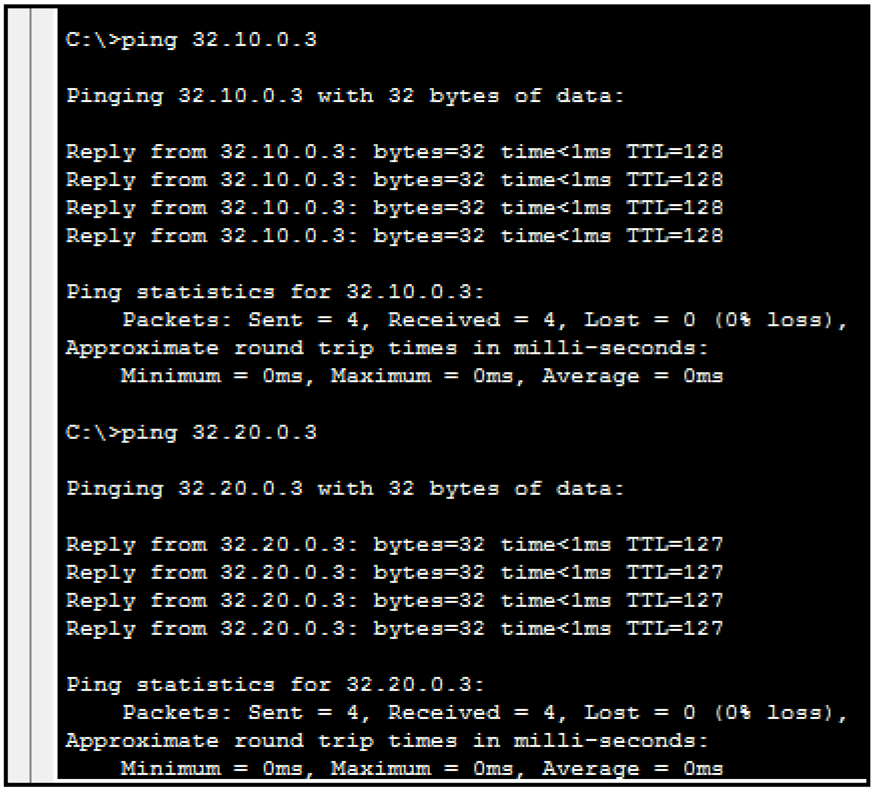
1) Departments:

From Computer Department: Dept. Head can communicate with professors, students, lab of Computer Department and can also communicate with other department's Dept. head, professors, students and lab



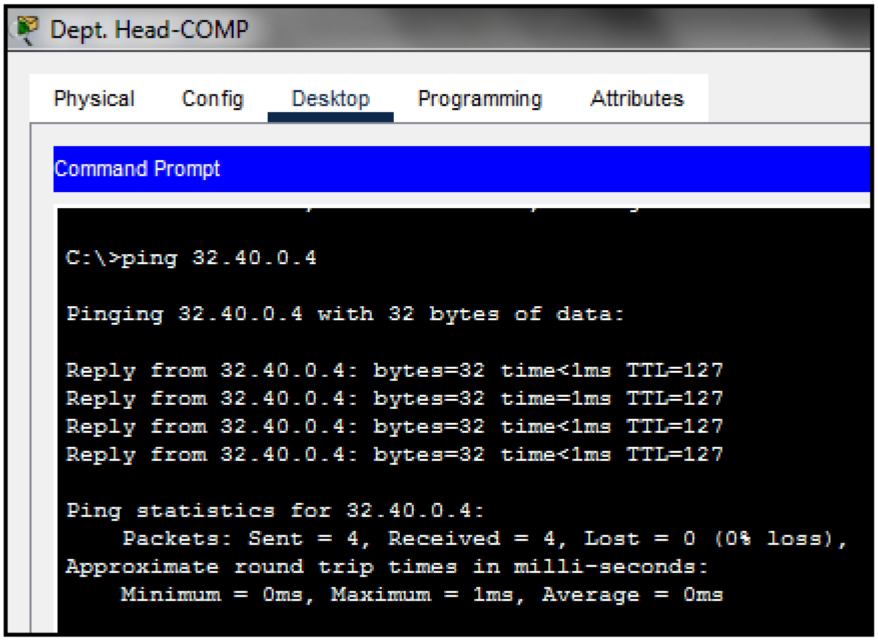
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 32.20.0.2

Pinging 32.20.0.2 with 32 bytes of data:

Reply from 32.20.0.2: bytes=32 time=1ms TTL=127
Reply from 32.20.0.2: bytes=32 time=10ms TTL=127
Reply from 32.20.0.2: bytes=32 time<1ms TTL=127
Reply from 32.20.0.2: bytes=32 time<1ms TTL=127

Ping statistics for 32.20.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 2ms

C:\>ping 32.30.0.2

Pinging 32.30.0.2 with 32 bytes of data:

Reply from 32.30.0.2: bytes=32 time=10ms TTL=127
Reply from 32.30.0.2: bytes=32 time=11ms TTL=127
Reply from 32.30.0.2: bytes=32 time=1ms TTL=127
Reply from 32.30.0.2: bytes=32 time=10ms TTL=127

Ping statistics for 32.30.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 11ms, Average = 8ms

C:\>ping 32.40.0.2

Pinging 32.40.0.2 with 32 bytes of data:

Reply from 32.40.0.2: bytes=32 time=14ms TTL=127
Reply from 32.40.0.2: bytes=32 time<1ms TTL=127
Reply from 32.40.0.2: bytes=32 time=10ms TTL=127
Reply from 32.40.0.2: bytes=32 time<1ms TTL=127

Ping statistics for 32.40.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Figure no. 4.4.1.1: Dept. head PC



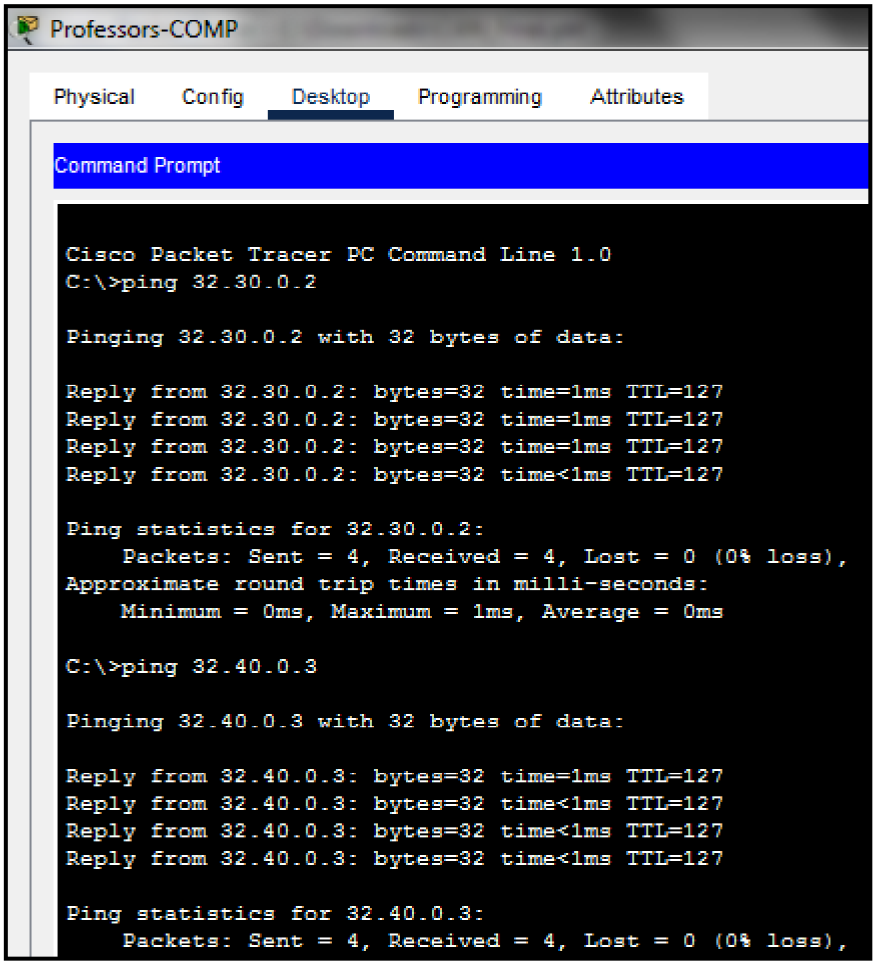
```
C:\>ping 32.10.0.3

Pinging 32.10.0.3 with 32 bytes of data:

Reply from 32.10.0.3: bytes=32 time<1ms TTL=128
Reply from 32.10.0.3: bytes=32 time<1ms TTL=128
Reply from 32.10.0.3: bytes=32 time<1ms TTL=128
Reply from 32.10.0.3: bytes=32 time<1ms TTL=128

Ping statistics for 32.10.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 32.20.0.3

Pinging 32.20.0.3 with 32 bytes of data:

Reply from 32.20.0.3: bytes=32 time<1ms TTL=127
Reply from 32.20.0.3: bytes=32 time<1ms TTL=127
Reply from 32.20.0.3: bytes=32 time<1ms TTL=127
Reply from 32.20.0.3: bytes=32 time<1ms TTL=127

Ping statistics for 32.20.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figure no. 4.4.1.2: Dept. head PC



```
C:\>ping 32.40.0.4

Pinging 32.40.0.4 with 32 bytes of data:

Reply from 32.40.0.4: bytes=32 time<1ms TTL=127
Reply from 32.40.0.4: bytes=32 time=1ms TTL=127
Reply from 32.40.0.4: bytes=32 time<1ms TTL=127
Reply from 32.40.0.4: bytes=32 time<1ms TTL=127

Ping statistics for 32.40.0.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Figure no. 4.4.1.3: Dept. head PC



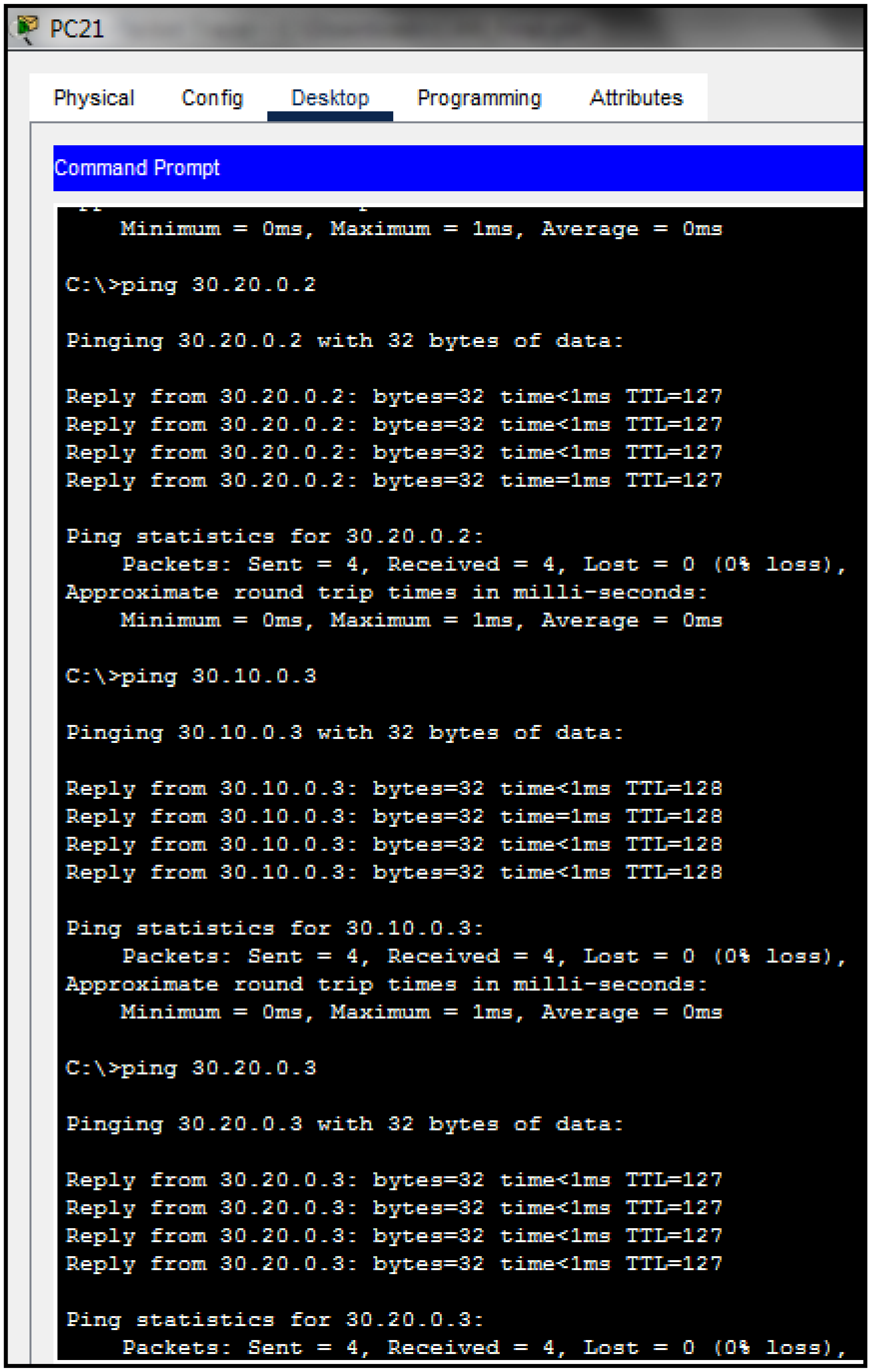
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 32.30.0.2

Pinging 32.30.0.2 with 32 bytes of data:

Reply from 32.30.0.2: bytes=32 time=1ms TTL=127
Reply from 32.30.0.2: bytes=32 time=1ms TTL=127
Reply from 32.30.0.2: bytes=32 time=1ms TTL=127
Reply from 32.30.0.2: bytes=32 time<1ms TTL=127

Ping statistics for 32.30.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 32.40.0.3

Pinging 32.40.0.3 with 32 bytes of data:

Reply from 32.40.0.3: bytes=32 time=1ms TTL=127
Reply from 32.40.0.3: bytes=32 time<1ms TTL=127
Reply from 32.40.0.3: bytes=32 time<1ms TTL=127
Reply from 32.40.0.3: bytes=32 time<1ms TTL=127

Ping statistics for 32.40.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Figure no. 4.4.1.4: Professors PC

Note: Anyone in department can communicate with any other department‘s Dept. head, professors, students and lab.

2) Hostel-A: (Boys-Hostel)

From Hostel-A: Warden from Hostel-A can communicate with students of Hostel-A and also warden, students of Hostel-B

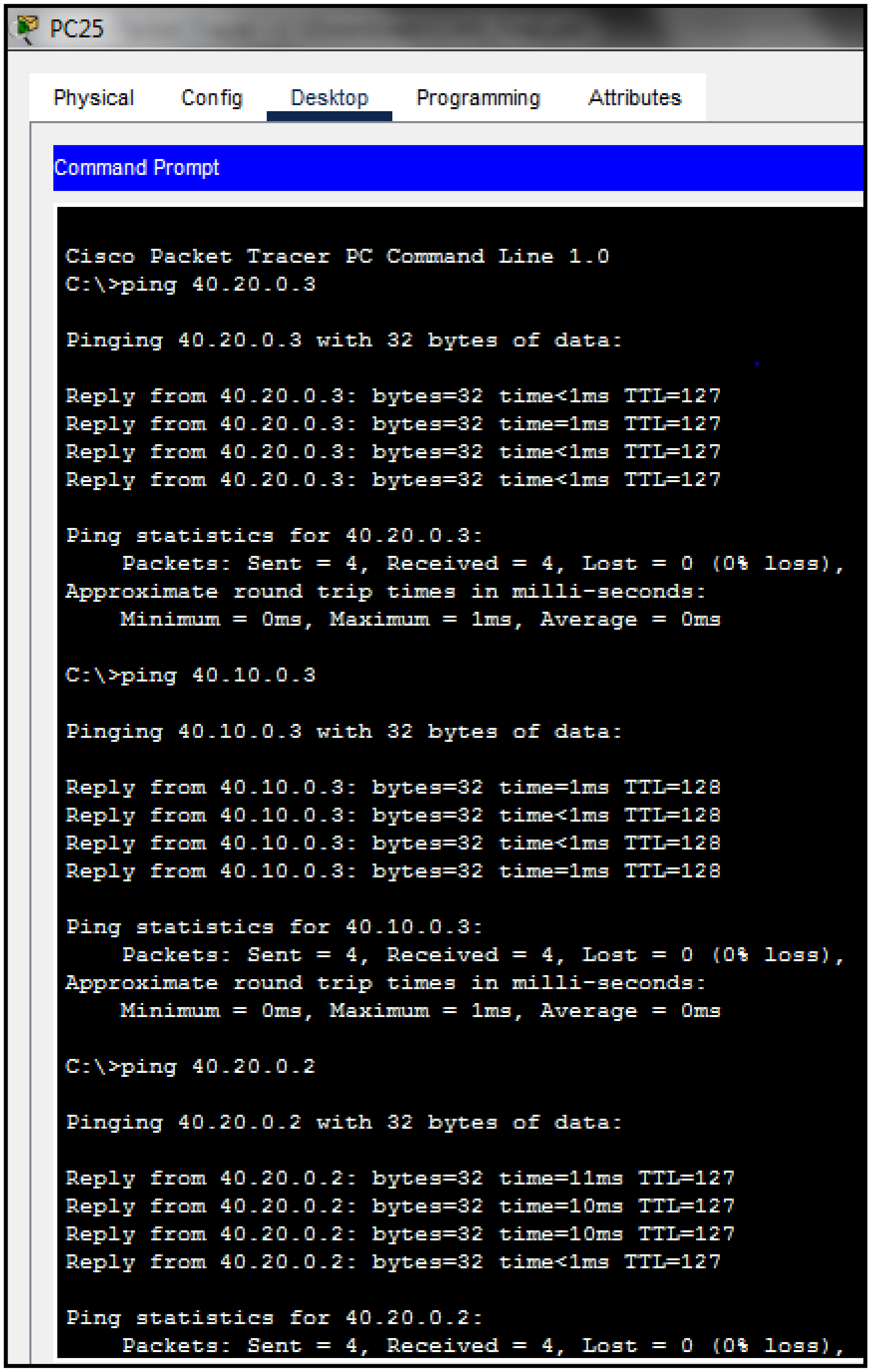


```
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 30.20.0.2

Pinging 30.20.0.2 with 32 bytes of data:

Reply from 30.20.0.2: bytes=32 time<1ms TTL=127
Reply from 30.20.0.2: bytes=32 time<1ms TTL=127
Reply from 30.20.0.2: bytes=32 time<1ms TTL=127
Reply from 30.20.0.2: bytes=32 time=1ms TTL=127

Ping statistics for 30.20.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 30.10.0.3

Pinging 30.10.0.3 with 32 bytes of data:

Reply from 30.10.0.3: bytes=32 time<1ms TTL=128
Reply from 30.10.0.3: bytes=32 time=1ms TTL=128
Reply from 30.10.0.3: bytes=32 time<1ms TTL=128
Reply from 30.10.0.3: bytes=32 time<1ms TTL=128

Ping statistics for 30.10.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 30.20.0.3

Pinging 30.20.0.3 with 32 bytes of data:

Reply from 30.20.0.3: bytes=32 time<1ms TTL=127
Reply from 30.20.0.3: bytes=32 time<1ms TTL=127
Reply from 30.20.0.3: bytes=32 time<1ms TTL=127
Reply from 30.20.0.3: bytes=32 time<1ms TTL=127

Ping statistics for 30.20.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Figure no. 4.4.2: Hostel-A Warden's PC

3) Hostel-C: (Girls-Hostel)

From Hostel-A: Warden from Hostel-C can communicate with students of Hostel-C and also warden, students of Hostel-D



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 40.20.0.3

Pinging 40.20.0.3 with 32 bytes of data:

Reply from 40.20.0.3: bytes=32 time<1ms TTL=127
Reply from 40.20.0.3: bytes=32 time=1ms TTL=127
Reply from 40.20.0.3: bytes=32 time<1ms TTL=127
Reply from 40.20.0.3: bytes=32 time<1ms TTL=127

Ping statistics for 40.20.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 40.10.0.3

Pinging 40.10.0.3 with 32 bytes of data:

Reply from 40.10.0.3: bytes=32 time=1ms TTL=128
Reply from 40.10.0.3: bytes=32 time<1ms TTL=128
Reply from 40.10.0.3: bytes=32 time<1ms TTL=128
Reply from 40.10.0.3: bytes=32 time=1ms TTL=128

Ping statistics for 40.10.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 40.20.0.2

Pinging 40.20.0.2 with 32 bytes of data:

Reply from 40.20.0.2: bytes=32 time=11ms TTL=127
Reply from 40.20.0.2: bytes=32 time=10ms TTL=127
Reply from 40.20.0.2: bytes=32 time=10ms TTL=127
Reply from 40.20.0.2: bytes=32 time<1ms TTL=127

Ping statistics for 40.20.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Figure no. 4.4.3: Hostel-C Warden's PC

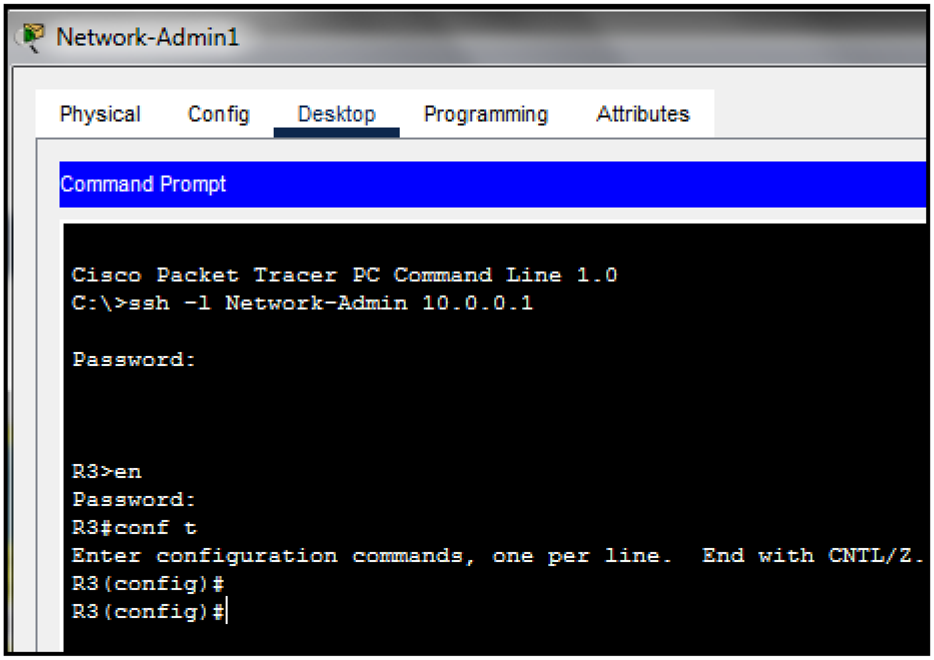
4) SSH:

1) Network-Admin1:

Using SSH, network-admin can remotely access Network- admin‘s Router and Switch

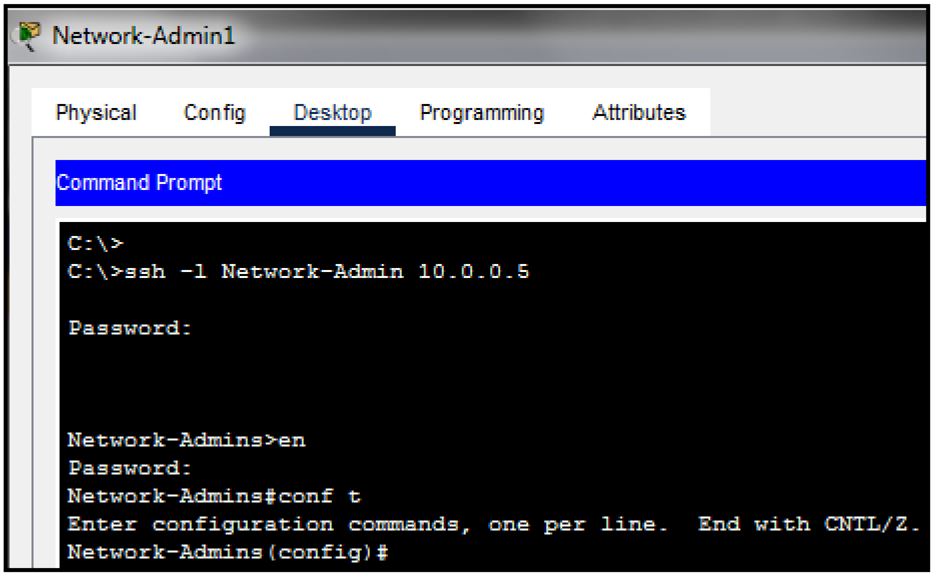
Username - Network-Admin Password – network-admin

Password - class



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l Network-Admin 10.0.0.1

Password:



R3>en
Password:
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#
R3(config)#
```

Figure no. 4.4.4.1: SSH Configuration (Router)



```
C:\>
C:\>ssh -l Network-Admin 10.0.0.5

Password:



Network-Admins>en
Password:
Network-Admins#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Network-Admins(config)#
```

Figure no. 4.4.4.2: SSH Configuration (Switch)

Chapter 5

Conclusion and Future Scope

This Chapter presents the conclusion & future work of the implemented project.

5.1 Conclusion:

- Network architecture and its security are necessary for any organization.
- As network security has become more and more important, the proper protection have to be built to achieve the open and secure network environment we aimed for.
- We used bus topology to design the campus network. Campus Network consists of Data-Centre, Network Admin office, Boys & Girls hostel, Reception area, 5 departments and library. The server consists of 4 servers viz. DNS, HTTP, SMTP, and FTP. As every entity is in different network we created virtual LANs in which with the help of inter-VLAN routing we can communicate with different networks.
- Maintenance of high efficiency of campus network is main problem that need to be resolved.

5.2 Future Work:

- Creating OSPFs, ACLs and implementing ASA firewall
- Limiting bandwidth and access to internet to specific users in the network
- Conduct a survey at data center to learn about possible attacks and disaster recovery and thereby implementing it on mininet software.
- Identify and analyze threats and take preventive measures
- Validation of Small network using Hardware Setup.

5.3 Timeline:

Semester 7	**Semester 8**
• Literature Survey of Project. • Design of Secured Robust Campus Area Network. • Creation of VLANs, InterVLAN's Communication and SSH.	• Creation OSPFs, ACLs and implementing firewall for internal and externalsecurity of network. • For security of the network, we will identify the threats which can happen in a campus area network and analyze them. • Validation of Small network using Hardware Setup.

Figure no.5.3: Timeline

References:

1. Mugdha Sharma, Chirag Pupreja, Akash Arora "Design and Implementation of University Network" July 2019 International Journal of Recent Technology and Engineering (IJRTE)
URL: https://www.ijrte.org/wp-content/uploads/papers/v8i2S6/B11740782S619.pdf

2. S. Sudharsan, M. Naga Srinivas, G. Sai Shabareesh, P.Kiran Rao "Campus Network Security and Management" November-December 2014 International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
URL: https://www.ijettcs.org/Volume3Issue6/IJETTCS-2014-11-21-53.pdf

3. Lalita Kumari Radhey Shyam Swapan Debbarma "Security Problems in Campus Problems and its solutions" January 2011 ResearchGate
URL:https://www.researchgate.net/publication/224771078_Security_Problems_in_Campus_Network_and_Its_Solutions

4. G.Michael "Design and Implementation of a Secure Campus Network" 2017 International Journal of Pure and Applied Mathematics(IJPAM)
URL: https://acadpubl.eu/jsi/2017-116-8/articles/8/51.pdf

5. Thin Naing , Aung Nway " Design and Implementation of a Secure Network Connection of the University" IJARIIE-ISSN(O)
URL:http://ijariie.com/AdminUploadPdf/DESIGN_AND_IMPLEMENTATION_OF_A_SECURE_NETWORK_CONNECTION_OF_THE_UNIVERSITY_ijariie10277.pdf

6. Md. Nadir Bin Ali "Design and Implementation of a Secure Campus Network" July 2015 ResearchGate
URL:https://www.researchgate.net/publication/299482260_Design_and_Implementation_of_a_Secure_Campus_Network

7. Zaka Ullah Muhammad Zulkifl Hasan "Implementation Challenges in Campus Network Security" November 2017 ResearchGate
URL:https://www.researchgate.net/publication/321360769_Implementation_challenges_in_Campus_Network_security

8. Khaing Khaing Wai,Thuzar Khin ,Khin Thet Mar "Design and Simulation of Campus Area Network Using Cisco Packet Tracer" 2019 International Journal of New Technologies in Science and Engineering
URL: http://ijntse.com/upload/1564122549final%20paper.pdf

9. Joysankar Bhattacharjee "Design and Implementation of a Cost-effective and Secured Private Area Network for smooth as well as hassle-free Computing in the University Campus" Jan - Feb 2016 IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
URL:https://www.iosrjournals.org/iosr-jece/papers/Vol.%2011%20Issue%201/Version-1/K011117277.pdf

10. Bagus Mulyawan “Campus Network Design And Implementation Using Top Down Approach” 2011 International Conference on Information Systems For Business Competitiveness (ICISBC)
URL: http://eprints.undip.ac.id/36065/1/bagus_mulyawan.pdf

11. Mohammed Nadir Bin Ali Prof. Dr. M. Lutfar Rahman Prof. Dr. Syed Akhter Hossain “Network Architecture and Security Issues in Campus” **2013** Networks Institute of Electrical and Electronics Engineers(IEEE)
URL: https://ieeexplore.ieee.org/document/6726595

12. Yaxun Lan Zhengshi Chen “The research on the OSPF security optimizing of Campus Network” 2015 Institute of Electrical and Electronics Engineers(IEEE)
URL: https://ieeexplore.ieee.org/document/7311959

Acknowledgements:

We would like to thank K. J. Somaiya College of Engineering for allowing us to work on this topic for our LY project. We are grateful to our principal Dr. Shubha Pandit as well as our HOD Dr. Bharti Singh for providing such an opportunity to us.

We would like to express our gratitude to Dr. Kiran Ajetrao, our project guide, for letting us perform this project under his valuable guidance. We are extremely grateful to him for giving his valuable time and attention. We have learned some very important skills from him in the duration of this semester 7 and look forward to learn even more in the next semester.