

Networking Topology in Thapar University

CISCO VIRTUAL INTERNSHIP PROGRAM 2023

By

Sushant Vij (102003759)



THAPAR INSTITUTE
OF ENGINEERING & TECHNOLOGY
(Deemed to be University)

Under the Guidance of

Dr. Gurpal Singh Chhabra

(June,2023-July,2023)

Department of Computer Science

Thapar University of Engineering and Technology

CERTIFICATE

Date: 19/07/2023

This is to certify that the project work entitled “Networking in University” submitted by Sushant Vij in fulfillment for the requirements of the award of Bachelor of Technology Degree in ComputerEngineering, from Thapar University is an authentic work carried out by them under my supervision and guidance. To the best of my knowledge, the matter embodied in the project has not been submitted to any other University / Institute for the award of any Degree.

Dr. Gurpal Singh Chhabra
Project Guide
Department of Computer Science
Thapar University of Engineering and Technology

ABSTRACT

Computer networks have a significant impact on the working of an organization. Universities depend on the proper functioning and analysis of their networks for education, administration, communication, e-library, automation, etc. An efficient network is essential to facilitate the systematic and cost-efficient transfer of information in an organization in the form of messages, files, and resources. The project provides insights into various concepts such as topology design, IP address configuration, and how to send information in the form of packets to the wireless networks of different areas of a University.

The aim of this project is to design the topology of the university network using the software Cisco Packet Tracer with the implementation of wireless networking systems. This university network consists of the following devices:

- 1) Router (1941)
- 2) Switches (2960-24TT)
- 3) Email server
- 4) DNS server
- 5) WEB server (HTTP)
- 6) Wireless Device (Access Point)
- 7) PCs
- 8) Laptops
- 9) Smartphones

The design includes the following parts of the University:

Hostel Blocks: Girls Hostel and Boys Hostel

Academic Blocks: LP and LT, Mech, ELE and other branches

CSED Lab and Library

TABLE OF CONTENTS

1.	Cover Page	1
2.	Certificate	2
3.	Abstract	3
4.	Table of Contents	4
5.	Chapter 1: Introduction	5
6.	Chapter 2: Literature Review	6
7.	Chapter 3: Work Done	10
8.	Chapter 4: Attack Surface Mapping and Results	25
9.	Chapter 5: Conclusions and Future Work	29
10.	References	30

CHAPTER 1

INTRODUCTION

● **Motivation**

The word “digital” is very significant in today’s world, with an increase in the development of technology the entire world is moving towards the digital era. The educational institution plays an important role in this digitalization, hence the campus should adapt to digital means of networking as well and become a “digital campus”. Going wireless plays an important role in this digitalization. The wireless network makes the connection easy with a reduction in the use of wires or cables. A wired connection makes it difficult to keep track of all the devices and to manage the cable connection, which is not only chaotic but also challenging to handle.

Campus networking via wireless connection becomes an important part of campus life and provides the main way for teachers and students to access educational resources, which gives an important platform to exchange information. As laptops and intelligent terminals are widely used, demand for access to information anytime and anywhere has become more and more urgent, but traditional cable networks cannot meet this requirement. Then wireless network construction becomes necessary and essential. The wireless network is one of the important components of a digital campus and wisdom campus. It provides an efficient way to explore the internet with a mobile terminal for teachers and students regardless of cables and places. This is an important mark of the modern campus as a supplement of a cable network. With the development of network and communication technology, cable networks on a university campus bring much convenience for teaching and research work. But for mobility and flexibility, it has obvious shortcomings. A wireless network can overcome these drawbacks and has been applied to the university campus.

● **Project Statement**

Choose a university/college campus and analyze its network topology. Map the network using Cisco Packet Tracer and identify the security controls that are in place, such as network segmentation, intrusion detection systems, firewalls, and authentication and authorization systems. Apply the knowledge gained from the NetAcad cyber security course to conduct an attack surface mapping, aiming to identify potential entry points for cyber-attacks. Propose countermeasures to mitigate these risks.

Tasks:

1. Campus Network Analysis: Choose a university or college campus and conduct an analysis of its existing network topology, including the layout, devices, and connections.
2. Network Mapping: Utilize Cisco Packet Tracer to map the network infrastructure, representing the placement and interconnectivity of routers, switches, firewalls, and other relevant network components.
3. Attack Surface Mapping: Conduct an attack surface mapping exercise to identify potential vulnerabilities and weaknesses within the network architecture and design,

considering factors such as unauthorized access, data breaches, and network availability.

4. Secure Access Controls: Incorporate appropriate security controls (e.g., VLANs, IDP/IPS, VPN, Firewalls, password management, vulnerability management etc.) in your design to enhance security posture.

Deliverables:

1. Network topology diagram depicting the existing infrastructure and attack surface findings.

2. Security assessment report highlighting identified security risks, proposed solutions, and countermeasures to mitigate attack surface risks.

CHAPTER 2

LITERATURE REVIEW

- What is 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. Packet Tracer makes use of a drag-and-drop user interface, allowing users to add and remove simulated network devices as they see fit. The software is mainly focused on Certified Cisco Network Associate Academy students as an educational tool for helping them learn fundamental CCNA concepts. Previously students enrolled in a CCNA Academy program could freely download and use the tool free of charge for educational use.

- Router

A router is a device like a switch that routes data packets based on their IP addresses. The router is mainly a Network Layer device. Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets. Router divides broadcast domains of hosts connected through it.

- Switch

A network switch (also called switching hub, bridging hub, officially MAC bridge is networking hardware that connects devices on a computer network by using packet switching to receive and forward data to the destination device. A network switch is a multiport network bridge that uses MAC addresses to forward data at the data link layer (layer 2) of the OSI model. Some switches can also forward data at the network layer (layer 3) by additionally incorporating routing functionality. Such switches are commonly known as layer-3 switches or multilayer switches.

- Network Packet

A network packet is a formatted unit of data carried by a packet-switched network. A packet consists of control information and user data, which is also known as the payload.

- Server

A server is a computer or system that provides resources, data, services, or programs to other computers, known as clients, over a network. In theory, whenever computers share resources with client machines they are considered servers. There are many types of servers, including web servers, mail servers, and virtual servers.

Many networks contain one or more of the common servers. The servers used in our project are as follows:

- DNS Server

DNS stands for Domain Name System servers which are application servers that provide a human-friendly naming method to the user computers in order to make IP addresses readable by users. The DNS system is a widely distributed database of names and other DNS servers, each of which can be used to request an otherwise unknown computer name. When a user needs the address of a system, it sends a DNS request with the name of the desired resource to a DNS server. The DNS server responds with the necessary IP address from its table of names.

- WEB Server

One of the widely used servers in today's market is a web server. A web server is a special kind of application server that hosts programs and data requested by users across the Internet or an intranet. Web servers respond to requests from browsers running on client computers for web pages, or other web-based services.

- EMAIL Server

An e-mail server is a server that handles and delivers e-mail over a network, using standard email protocols. For example, the SMTP protocol sends messages and handles outgoing mail requests. The POP3 protocol receives messages and is used to process incoming mail. When you log on to a mail server using a webmail interface or email client, these protocols handle all the connections behind the scenes.

- Wireless Network

A wireless network broadcasts an access signal to the workstations or PCs. This enables mobility among laptops, tablets, and PCs from room to room while maintaining a firm network connection continuously. A wireless network also presents additional security requirements.

- Ethernet

This is the backbone of our network. It consists of the cabling and is typically able to transfer data at a rate of 100mb/s. It is a system for connecting a number of computer systems to form a local area network, with protocols to control the passing of information and to avoid simultaneous transmission by two or more systems. Among the different types of ethernet, we have used Gigabit Ethernet, which is a type of Ethernet network capable of transferring data at a rate of 1000 Mbps and fast Ethernet is a type of Ethernet network that can transfer data at a rate of 100 Mbps.

- Computing Device

Computing devices are the electronic devices that take user inputs, process the inputs, and then provide us with the end results. These devices may be Smartphones, PC Desktops, Laptops, printer, and many more.

- Internet Protocol

Internet Protocol (IP) is one of the fundamental protocols that allow the internet to work. IP addresses are a unique set of numbers on each network and they allow machines to address each other across a network. It is implemented on the internet layer in the IP/TCP model.

- SSH Protocol

Secure Shell enables a user to access a remote device and manage it remotely. However, with SSH, all data transmitted over a network (including usernames and passwords) is encrypted and secure from eavesdropping.

SSH is a client-server protocol, with an SSH client and an SSH server. The client machine (such as a PC) establishes a connection to an SSH server running on a remote device (such as a router). Once the connection has been established, a network admin can execute commands on the remote device.

- Benefits of wireless networking over wired networking^[5]

To better understand the wide usage of wireless networking in today's world, is to start with the benefits it has over traditional wired networking is crucial for our project implementation. Some major aspects have been stated below that show the various advantages of a wireless network over wired ones.

1. Mobility

One of the major advantages of wireless is mobility. Users have the freedom to move within the area of the network with their computing devices staying connected to a network without being concerned about the cable connection.

2. Less Hassle

The wireless network helps in the reduction of large amounts of cables or wires which becomes chaotic and difficult to maintain, it makes the connection hassle-free.

3. Accessibility

Provide network access across your organization, even in areas that have been challenging to reach with the wired network, so your entire team can stay in touch.

4. Expandability

The wireless network helps in the expansion of the network to a wide range by adding multiple new users and locations without additional need to run cables and wires.

5. Guest Access

Offer secure network access to guest users, including customers and business partners, while keeping your network resources protected.

With lots of advantages, there come disadvantages as well, like security issues which can be resolved using strict protection passwords. Also, the Speed of wireless networks is considered to be slow and having low bandwidth when compared to the direct cable connection networks.

- Simulation Environment

The simulations of our network topology can be easily achieved using cisco packet tracer. Using a simulation mode, you can see packets flowing from one node to another and can also click on a packet to see detailed information about the OSI layers of the networking. Packet Tracer offers a huge platform to combine realistic simulation and visualize them simultaneously. Cisco Packet Tracer makes learning and teaching significantly easier by supporting multi-user collaboration and by providing a realistic simulation environment for experimenting with projects.

CHAPTER 3

WORK DONE

In order to make our project understandable, we have divided the content into steps. They are as follows:

1. Software and hardware requirements

Before heading towards the implementation we need to make sure of the following requirements.

- A proper workstation (any mid-high range laptop will suffice).
- Packet Tracer by Cisco
- 8 GB RAM.
- Any 10,000+ Average CPU Mark scored processor.
- 16 GB of dedicated hard disk space.
- USB 3.0+ port.

2. Brief knowledge about our approach

The proposed wireless network is implemented for a university campus. We have made a virtual visualization of the network using the Cisco Packet tracer which provides a huge platform for users to test their projects using simulation tools. A Wireless network in an educational campus makes it easier for teachers and students to access educational resources, by enabling an important platform to exchange information.

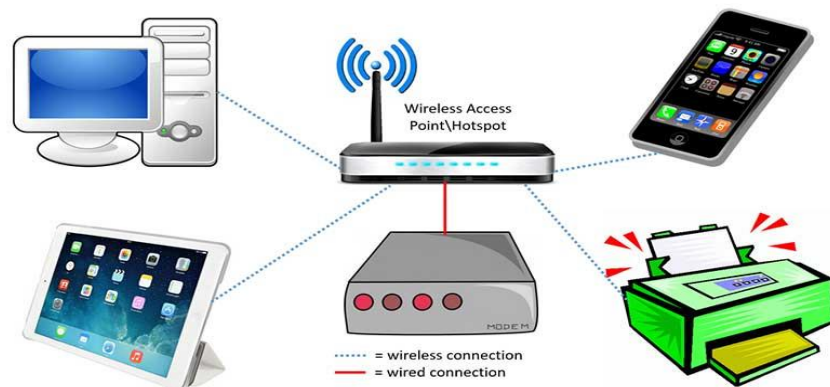


Figure 1: Shows the wireless connection access by various tool

3.) Network Requirements

Thapar University, Patiala outline is considered for this wireless university network.
The network is divided into 2 areas :

1. Campus Area

The Campus area is further divided into various accessing points like CSED LAB building, Library, LP and LT and other branches Server Center, and registry office and accounts office .

2. Hostel Area

The Hostel area is further divided into Boys blocks and Girls blocks respectively.

Figure 2: Basic layout of our wireless access points in University

Devices Used In The Network

Devices	Quantity
1) Router (1941)	3
2) Switches (2960-24TT)	3
3) EMAIL server	1
4) DNS server	1
5) WEB server (HTTP)	1
6) Wireless Device (Access Point)	7
7) PCs	12
8) Laptops	10
9) Smartphones	2

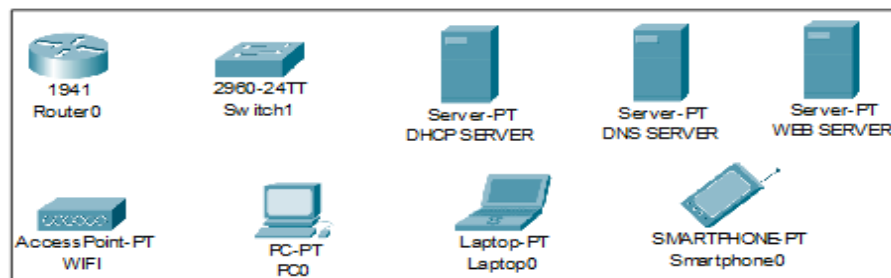
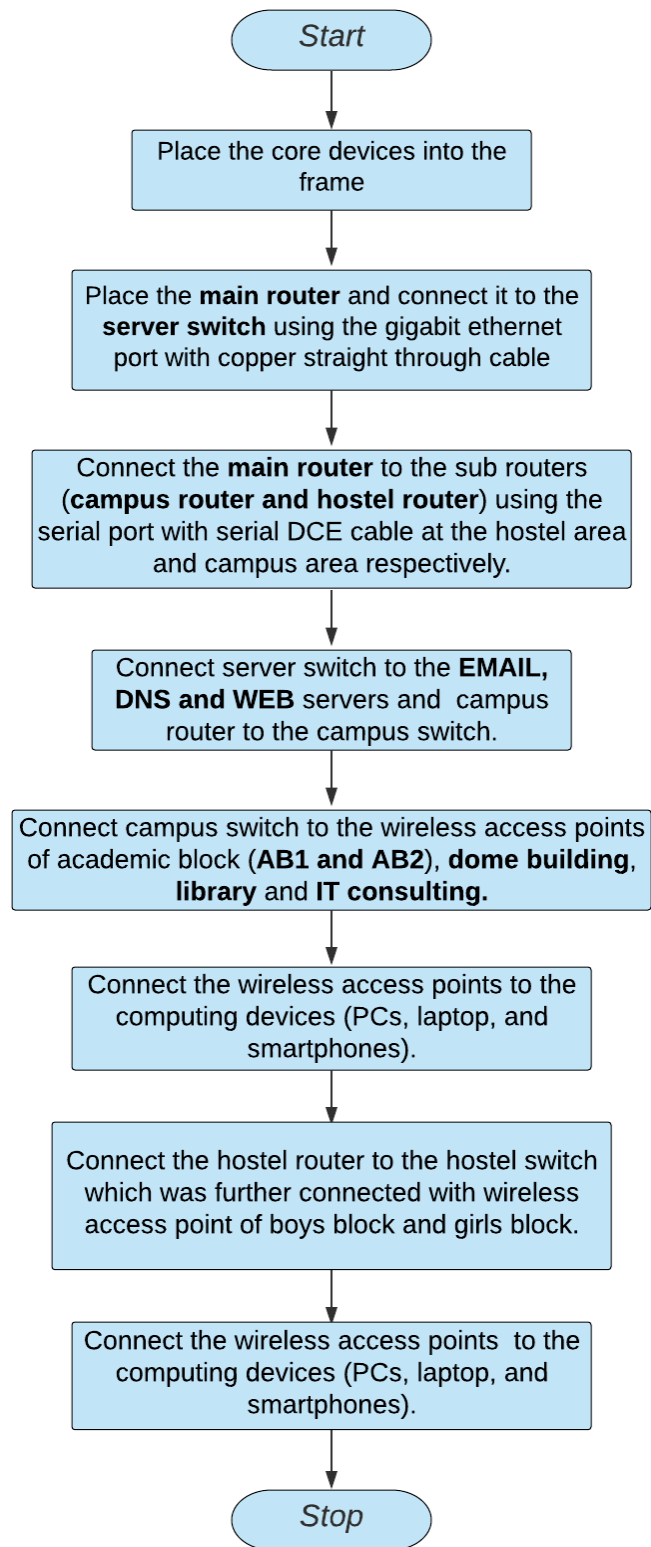


Figure 3: Devices used in the network

3. Implementation and Flow Diagram

- To design the wireless network of the university we initially started by placing the core devices into the frame as mentioned in the layout.
- Firstly, we placed the **main router** at the center of the university outline, which was further connected to the **server switch** using the gigabit ethernet port with copper straight-through cable and sub routers (**campus router and hostel router**) using the serial port with serial DCE cable at the hostel area and campus area respectively.
- The server switch was further connected to the **EMAIL, DNS, and WEB** servers respectively.
- Campus router was connected to the campus switch which was further connected with wireless access points of the academic block LP and LT ,other branches classes **CSED LAB , library, and LP and LT .**
- The wireless access points were then connected to computing devices (PCs, laptops, and smartphones).
- Similarly, the hostel router was connected to the hostel switch which was further connected with the wireless access point of boys block and girls block.
- The wireless access points were then connected to the computing devices (PCs, laptops, and smartphones), every area has a dedicated access point which can only be connected with the help of a password.
- All these connections are made through ethernet ports (gigabit ethernet and fast ethernet) using copper straight-through cables.



This is the flow diagram for a better understanding of the steps mentioned above.

4. Configuring IP Addresses

We have attached the screenshots of all the IP configuration below:

- Main Router configuration

Global Settings	
Display Name	<input type="text" value="main_router"/>
Hostname	<input type="text" value="main_router"/>
NVRAM	<input type="button" value="Erase"/> <input type="button" value="Save"/>
Startup Config	<input type="button" value="Load..."/> <input type="button" value="Export..."/>
Running Config	<input type="button" value="Export..."/> <input type="button" value="Merge..."/>

GigabitEthernet0/1

IP Configuration	
IP Address	<input type="text" value="192.168.2.1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>

Serial0/1/0

IP Configuration	
IP Address	<input type="text" value="10.0.0.1"/>
Subnet Mask	<input type="text" value="255.0.0.0"/>

Serial0/1/1

IP Configuration	
IP Address	<input type="text" value="11.0.0.1"/>
Subnet Mask	<input type="text" value="255.0.0.0"/>

RIP

Network Address
10.0.0.0
11.0.0.0
192.168.1.0
192.168.2.0

- DNS SERVER

IP Configuration

☐ DHCP ☒ Static

IP Address

Subnet Mask

Default Gateway

DNS Server

Global Settings

Display Name

Gateway/DNS IPv4

☐ DHCP ☒ Static

Gateway

DNS Server

- WEB SERVER

IP Configuration

☐ DHCP ☒ Static

IP Address

Subnet Mask

Default Gateway

DNS Server

Global Settings

Display Name

Gateway/DNS IPv4

☐ DHCP ☒ Static

Gateway

DNS Server

- EMAIL SERVER

IP Configuration

☐ DHCP
 ☒ Static

IP Address: 192.168.2.2
 Subnet Mask: 255.255.255.0
 Default Gateway: 192.168.2.1
 DNS Server: 192.168.2.3

Global Settings

Display Name: EMAIL

Gateway/DNS IPv4
☐ DHCP
☒ Static

Gateway: 192.168.2.1
 DNS Server: 192.168.2.3

- COLLEGE ROUTER

Global Settings		Network Address
Display Name	College Router	11.0.0.0
Hostname	Router1	192.168.1.0

GigabitEthernet0/0

IP Configuration

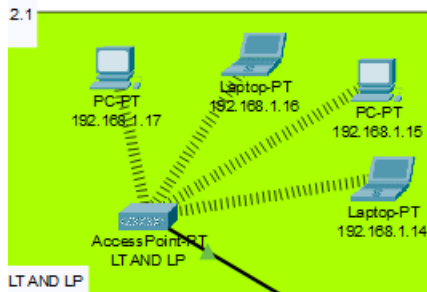
IP Address: 192.168.1.1
 Subnet Mask: 255.255.255.0

Serial0/1/0

IP Configuration

IP Address: 11.0.0.2
 Subnet Mask: 255.0.0.0

- LP AND LT



IP Address are as follows

192.168.1.14- Laptop

192.168.1.15- PC

192.168.1.16- Laptop

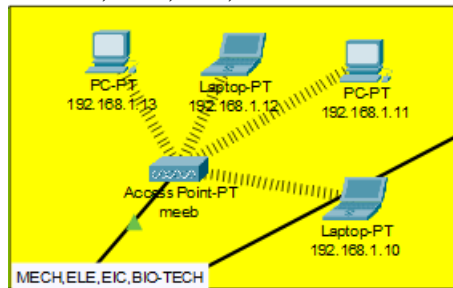
192.168.1.17- PC

Subnet Mask- 255.255.255.0

Default Gateway- 192.168.1.1

DNS Server- 192.168.2.3

- MECH,ELE,EIC,BIO-TECH



IP Address are as follows

192.168.1.10- Laptop

192.168.1.11- PC

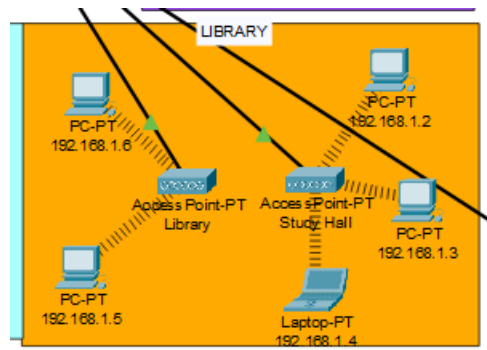
192.168.1.12- Laptop

192.168.1.13- PC

Subnet Mask- 255.255.255.0

Default Gateway- 192.168.1.1

DNS Server- 192.168.2.3



- LIBRARY

IP Addresses are as follows

192.168.1.2- PC

192.168.1.3- PC

192.168.1.4- Laptop

Subnet Mask- 255.255.255.0

Default Gateway- 192.168.1.1

DNS Server- 192.168.2.3

IP Addresses are as follows

192.168.1.5- PC

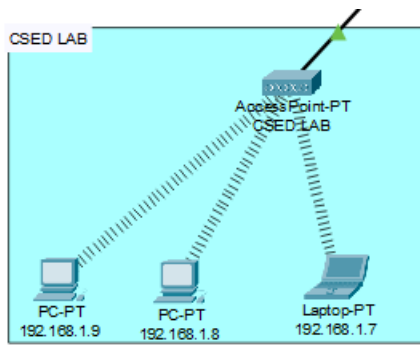
192.168.1.6- PC

Subnet Mask- 255.255.255.0

Default Gateway- 192.168.1.1

DNS Server- 192.168.2.3

- CSED LAB



IP Addresses are as follows
 192.168.1.7- Laptop
 192.168.1.8- PC
 192.168.1.9- PC
 Subnet Mask- 255.255.255.0
 Default Gateway- 192.168.1.1
 DNS Server- 192.168.2.3

- HOSTEL ROUTER

Global Settings		Network Address
Display Name	Hostel Router	10.0.0.0
Hostname	Router2	192.168.3.0

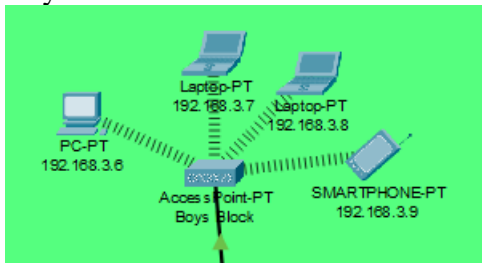
GigabitEthernet0/0

IP Configuration	
IP Address	192.168.3.1
Subnet Mask	255.255.255.0

Serial0/1/0

IP Configuration	
IP Address	10.0.0.2
Subnet Mask	255.0.0.0

- Boys Hostel



IP Addresses are as follows

192.168.3.6- PC

192.168.3.7-Laptop

192.168.3.8- PC

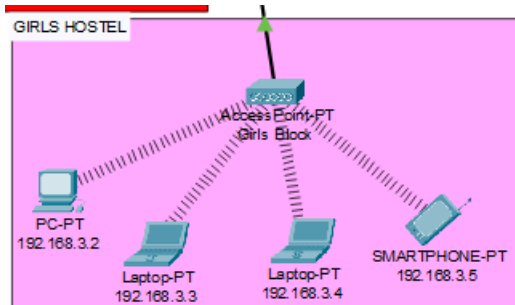
192.168.3.9- Smartphone

Subnet Mask- 255.255.255.0

Default Gateway- 192.168.3.1

DNS Server- 192.168.2.3

- Girls Hostel



IP Addresses are as follows

192.168.3.2- PC

192.168.3.3-Laptop

192.168.3.4- PC

192.168.3.5- Smartphone

Subnet Mask- 255.255.255.0

Default Gateway- 192.168.3.1

DNS Server- 192.168.2.3

- WIRELESS ACCESS POINT

SSID	Password
------	----------

1)tiet_hall	1234567890
2)tiet_library	1234567890
3)tiet_lab	1234567890
4)tiet_LP<	1234567890
5)tiet_meeb	1234567890
6)tiet_boys	1234567890
7)tiet_girls	1234567890

Port 1

Port Status

☒ On

SSID

Tiet_hall

2.4 GHz Channel

6

Coverage Range (meters)

140.00

Authentication

☐ Disabled
☒ WEP
☐ WPA-PSK
☐ WPA2-PSK

WEP Key

1234567890

PSK Pass Phrase

User ID

Password

Encryption Type

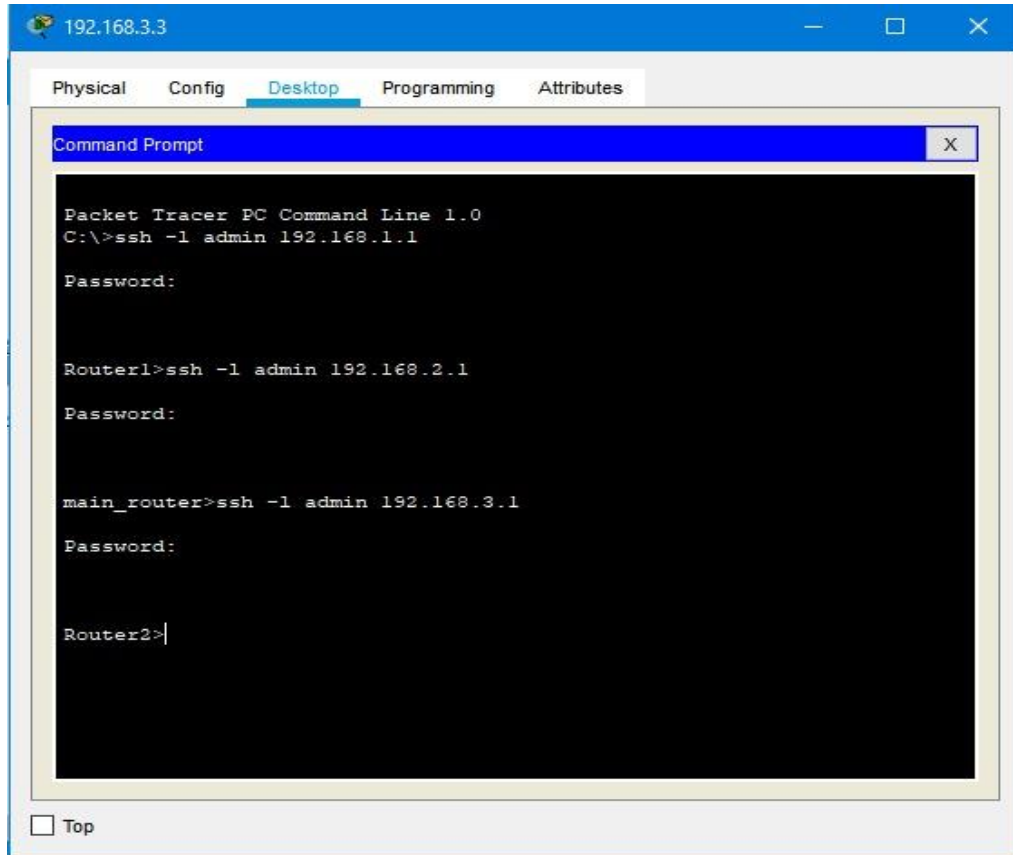
40/64-Bits (10 Hex digits)

5. Securing the network

Passwords are used in accessing the router and all the wireless networks (mentioned in step 5 wireless access point) to make the access limited to University authorized users only.

Routers are also secured with ssh (Secure Shell). Routers and their assigned passwords are mentioned below:

Router Name	Passwords
1)main_router	Console password: cisco ssh password: admin
2)Router1(College Router)	Console password:tiet@123 ssh password: admin
3)Router2(Hostel Router)	Console password:tiet@123 ssh password: admin



The screenshot shows a Packet Tracer PC Command Line window for a PC with IP 192.168.3.3. The window has tabs for Physical, Config, Desktop (selected), Programming, and Attributes. The Command Prompt area shows the following commands and output:

```
Packet Tracer PC Command Line 1.0
C:\>ssh -l admin 192.168.1.1

Password:

Router1>ssh -l admin 192.168.2.1

Password:

main_router>ssh -l admin 192.168.3.1

Password:

Router2>|
```

At the bottom left of the window, there is a checkbox labeled "Top" which is currently unchecked.

WEP Key Needed for Connection

This wireless network has WEP encryption enabled. To connect, you must enter the required passphrase or WEP key in the field below.

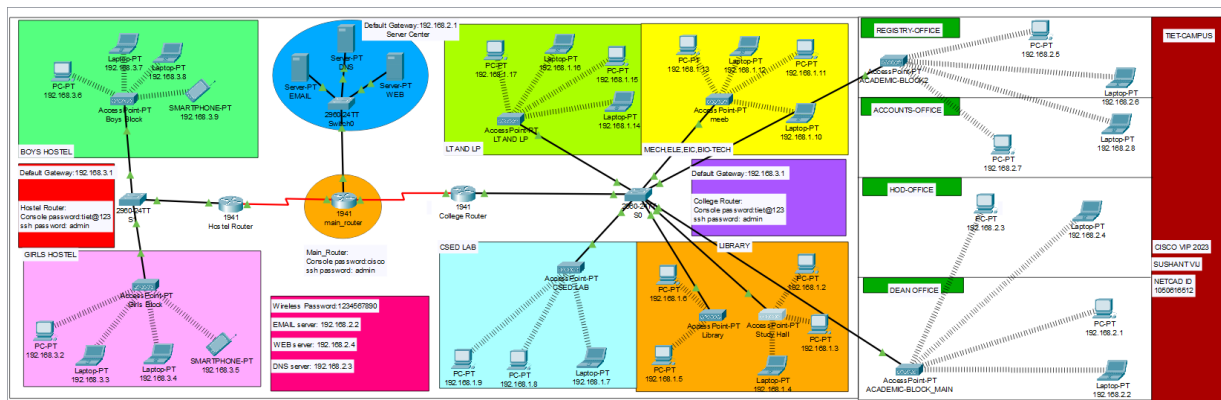
Security	WEP	▼	Please select a security type from the list.
WEP	64-bit	▼	To use WEP encryption, you must enter a valid WEP key.
Passphrase	<input type="text"/>		The Passphrase must be at least 8 characters long.
WEP Key 1	<input type="text" value="1234567890"/>		When entering a WEP key, you must enter a valid hexadecimal key. Valid hexadecimal keys are 10, 26, or 58 characters long.

Connectivity of wireless network on computing devices

CHAPTER 4

ATTACK SURFACE MAPPING AND RESULTS

Finally, we have combined all the steps as mentioned in chapter 3 (work done) and implemented the desired wireless network for University. We have the complete network providing various facilities to the teaching staff, non-teaching staff, and students.



The complete diagram of the University Area Network Scenario created in Packet Tracer environment

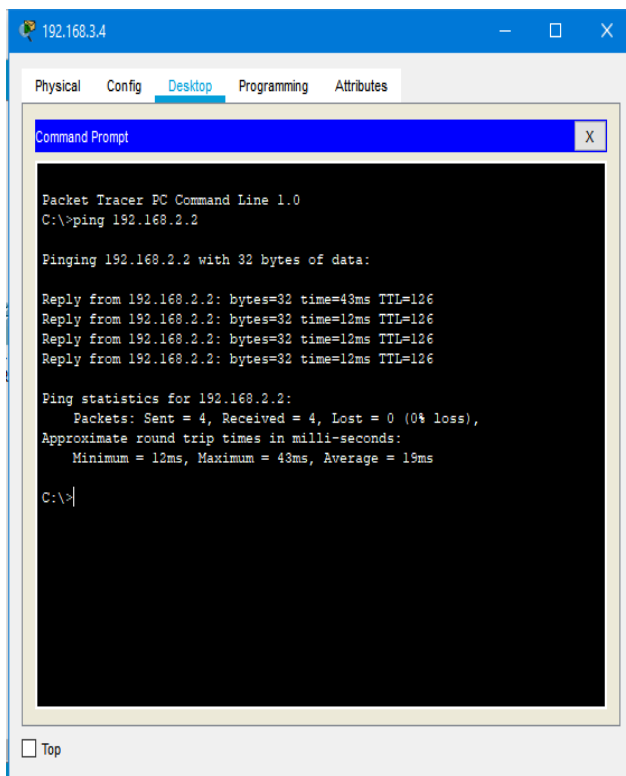
- Final Simulation

In Simulation Mode, you can watch your network run at a slower pace, observing the paths that packets take and inspecting them in detail. The proposed architecture, when simulated on Cisco Packet Tracer, produced results which are demonstrated as follows:



Final simulation for the network system to check all the connections

- Ping Test: Network connectivity and communication can be tested using the ping command, followed by the domain name or the IP address of the device (equipment) whose connectivity one wishes to verify.



```
192.168.3.4
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.2

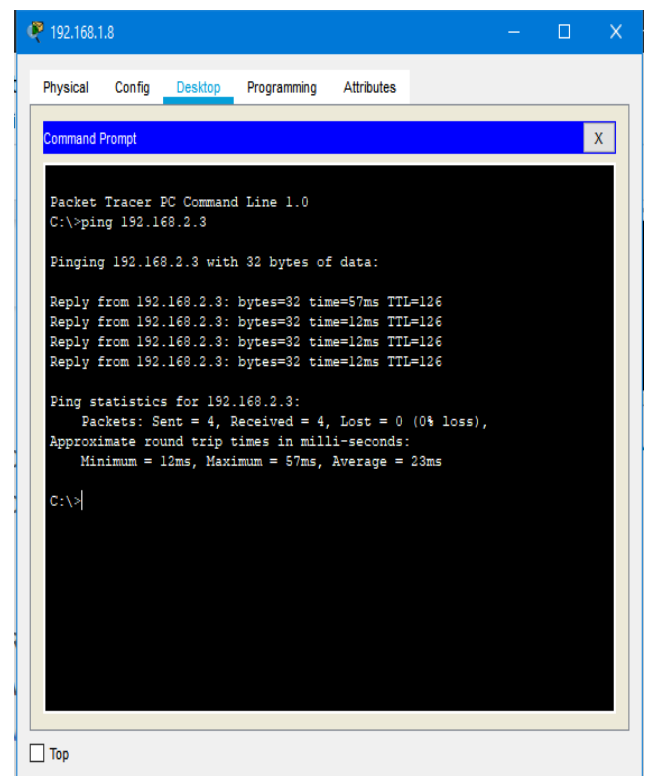
Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time=43ms TTL=126
Reply from 192.168.2.2: bytes=32 time=12ms TTL=126
Reply from 192.168.2.2: bytes=32 time=12ms TTL=126
Reply from 192.168.2.2: bytes=32 time=12ms TTL=126

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 43ms, Average = 19ms

C:\>
```

Ping Test for EMAIL server



```
192.168.1.8
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.3

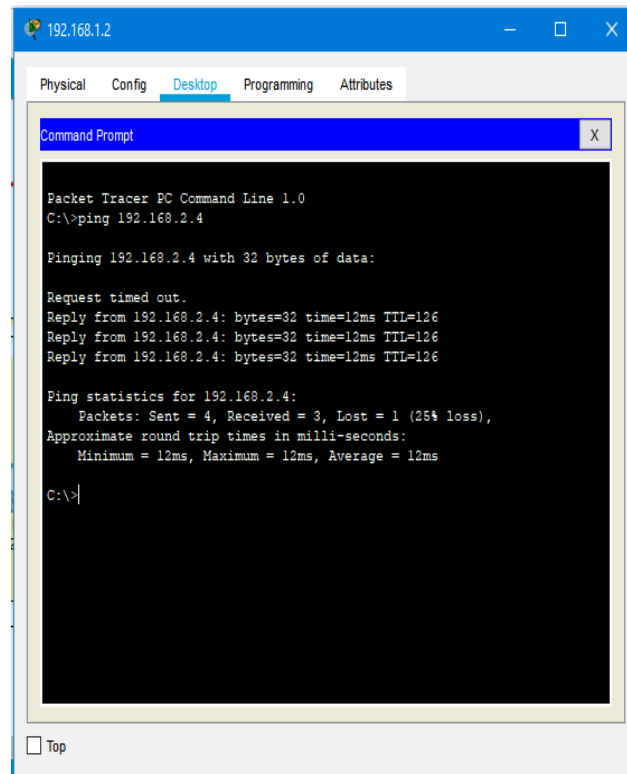
Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.2.3: bytes=32 time=57ms TTL=126
Reply from 192.168.2.3: bytes=32 time=12ms TTL=126
Reply from 192.168.2.3: bytes=32 time=12ms TTL=126
Reply from 192.168.2.3: bytes=32 time=12ms TTL=126

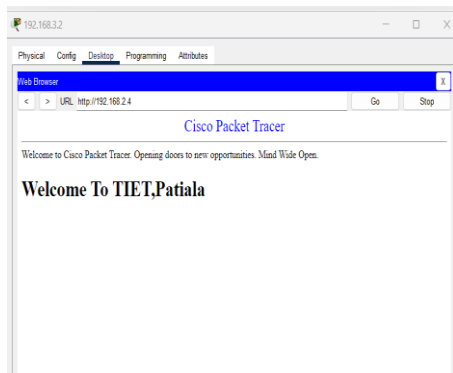
Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 57ms, Average = 23ms

C:\>
```

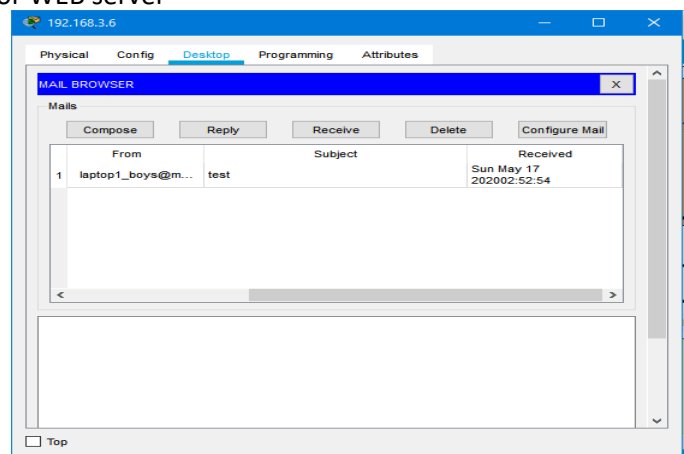
Ping Test for DNS server



Ping Test for WEB server



Website accessed through Web Browser in Packet Tracer



Email received on device sent through EMAIL server

ATTACK SURFACE MAPPING

a) Unauthorized Access:

- Check for Weak Authentication Mechanisms: Review the authentication methods used for network devices, servers, and applications. Look for weak passwords, lack of multi-factor authentication, or outdated authentication protocols.
- Default Credentials: Verify that default credentials are not being used for any network devices or services, as these are commonly known and easily exploitable.
- Open Ports: Identify open ports on routers, switches, servers, and other devices. Ensure that only necessary ports are open, and unnecessary services are disabled.
- Default Settings: Cisco Packet Tracer may sometimes use default credentials for certain simulated devices. Verify if any default credentials are present in the configurations of network devices and services.
- Change Default Credentials: If default credentials are found, change them immediately to strong and unique passwords for improved security. Use the "configure terminal" command to enter global configuration mode and change passwords using "username [username] privilege [level] secret [password]" command.

1)wrong console password

```
User Access Verification
Password:
Password:
Password:
% Bad passwords
```

2)wrong ssh password

```
User Access Verification
Password:

main_router>enable
Password:
Password:
Password:
% Bad secrets
```

3)entering both password

```

main_router>enable
Password:
main_router#show running-config
Building configuration...

Current configuration : 1347 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname main_router
!
!
!
enable password admin
!
!
ip dhcp excluded-address 192.168.2.1 192.168.2.3
!
ip dhcp pool netA
 network 192.168.2.0 255.255.255.0
 default-router 192.168.2.1
ip dhcp pool my_lan

```

b) Data Breaches :

A) Sensitive Data Storage:

- **Identify Data Storage Devices:** Review the network topology and identify devices that may store sensitive data, such as servers or databases. Pay special attention to devices that host applications handling student records, financial data, or research information.

1) No such device to store sensitive data

- **Access Control Review:** Access the configuration of devices containing sensitive data. Review the access control settings, including user permissions, to ensure that only authorized personnel have access to the data.
- **Encryption Check:** Verify if data at rest (stored data) is encrypted. Look for any encryption configurations in the settings of the devices storing sensitive information.

1) encryption is not supported for stored data

- **Audit Logs:** Check if audit logs are enabled to track access to sensitive data. Audit logs can help identify unauthorized access attempts or suspicious activities.

B) Data Transmission:

- **Wired and Wireless Connections:** Identify all wired and wireless connections used to transmit data within the network. Focus on connections used to transfer sensitive data.

Wireless0	
Port Status	<input checked="" type="checkbox"/> On
Bandwidth	24 Mbps
MAC Address	0002.1608.7A8C
SSID	TIET_girls
<div>Authentication</div> <div> <input type="radio"/> Disabled <input checked="" type="radio"/> WEP <input type="radio"/> WPA-PSK <input type="radio"/> WPA2-PSK <input type="radio"/> WPA <input type="radio"/> WPA2 <input type="radio"/> 802.1X Method: </div> <div> WEP Key: 1234567890 PSK Pass Phrase: User ID: Password: MD5 User Name: Password: </div> <div>Encryption Type: 40/64-Bits (10 Hex digits)</div>	
<div>IP Configuration</div> <div> <input type="radio"/> DHCP <input checked="" type="radio"/> Static </div> <div> IPv4 Address: 192.168.3.2 Subnet Mask: 255.255.255.0 </div>	
<div>IPv6 Configuration</div> <div> <input checked="" type="radio"/> Automatic <input type="radio"/> Static </div> <div> IPv6 Address: / Link Local Address: FE80::202:16FF:FE08:7A8C </div>	

- Encryption Review: For wireless connections, ensure that WPA2 or higher encryption protocols are used. Check for any unencrypted data transmission within the network.

1) Lower encryption protocols and WEP used

Authentication		
<input type="radio"/> Disabled	<input checked="" type="radio"/> WEP	WEP Key: 1234567890
<input type="radio"/> WPA-PSK	<input type="radio"/> WPA2-PSK	PSK Pass Phrase:
<input type="radio"/> WPA	<input type="radio"/> WPA2	User ID:
<input type="radio"/> 802.1X	Method:	Password:
		MD5
		User Name:
		Password:
Encryption Type		40/64-Bits (10 Hex digits)

- VPN Configuration: If virtual private networks (VPNs) are used for secure remote access, verify that proper encryption is employed for data transmission over the VPN.

1) no VPN used

- Network Segmentation: Assess network segmentation to separate sensitive data traffic from regular network traffic. Use VLANs or other techniques to isolate sensitive data transmissions.

1)only VLAN 10 used over the campus network which is not suitable

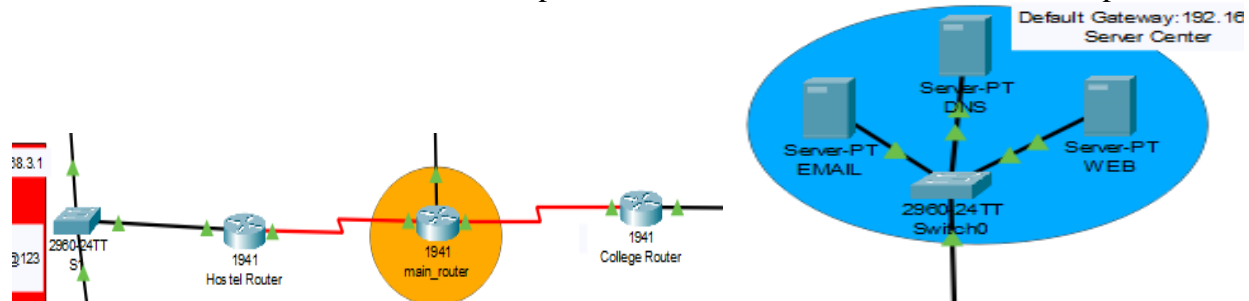
- Firewall Rules: Review firewall rules to control traffic flow between different network segments, ensuring that sensitive data transmissions are adequately protected.

1)Firewalls are highly required

c) Network Availability:

Redundancy:

a) Identify Critical Components: Review the network topology and identify critical components such as routers, switches, servers, and important links that are essential for network operation.



1)you can visually identify critical components by inspecting the network topology.

b) Assess Redundant Power Supplies: Check if critical devices have redundant power supplies configured. This ensures that in case of a power supply failure, the device can continue to function without interruption.

1) power supply redundancy may not be explicitly configurable. The simulation assumes that devices have built-in redundant power supplies.

c) Verify Redundant Links: For critical links, such as uplinks between switches or connections to important servers, ensure that redundancy is in place. This can be achieved using technologies like Spanning Tree Protocol (STP) or link aggregation (EtherChannel).

d) Network Device Resiliency: Verify if devices support features like hot-swapping or fast recovery, which can reduce downtime during hardware failures.

1)it is simulated by default.

Bandwidth and Load Balancing:

a) Analyze Network Traffic: Use tools like Packet Tracer's traffic simulation or monitoring features to analyze network traffic and identify potential bottlenecks.

b) Load Balancing Mechanisms: Check if load balancing mechanisms are implemented for critical links to evenly distribute traffic and avoid congestion. Technologies like Port Channel or Equal-Cost Multipath (ECMP) can be used for load balancing.

c) QoS Implementation: Review Quality of Service (QoS) configurations to prioritize critical traffic and ensure that important applications receive the necessary bandwidth and low latency.

d) Performance Monitoring: Configure performance monitoring on network devices to continuously monitor traffic patterns and detect potential issues before they cause disruptions.

d) Vulnerable Services:

Software Updates:

- **Access Device Configurations:** Access the configuration of routers, switches, servers, and other network devices in Packet Tracer by entering privileged EXEC mode. Use the "enable" command to access this mode and enter the appropriate password if required.
- **Check for Outdated Software:** Review the running configuration of devices and check for outdated firmware or software versions. This includes the operating system of network devices and any applications running on servers.
- **Update Firmware and Software:** If any devices or applications are running outdated versions, apply the latest security patches and updates. Cisco Packet Tracer may not have real-time updates, but you can simulate the process of updating software configurations manually.

Network Services:

- **Show Running Configuration:** Use the "show running-config" command to display the running configuration of routers and switches. Look for enabled services that might present security risks, such as Telnet or SNMP.
- **Disable Unnecessary Services:** In the configuration mode, use the "no [service]" command to disable any unnecessary services that are not required for network operation. For example, you can disable Telnet and enable Secure Shell (SSH) for remote access.

Application Security:

- **Review Web Applications:** If there are web applications running on servers in the simulation, assess their security measures. Look for input validation mechanisms and other secure coding practices to prevent common web application vulnerabilities like SQL injection and cross-site scripting (XSS).
- **Check Web Application Configuration:** Examine the web server's configuration and ensure that security headers, such as HTTP Strict Transport Security (HSTS) and Content Security Policy (CSP), are properly set to enhance web application security.

CHAPTER 5

CONCLUSION AND FUTURE WORK

- Conclusion

We started our discussion with the word “digitalization” and in order to achieve it, we aimed to start with an educational institute, and finally, we designed a network for a University, which is wireless. As we mentioned, mobility and efficiency are the key aspects of wireless networks, which were our main goal, and hence, we decided to shift to a wireless network instead of a wired one, making our network clean and less chaotic.

In this project, we designed a University Network using Cisco Packet Tracer that uses a networking topology implemented using servers, routers, switches, and end devices in a multiple area networks. We have covered all the necessary features that are required for a network to function properly. We have included a DNS server and a web server for establishing a smooth communication system between different areas of our network and specifically for the communication between students and teachers. We have included an email server to facilitate intra university communication through emails within the domain. We have used console passwords and ssh protocol to ensure a safe and secure transfer of data.

- Future Work

The configuration and specifications are for the initial prototype and can further be developed and additional functionality can be added to increase support and coverage of our existing network.

REFERENCES

- [1]https://en.wikipedia.org/wiki/Packet_Tracer
- [2]<https://www.paessler.com/it-explained/server>
- [3]<https://computernetworking747640215.wordpress.com/2018/07/05/secure-shell-ssh-configuration-on-a-switch-and-router-in-packet-tracer/>
- [4]<http://router.over-blog.com/article-how-to-configure-cisco-router-password-106850439.html>
- [5]<https://www.cognoscape.com/benefits-going-wireless/>