**FINAL YEAR PROJECT**

**(2019-23)**

**Campus Area Network**

**FINAL REPORT**

**Government College University Faisalabad**

# Submitted by-

***Muhammad Usama (191828)***

**Supervised By: - Mr. Salman**

**Department of Computer Science**

# 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 (2911)
2. Switches (2960-24TT)
3. Email server
4. DNS server
5. WEB server (HTTP)
6. NTP Server 4
7. AAA Server 5
8. FTP Server 2
9. DHCP Server0
10. Wireless Device (Wireless Router)
11. PCs
12. Laptops
13. Smartphones

The design includes the following parts of the University:

• **Hostel Blocks**: Girls Block and Boys Block

## • Academic Blocks: AB1 and AB2

## • Department Building

• **IT Consulting**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Table Of Content\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

|  |  |  |
| --- | --- | --- |
| 1. | Cover Page | 1 |
| 3. | Abstract | 2 |
| 4. | Table of Content | 4 |
| 5. | Chapter 1: Introduction | 5 |
| 6. | Chapter 2: Literature Review | 7 |
| 7. | Chapter 3: Work Done | 25 |
| 8. | Chapter 4: Results and Discussion | 43 |
| 9. | Chapter 5: Conclusions and Future Work | 52 |
| 10. | References | 53 |

**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.

Campus networking via wireless or wire 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. 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.

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

In this project, we defined a simulation of campus networks based on wireless and wired networking. The network is divided into two sets: one for the campus area and the other for the hostel area.

The major aim of this project is to show the wireless and wired connectivity that is used in universities to make the network efficient and mobile at the same time. Mobility is the major concentration of this project. In order to provide equal functionality to all the users (college staff and students), we have added DNS,DHCP,FTP, Email,NTP, and AAA servers for the maximum utilization of resources.

Hence the campus network provides different services such as connecting the user to the internet, data sharing among users (students, teachers, and different university members), accessing different web services for different functionalities, so it needs wireless networking for smooth processing.

**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.



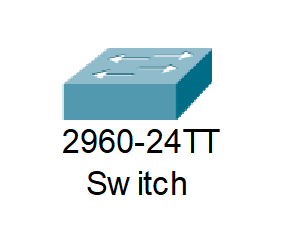
## ● Router

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

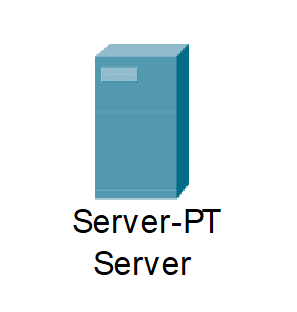
A network packet is a formatted unit of data carried by a packet-switched network. A packet consists of control information and user data, which is also known as the payload.

## ● 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.

## ● Server

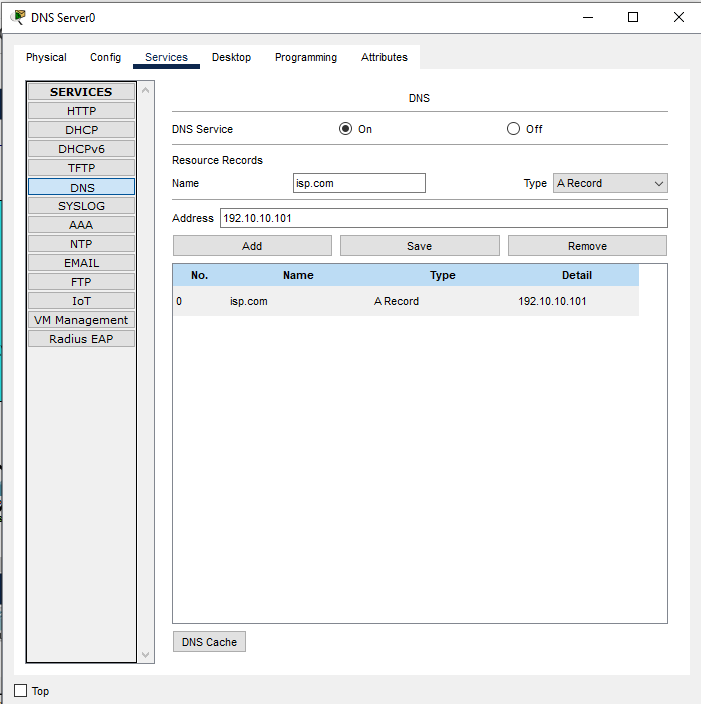
A server is a computer or system that provides resources, data, services, or programs to other computers, known as clients, over a network. In theory, whenever computers share resources with client machines they are considered servers. There are many types of servers, including web servers, mail servers,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



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

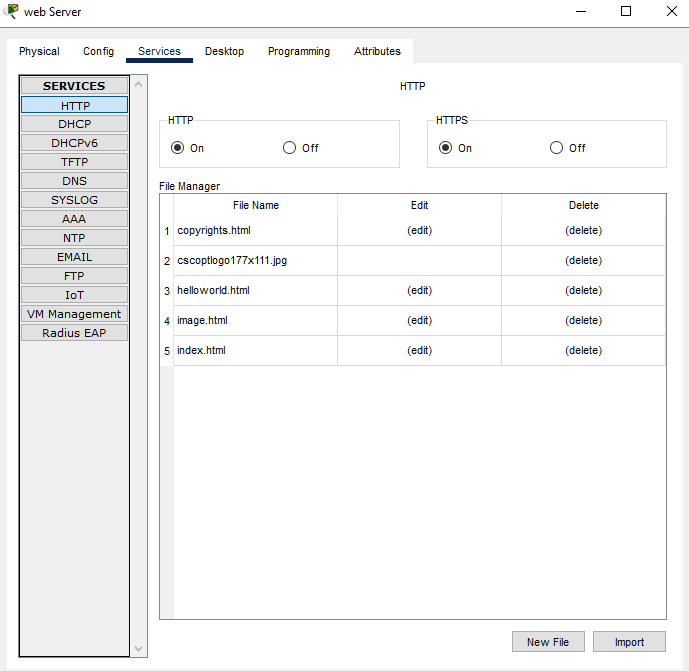
➢ DNS Server

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.



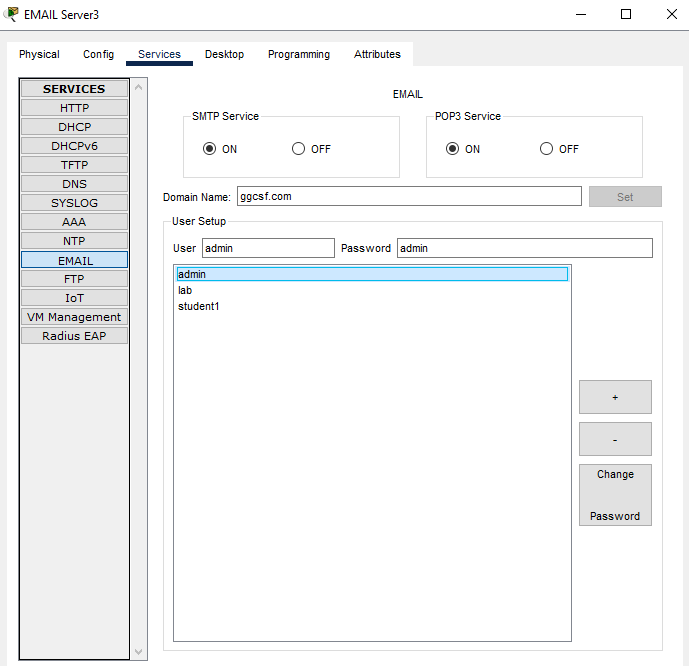
## ➢ WEB Server

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.



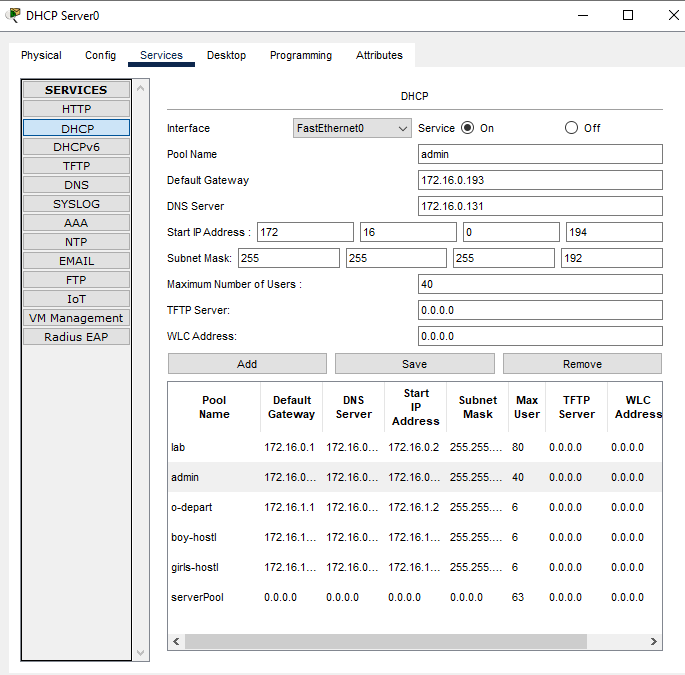
## ➢ EMAIL Server

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.



## ➢ DHCP Server

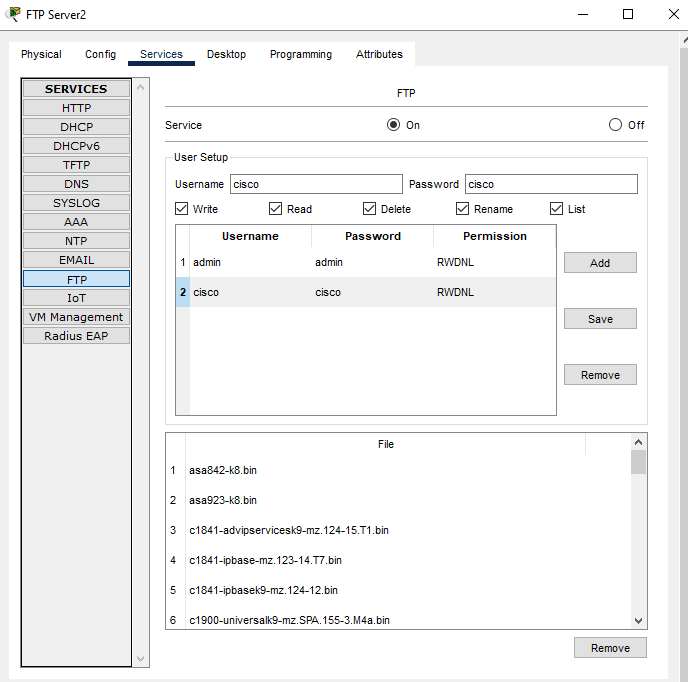
For service providers, a DHCP server is a mission-critical application that determines the continuity of their services. What service providers need is therefore a server that’s resilient, scalable, capable of handling complex configurations, and easy to integrate with other systems. IP overlapping addresses support, full IPAM, flexible runtime configuration, 24/7 support. All the features of a carrier-grade IPv4/IPv6 dual stack mission critical **DHCP server**.



## ➢ FTP Server

The primary purpose of an FTP server is to allow users to upload and download files.An FTP server is a computer that has a file transfer protocol (FTP) address and is dedicated to receiving an FTP connection. FTP is a protocol used to transfer files via the internet between a server (sender) and a client (receiver)**.**An FTP server is a computer that offers files available for download via an FTP protocol, and it is a common solution used to facilitate remote data sharing between computers.

An FTP server is an important component in FTP architecture and helps in exchanging files over the internet. The files are generally uploaded to the server from a personal computer or other removable hard drives (such as a USB flash drive) and then sent from the server to a remote client via the FTP protocol. An FTP server needs a TCP/IP network to function and is dependent on the use of dedicated servers with one or more FTP clients. In order to ensure that connections can be established at all times from the clients, an FTP server is usually switched on; up and running 24/7.



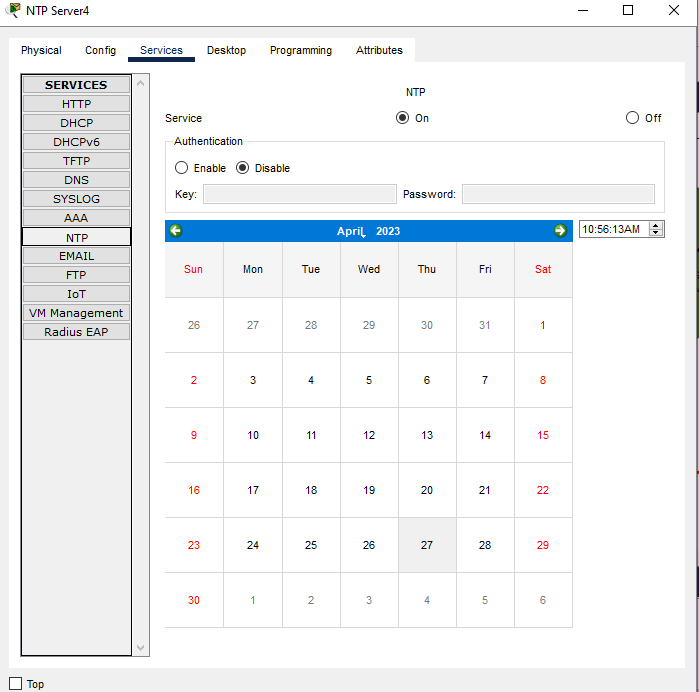
## ➢ NTP Server

Using the Network Time Protocol (NTP) is a simple and effective way to set your local time. But how can you ensure that the time you are getting is correct, what can you do to improve time accuracy, and how do you decide which NTP servers are best for you?

**How Many NTP Server Should I Use?**

There is an old saying that goes: "A man with one watch knows what time it is. A man with two watches is never sure”. If you have only one clock, that is the only one you can trust. If you have two and they start to show different times, it is difficult to know which one has gone wrong. To guarantee accuracy, you need at least three clocks. If two of them show the same time, you can be relatively sure when the third clock has gone wrong. The more clocks you have showing the same time, the more sure you can be that they are right and that any clock showing a different time is incorrect.

The same principle holds true for getting time over the Network Time Protocol (NTP). If your client allows it, you should connect to multiple NTP servers. In the case that your client only allows you to specify a single NTP server, use: ntp.netnod.se (or nts.netnod.se if your client supports network time security.



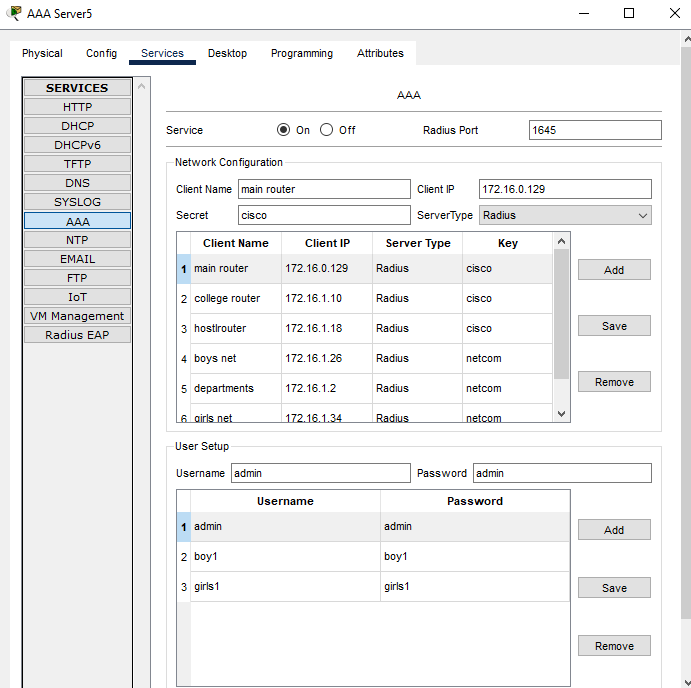
## ➢ AAA Radious Server

An AAA server is a server program that handles user requests for access to computer resources and, for an enterprise, provides authentication, authorization, and accounting (AAA) services.

**Authentication** is the process of identifying an individual, usually based on a username and password. Authentication is based on the idea that each individual user will have unique information that sets him or her apart from other users.

**Authorization** is the process of granting or denying a user access to network resources once the user has been authenticated through the username and password. The amount of information and the amount of services the user has access to depend on the user's authorization level.

**Accounting** is the process of keeping track of a user's activity while accessing the network resources, including the amount of time spent in the network, the services accessed while there and the amount of data transferred during the session. Accounting data is used for trend analysis, capacity planning, billing, auditing and cost allocation.



## ● 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.   
Ethernet is the traditional technology for connecting devices in a wired local area network (LAN) or wide area network (WAN). It enables devices to communicate with each other via a protocol, which is a set of rules or common network language.

Ethernet describes how network devices format and transmit data so other devices on the same LAN or campus network can recognize, receive and process the information. An Ethernet cable is the physical, encased wiring over which the data travels.

Connected devices that use cables to access a geographically localized network -- instead of a wireless connection -- likely use Ethernet. From businesses to gamers, diverse end users rely on the benefits of Ethernet connectivity, which include reliability and security.

Compared to wireless LAN (WLAN) technology, Ethernet is typically less vulnerable to disruptions. It can also offer a greater degree of network security and control than wireless technology because devices must connect using physical cabling. This makes it difficult for outsiders to access network data or hijack bandwidth for unsanctioned devices.

## ● 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. The Internet Protocol (IP) is a protocol, or set of rules, for routing and addressing packets of data so that they can travel across networks and arrive at the correct destination. Data traversing the Internet is divided into smaller pieces, called packets. IP information is attached to each packet, and this information helps routers to send packets to the right place. Every device or domain that connects to the Internet is assigned an IP address, and as packets are directed to the IP address attached to them, data arrives where it is needed.

Once the packets arrive at their destination, they are handled differently depending on which transport protocol is used in combination with IP. The most common transport protocols are TCP and UDP.

## ● 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) isencrypted and secure from eavesdropping.

SSH is aclient-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.

## Typical uses of the SSH protocol

The protocol is used in corporate networks for:

* providing secure access for users and automated processes
* interactive and automated file transfers
* issuing remote commands
* managing network infrastructure and other mission-critical system components.

**Access Control List ( ACL )**

A network access control list (ACL) is made up of rules that either allow access to a computer environment or deny it. In a way, an ACL is like a guest list at an exclusive club. Only those on the list are allowed in the doors. This enables administrators to ensure that, unless the proper credentials are presented by the device, it cannot gain access.

**Types of ACL:**

# Standard Access-List

Access-list (ACL) is a set of rules defined for controlling network traffic and reducing network attacks. ACLs are used to filter traffic based on the set of rules defined for the incoming or outgoing of the network.

* **Extended ACL**

To be more precise when matching a certain network traffic, extended access lists are used. Extended access lists are more difficult to configure and require more processor time than the standard access lists, but they enable a much more granular level of control.

# Configuring named ACLs

Just like the numbered ACLs we’ve used so far, named ACLs allow you to filter network traffic according to various criteria.

**NAT:**

NAT stands for network address translation. It’s a way to map multiple private addresses inside a local network to a public IP address before transferring the information onto the internet. Organizations that want multiple devices to employ a single IP address use NAT, as do most home routers. If you’re connecting from your home right now, chances are your cable modem or DSL router is already providing NAT to your home.

PAT:

Port Address Translation (PAT), is an extension to network address translation (NAT) that permits multiple devices on a local area network (LAN) to be mapped to a single public ip address. The goal of PAT is to conserve IP addresses. Most home networks use PAT. In such a scenario, the Internet Service Provider (ISP)assigns a single IP address to the home network's router. When Computer X logs on the Internet, the router assigns the client port number, which is appended to the internal IP address. This, in effect, gives Computer X a unique address. If Computer Z logs on the Internet at the same time, the router assigns it the same local IP address with a different port number. Although both computers are sharing the same public IP address and accessing the Internet at the same time, the router knows exactly which computer to send specific packets to because each computer has a unique internal address.

VLAN:

A virtual local area network (VLAN) is a virtualized connection that connects multiple devices and network nodes from different LANs into one logical network.Virtual local area networks have become crucial for organizations with complex networking systems. Organizations require solutions that allow them to scale their networks, segment them to increase security measures, and decrease network latency. While LAN is used to connect a group of devices such as computers and printers to a server via cables, VLANs allow multiple LANs and associated devices to communicate via wireless internet.

**Data Encapsulation :**  
Encapsulation is the process of adding additional information when data is traveling in OSI or TCP/IP model. The additional information has been added on sender’s side, starting from Application layer to Physical layer.

**Routing:**

Routing is the process of path selection in any network. A computer network is made of many machines, called nodes, and paths or links that connect those nodes. Communication between two nodes in an interconnected network can take place through many different paths.

**Static Routing:**

Static routing performs routing decisions with preconfigured routes in the routing table, which can be changed manually only by administrators. Static routes are normally implemented in those situations where the choices in route selection are limited, or there is only a single default route available. Also, static routing can be used if you have only few devices for route configuration and there is no need for route change in the future.

**Port Securty:**

Port security is the process of restricting access to a network by limiting which devices can connect to the network, and how they can connect. Only specific devices or MAC addresses can access it. It is a way of controlling which devices can access the network.

**Ip Address:**

An IP address is a unique address that identifies a device on the internet or a local network. IP stands for "Internet Protocol," which is the set of rules governing the format of data sent via the internet or local network.

**Mac Address:**

A MAC (Media Access Control) address, sometimes referred to as a hardware or physical address, is a unique, 12-character alphanumeric attribute that is used to identify individual electronic devices on a network. An example of a MAC address is: 00-B0-D0-63-C2-26.

## ● 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. Network Requirements

The network is divided into 2 areas :

## 1. Campus Area

The Campus area is further divided into various accessing points like Dome building, Academic Blocks (AB1 and AB2), Server Center, and IT consulting.

## 2. Hostel Area

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

### 3. Layout

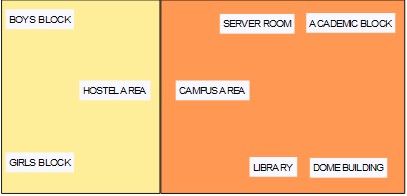


Figure – Basic Layout of our wireless access points in University

Devices Used In The Network

|  |  |
| --- | --- |
| Devices | Quantity |
| 1) Router (1941) | 3 |
| 2) Switches (2960-24TT) | 4 |
| 3) EMAIL server | 1 |
| 4) DNS server | 1 |
| 5) DHCP server | 1 |
| 6) AAA server | 1 |
| 7) WEB server (HTTP) | 1 |
| 8) NTP server | 1 |
| 9) Wireless Router | 3 |
| 10) PCs | 17 |
| 11) Laptops | 6 |
| 12) Smartphones | 5 |

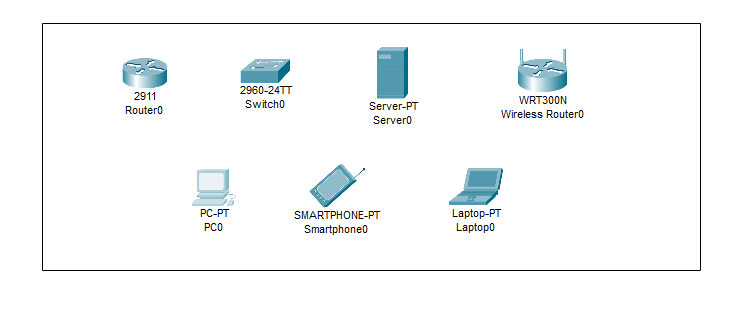
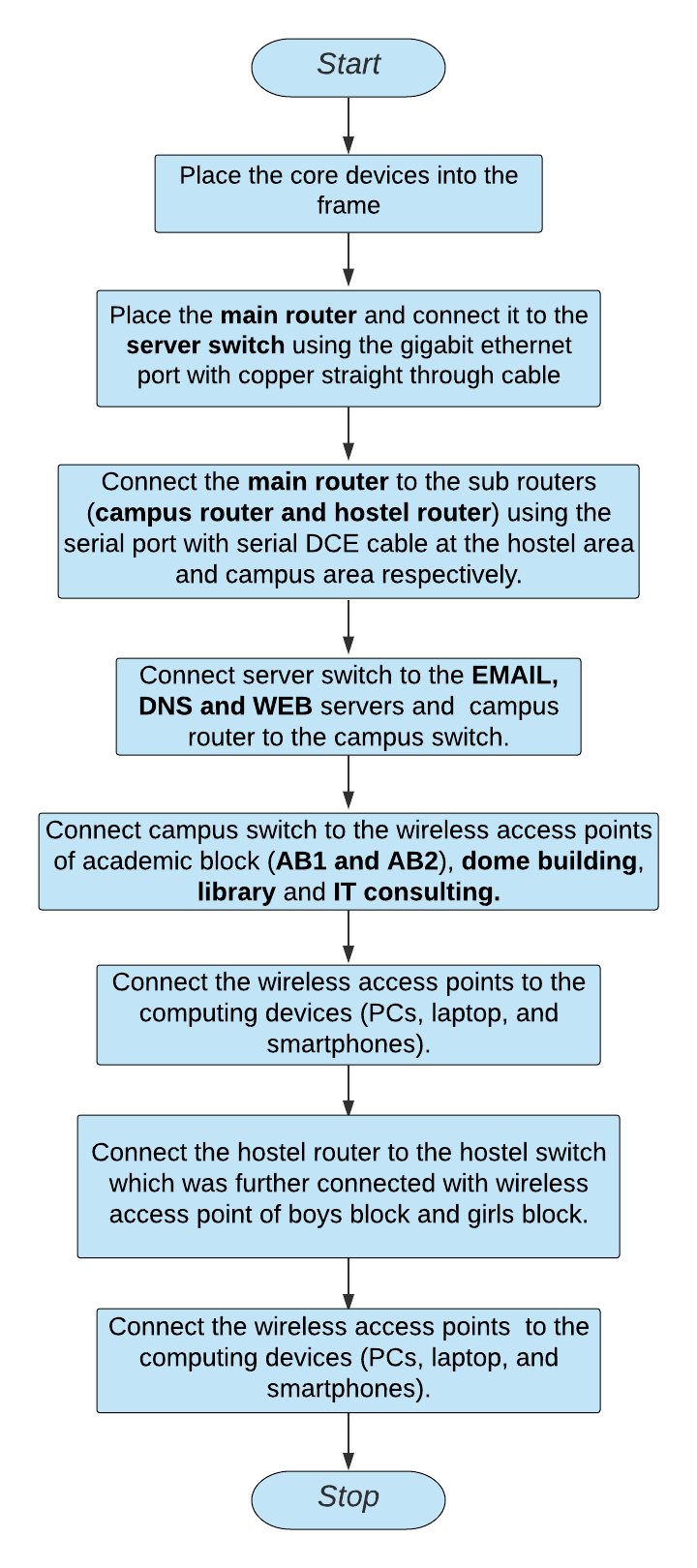


Figure 3: Devices used in the network

### 4. Implementation and Flow Diagram

* To design the network of the college/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,DHCP,NTP, FTP and AAA (RADIOUS)** servers respectively.
* Campus router was connected to the campus switch which was further connected with campus router of the academic block switch (**AB1 and AB2**), **dome building wireless router**, and **IT consulting.**
* The wireless router 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 router of boys block and girls block.
* The wireless router 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 user id and password.
* All these connections are made through ethernet ports (gigabit ethernet and fast ethernet) using copper straight-through cables.

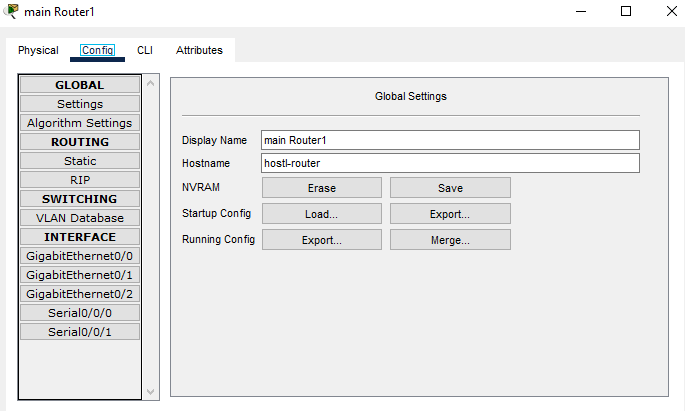


This is the flow diagram for a better understanding of the steps mentioned above.

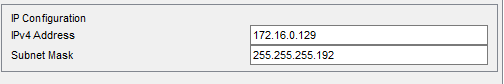
### 5. Configuring IP Addresses

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

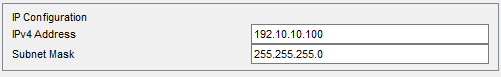
* Main Router configuration



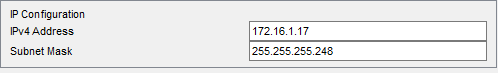
GigabitEthernet0/0



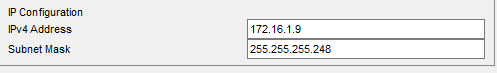
GigabitEthernet0/1



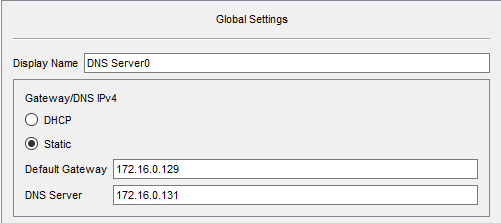
Serial0/0/0

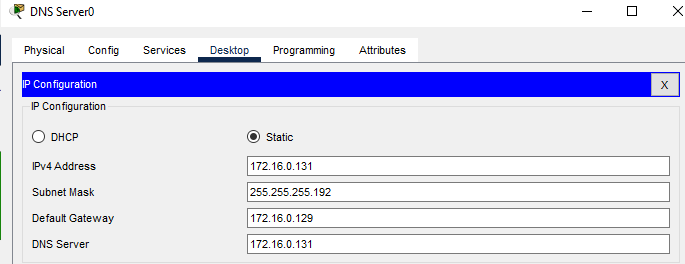


Serial0/0/1

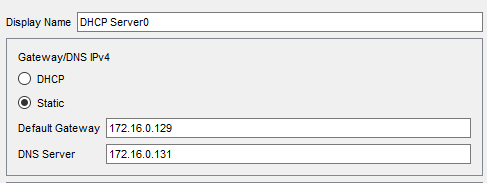


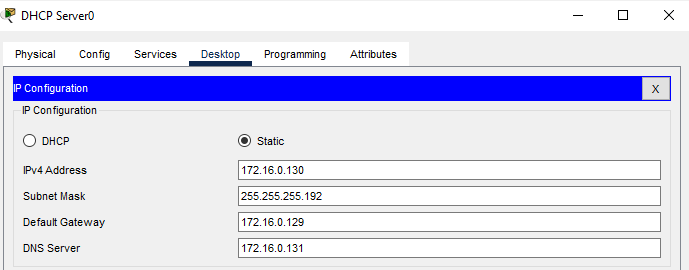
* **DNS SERVER**



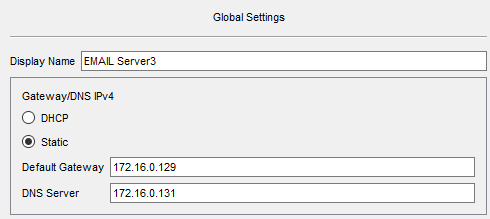


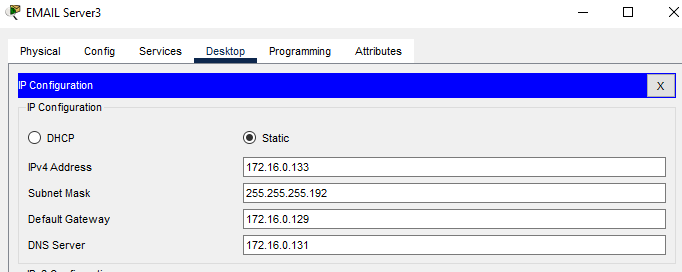
* **DHCP SERVER**



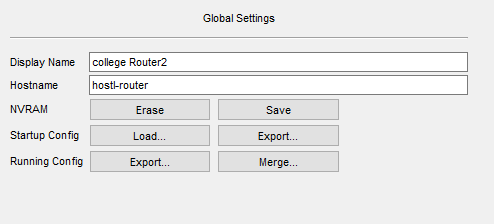


* **EMAIL SERVER**

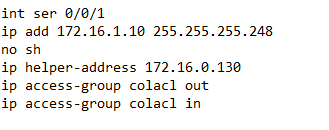




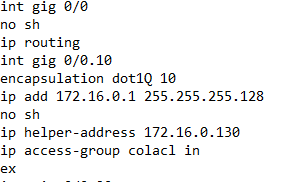
* **COLLEGE ROUTER**

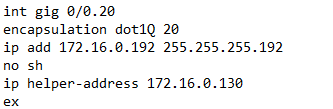


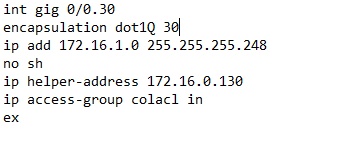
Serial 0/0/1



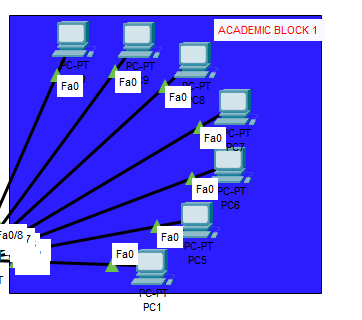
Gigabitethernet







### ● ACADEMIC BLOCK 1



IP Address are as follows

172.16.0.0 /25

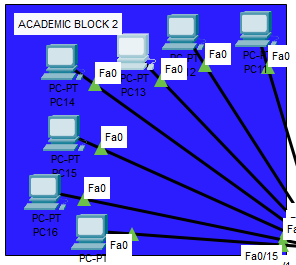
Subnet Mask- 255.255.255.128

Default Gateway- 172.16.0.1

DNS Server- 172.16.0.131

Vlan-10

### ● ACADEMIC BLOCK 2



IP Address are as follows

172.16.0.0 /25

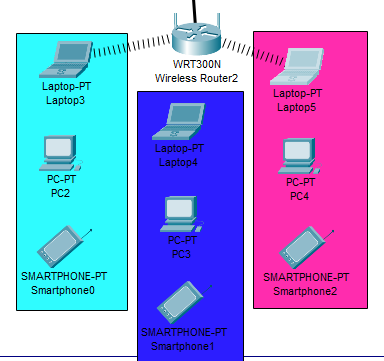
Subnet Mask- 255.255.255.128

Default Gateway- 172.16.0.1

DNS Server- 172.16.0.131

Vlan-10

### ● DOME BUILDING



IP Address are as follows

172.16.1.0 /29

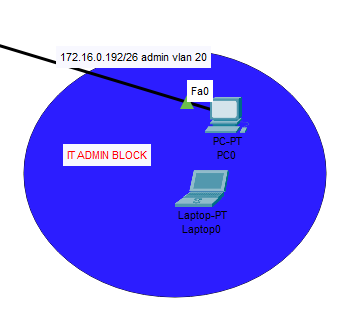
Subnet Mask- 255.255.255.248

Default Gateway- 172.16.1.1

DNS Server- 172.16.0131

Vlan-30

### ● IT ADMIN BOLCK



IP Address are as follows

172.16.0.192 /26

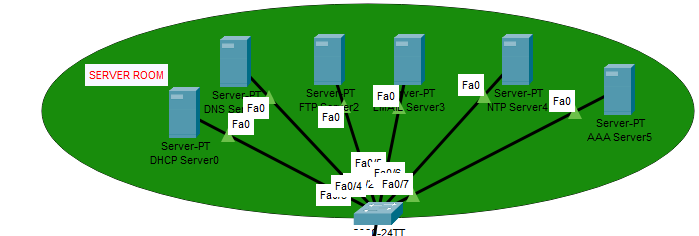
Subnet Mask- 255.255.255.192

Default Gateway- 172.16.0.192

DNS Server- 172.16.0131

Vlan-20

### ● SERVER ROOM



IP Address are as follows

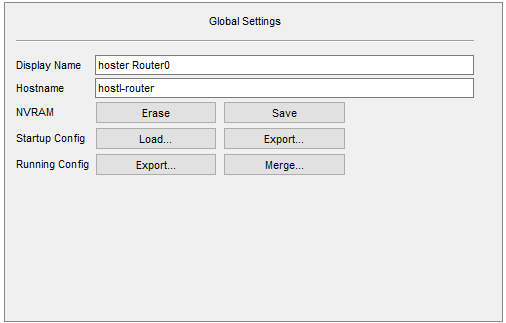
172.16.0.128 /26

Subnet Mask- 255.255.255.130

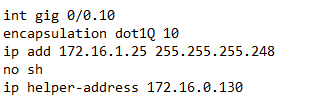
Default Gateway- 172.16.0.129

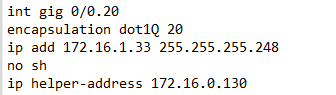
DNS Server- 172.16.0131

### ● HOSTEL ROUTER

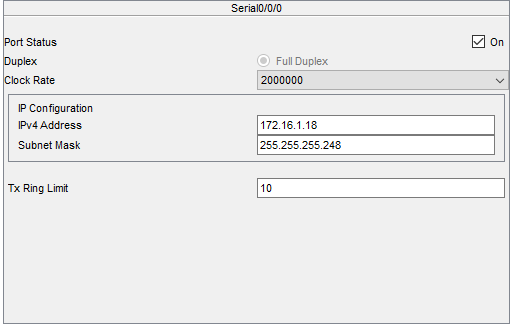


GigabitEthernet0/0

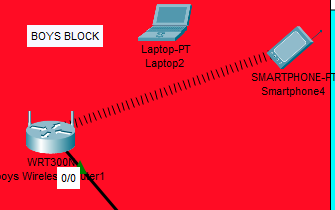




Serial 0/0/0



### ● Boys Block



IP Address are as follows

172.16.1.24/29

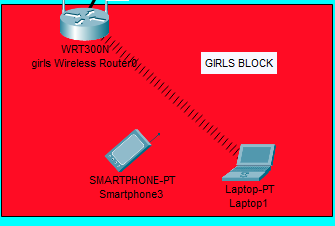
Subnet Mask- 255.255.255.248

Default Gateway- 172.16.1.25

DNS Server- 172.16.0.131

Vlan-10

### ● Girls Block



IP Address are as follows

172.16.1.32/29

Subnet Mask- 255.255.255.248

Default Gateway- 172.16.1.33

DNS Server- 172.16.0.131

Vlan-20

### ● WIRELESS ACCESS POINT

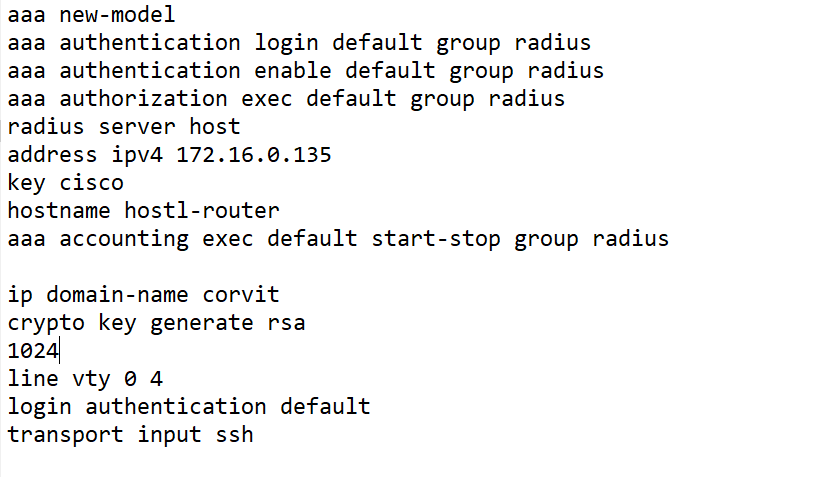
|  |  |  |
| --- | --- | --- |
| SSID | User ID | Password |
| 1) boys net | boy1 | boy1 |
| 2) girls net | girls1 | girls1 |
| 3) departments | dep1 | dep1 |
| 3) departments | dep2 | dep2 |

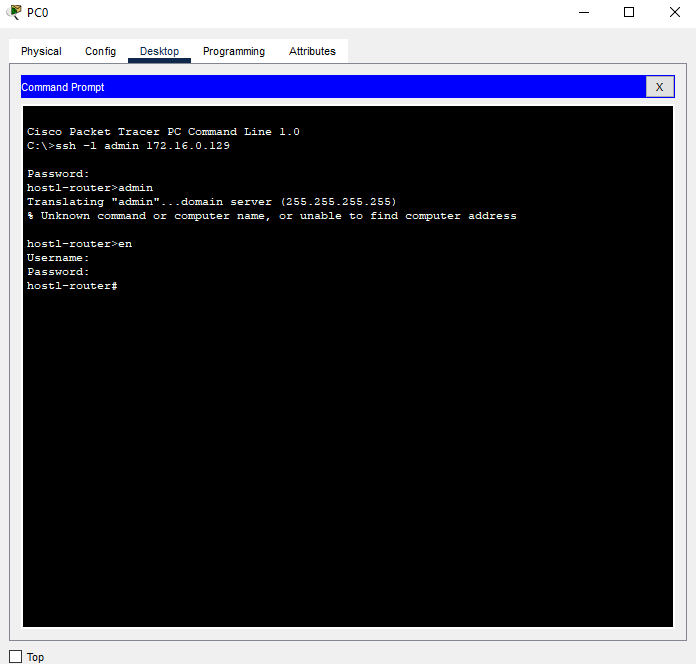
## 6. Securing the network

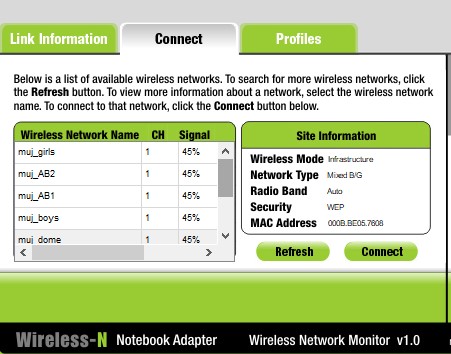
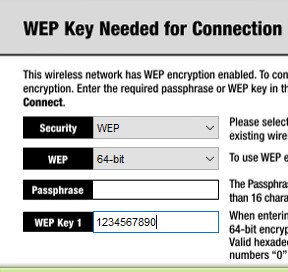
User Id and Passwords are used in accessing the router and all the wireless networks to make the access limited to University authorized users only.

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

|  |  |  |
| --- | --- | --- |
| Router Name | IP ADDRESS | User Id and Passwords |
| 1)main\_router | 172.16.0.129 | USER ID: admin password: admin |
| 2)Router2(College Router) | 172.16.1.10 | USER ID: admin password: admin |
| 3)Router0(Hostel Router) | 172.16.1.18 | USER ID: admin password: admin |





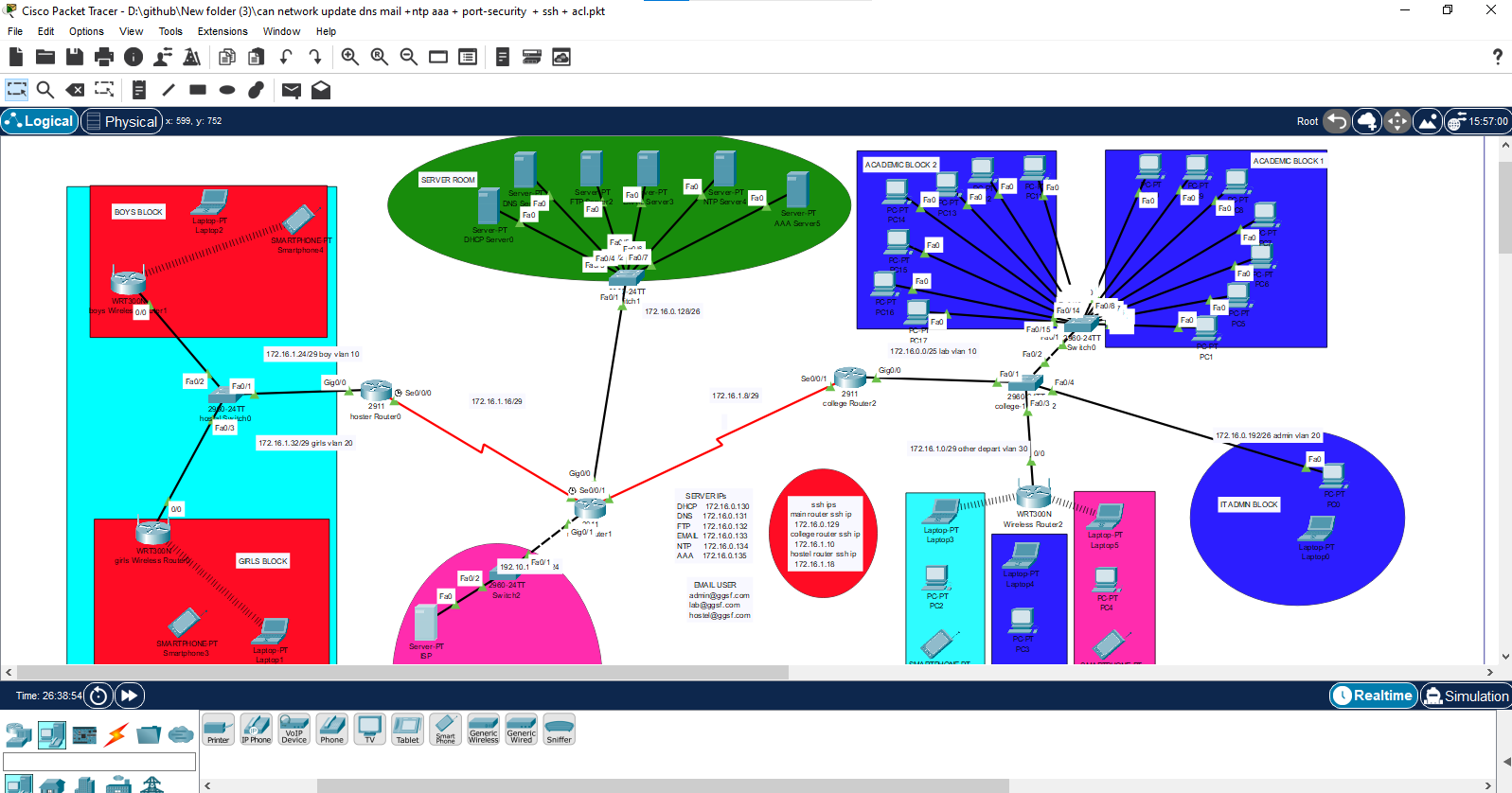


**Connectivity of wireless network on computing devices**

**CHAPTER 4**

# RESULT & DISCUSSION

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.

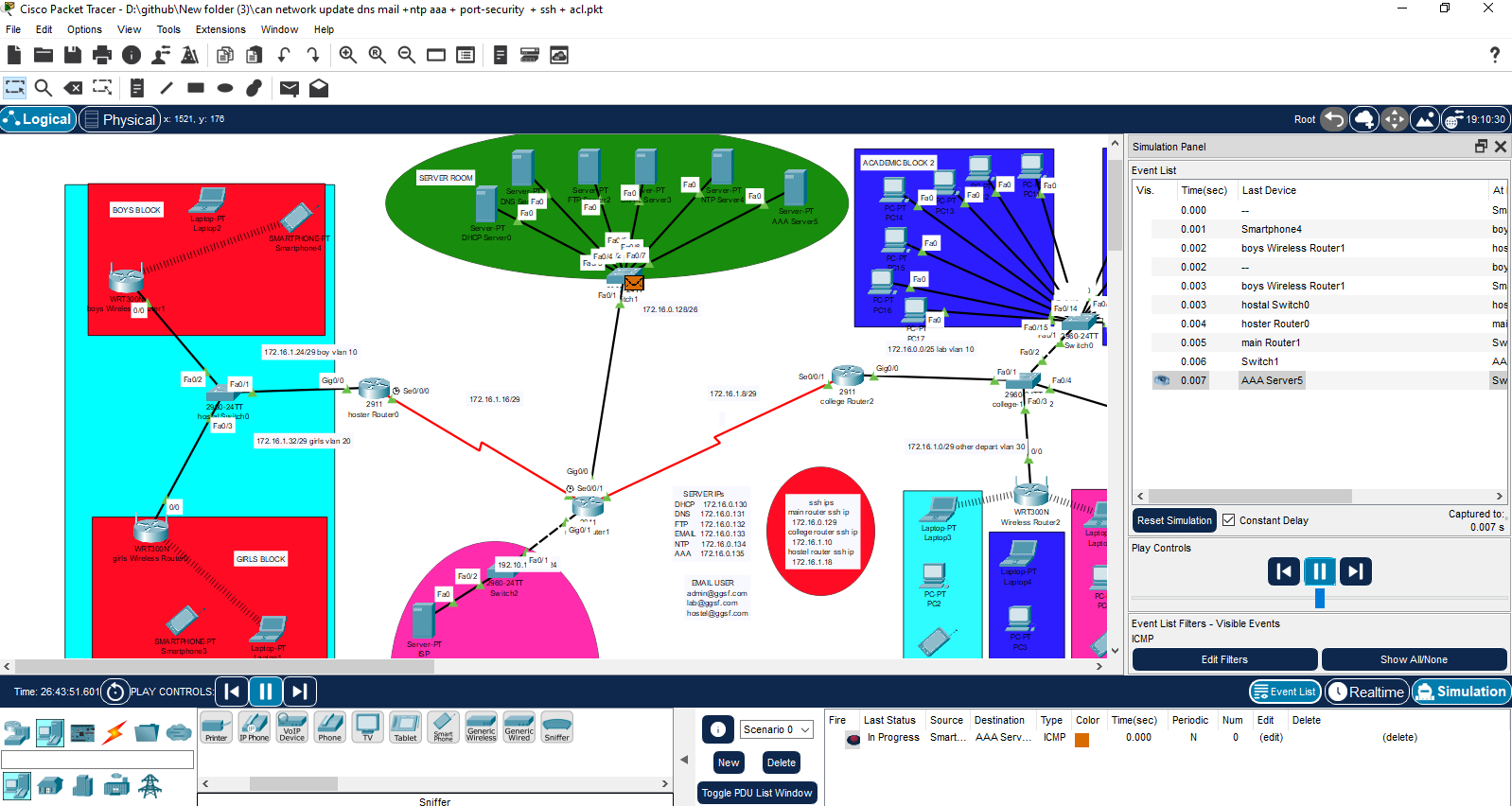


The complete diagram of the University Area Network Scenario created in Packet

Tracer environment

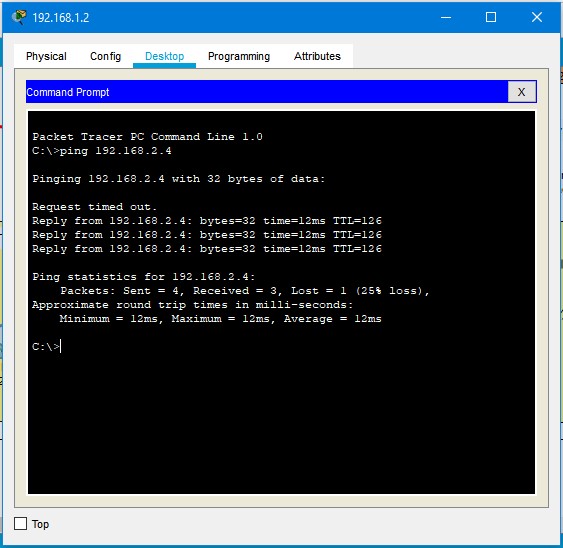
## ● Final Simulation

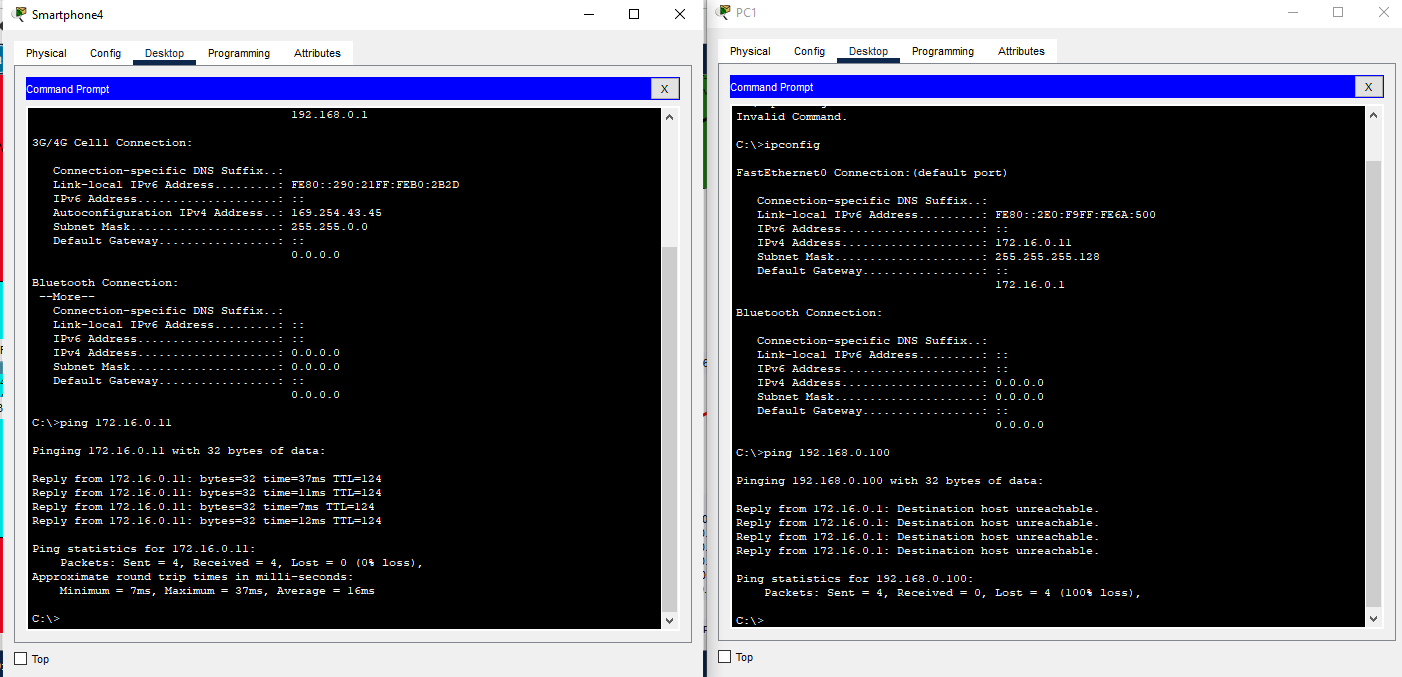
In Simulation Mode, you can watch your network run at a slower pace, observing the paths that packets take and inspecting them in detail. The proposed architecture, when simulated on Cisco Packet Tracer, produced results which are demonstrated as follows:

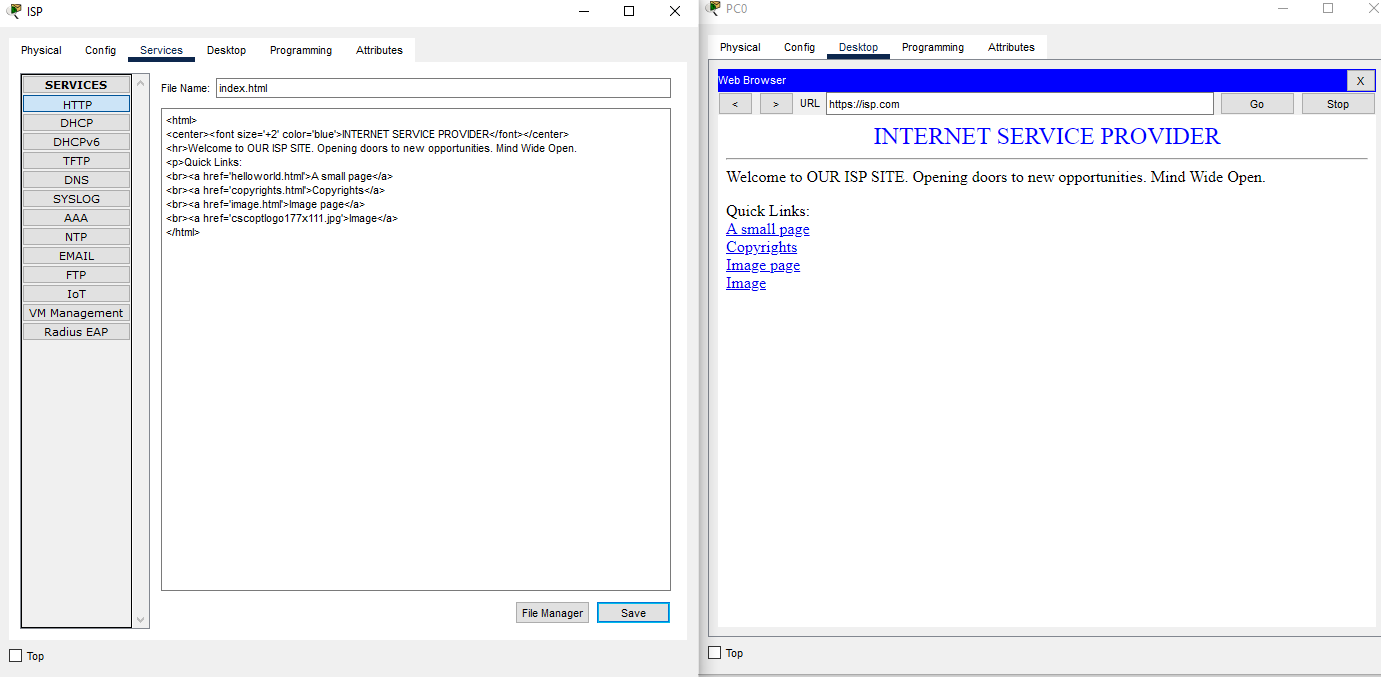


Final simulation for the network system to check all the connections

● **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.

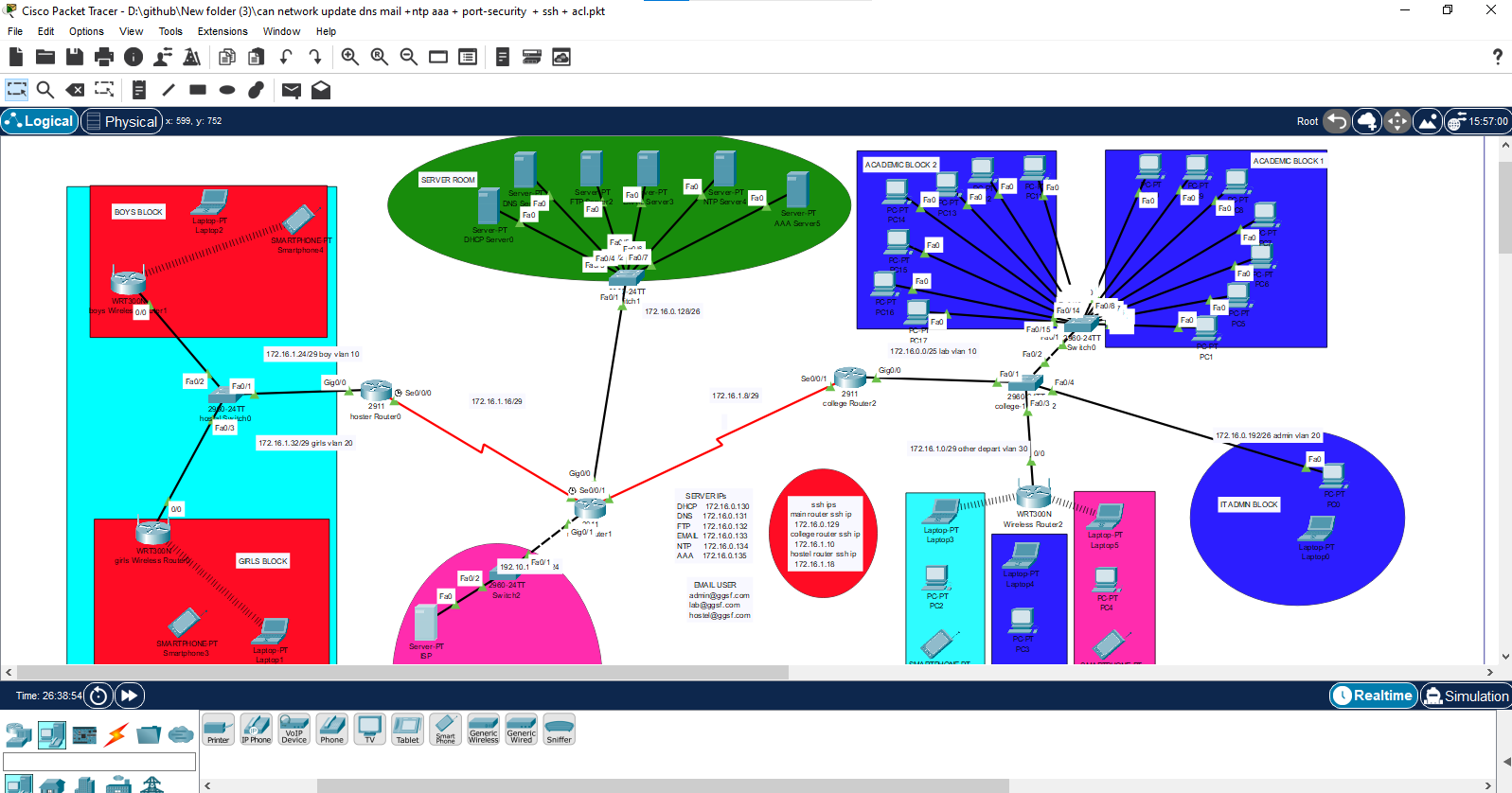




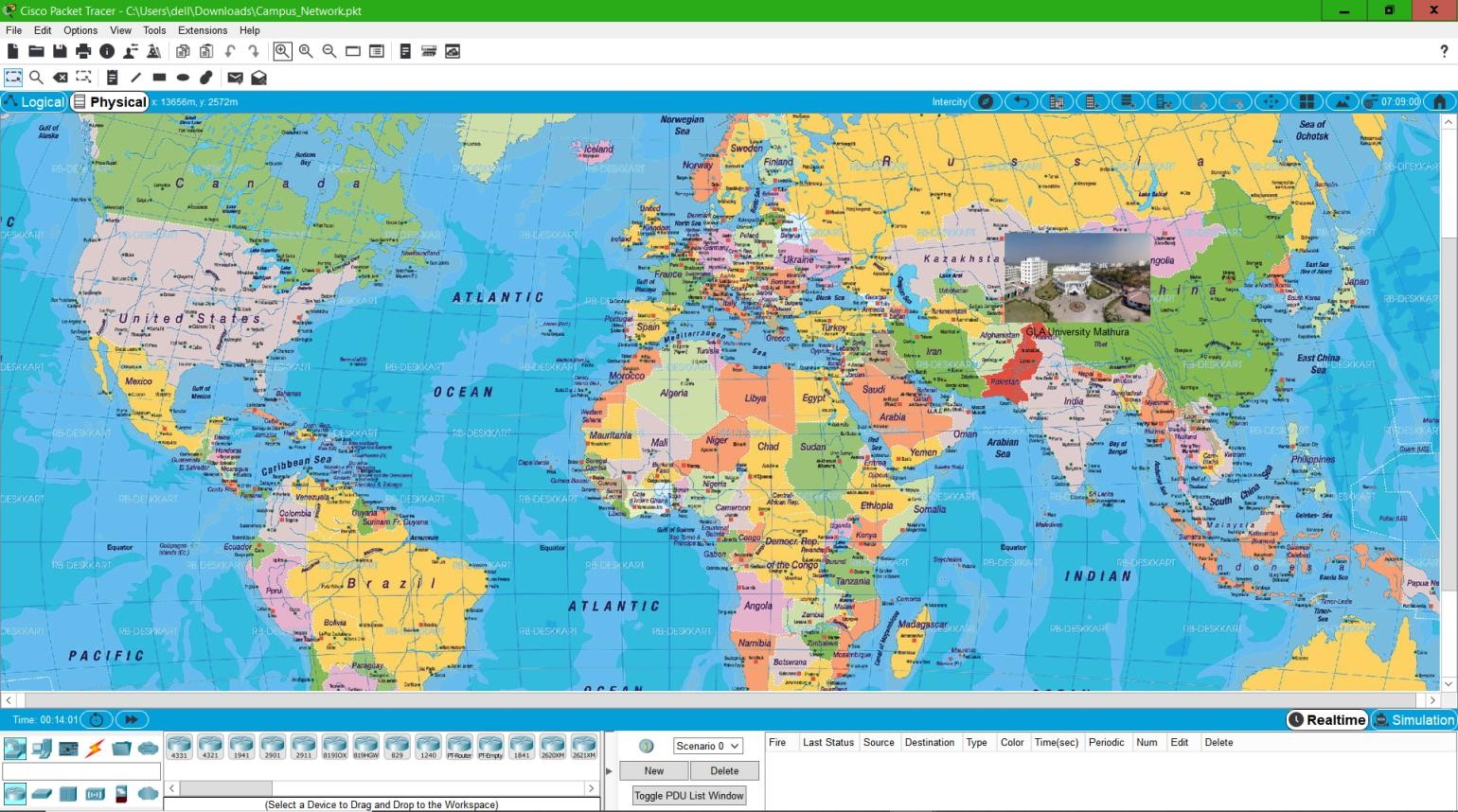


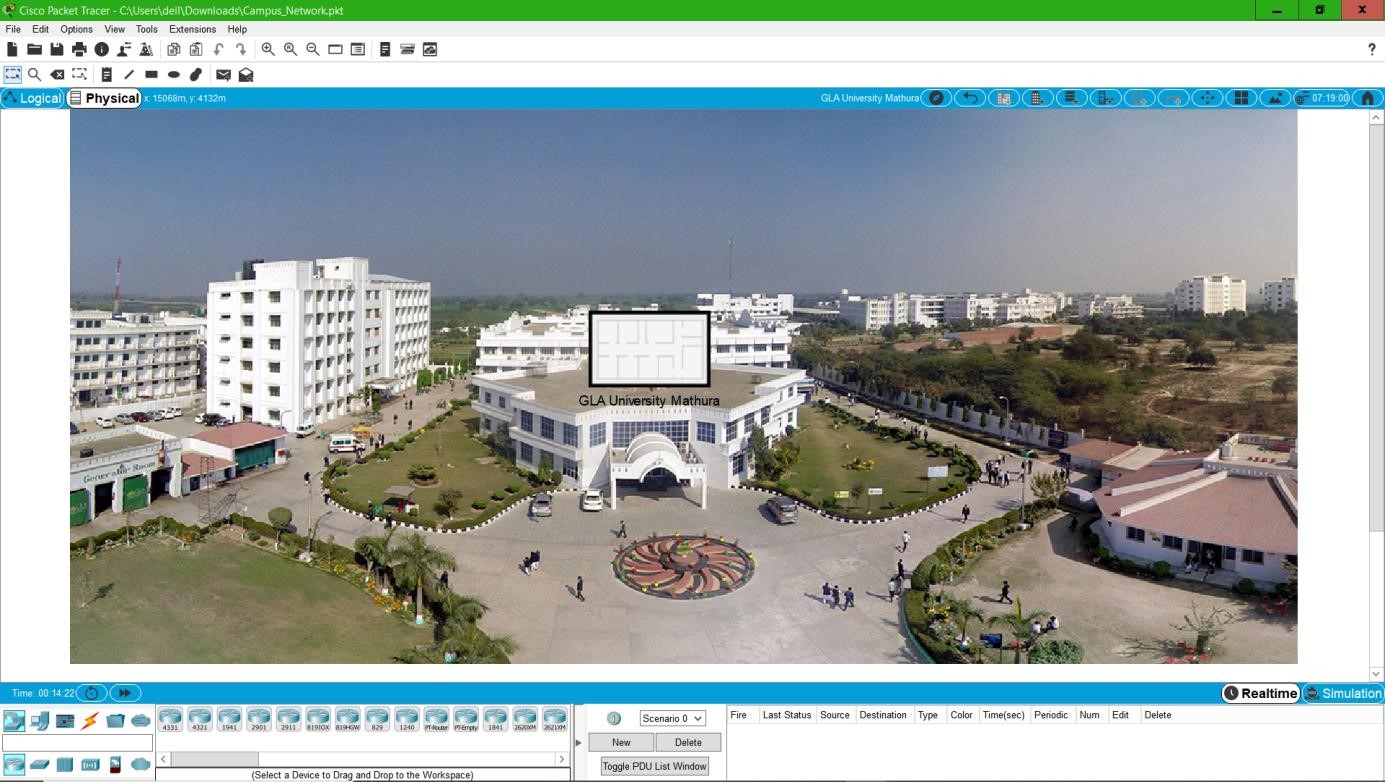
**SCREENSHOTS –**

## Logical View

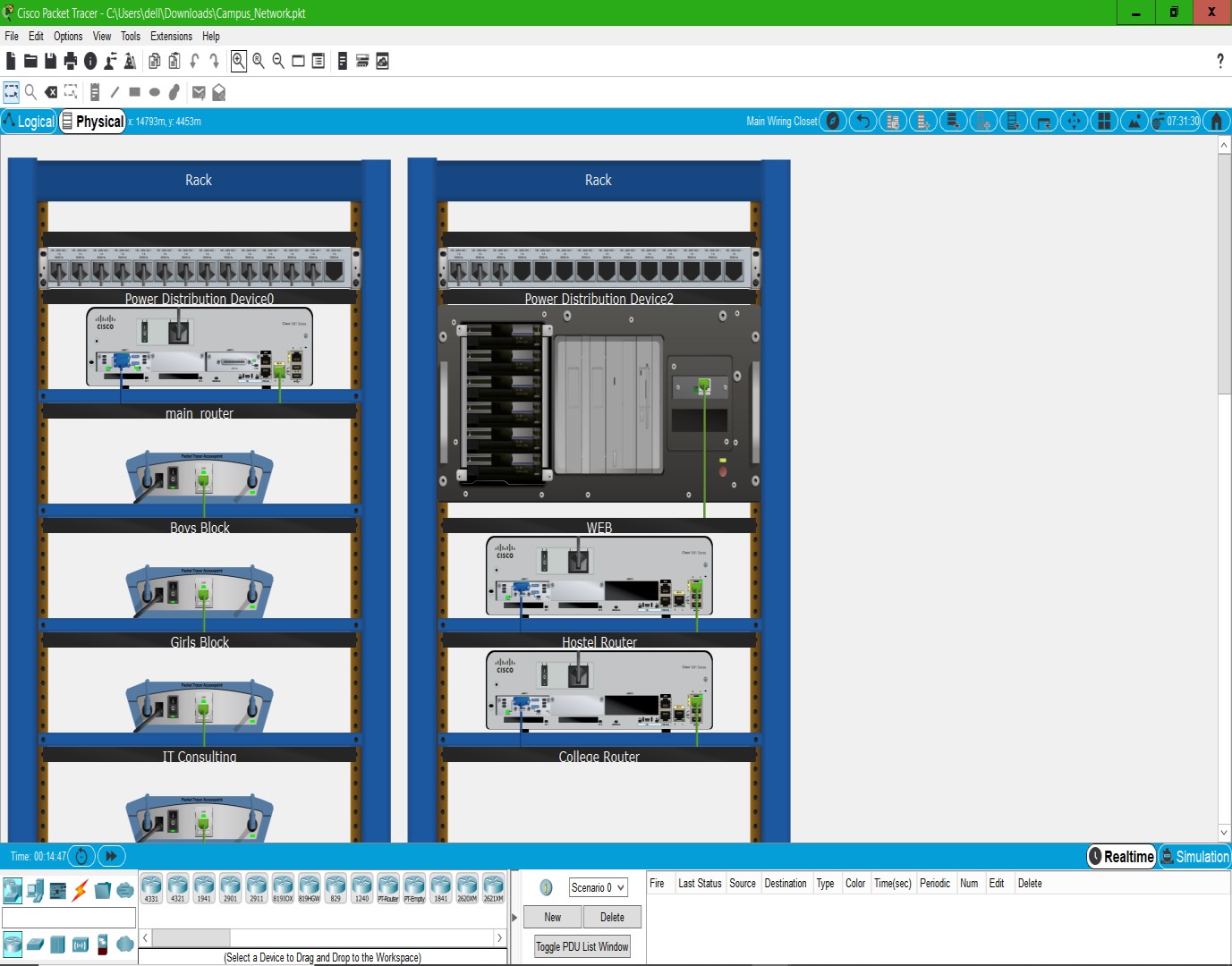


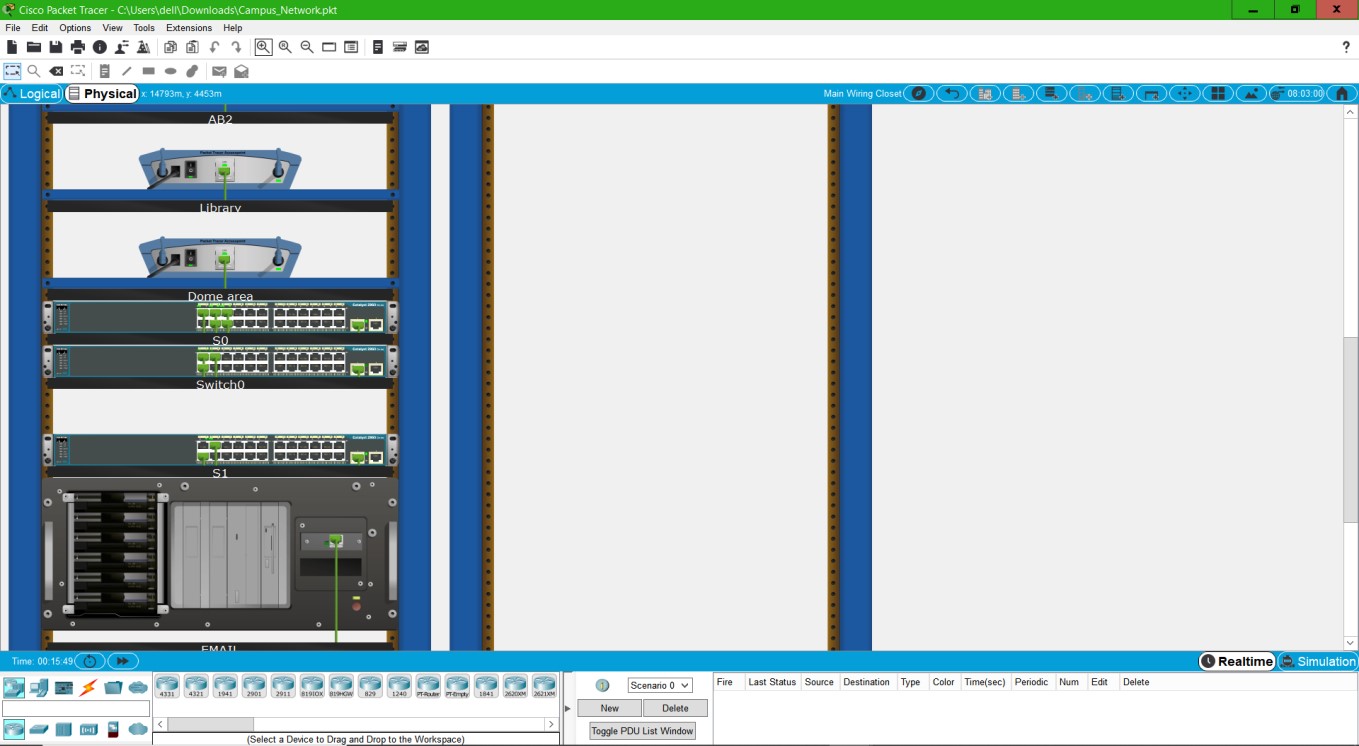
## Physical View -



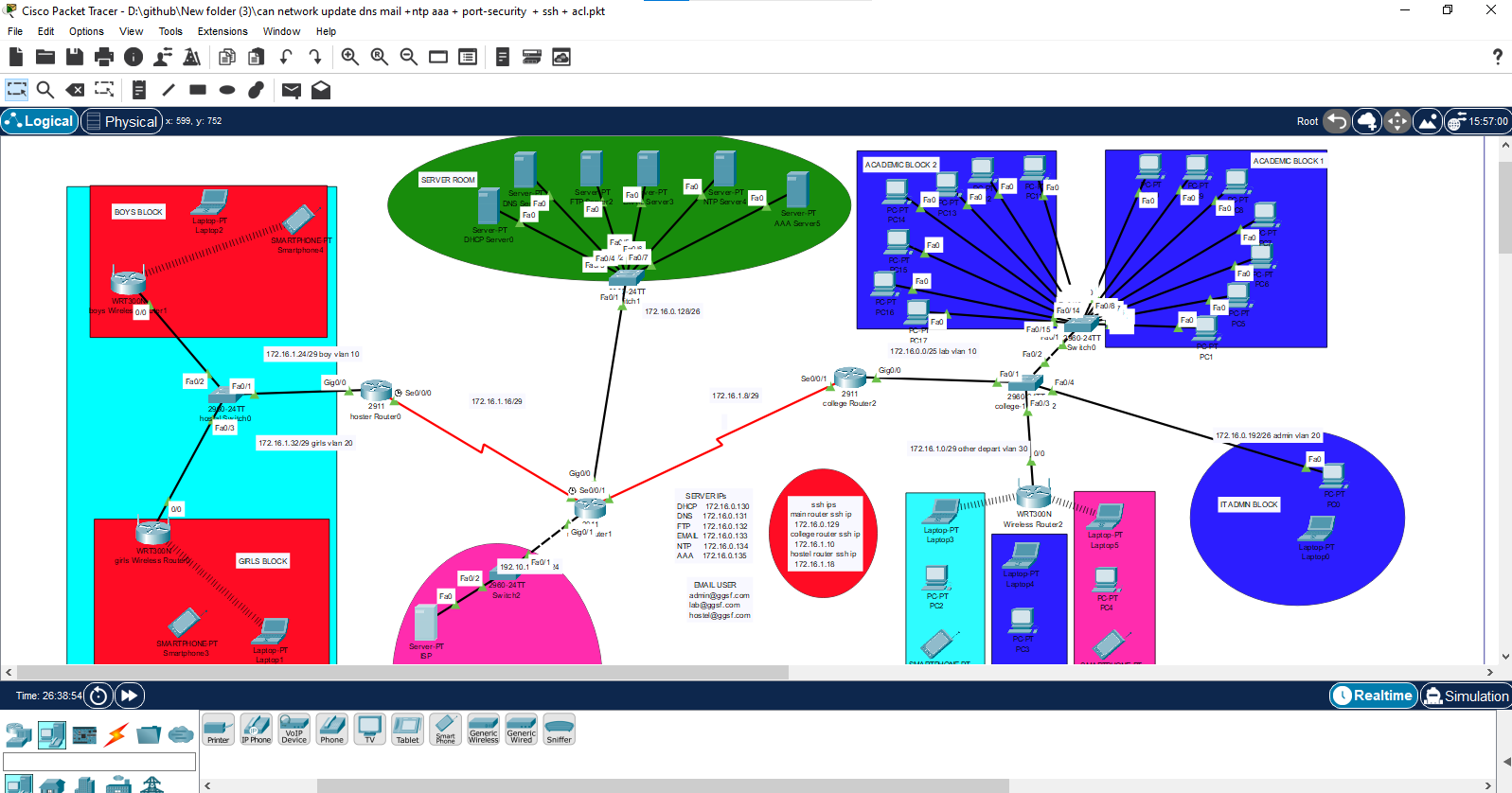


## Racks –





### Final Network Design –



**CHAPTER 5**

# CONCLUSION AND FUTURE WORK

## ● Conclusion

In this project, we will design 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 will include 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 will also include an email server to facilitate intra university communication

through emails within the domain. We will also use console pass words and SSH

protocol to ensure a safe and secure transfer of data.

We also use Access Control List to secure the network and control the traffic and

control the accessing the devices. We use NTP Server for update time & calendar

of devices. We use subnetting network ip. We use port security in labs switches ports.

## ● 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-sshconfiguration-on-a-switch-and-router-in-packet-tracer/](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-](http://router.over-blog.com/article-how-to-configure-cisco-router-password-106850439.html)

[106850439.html](http://router.over-blog.com/article-how-to-configure-cisco-router-password-106850439.html)

[5]<https://www.cognoscape.com/benefits-going-wireless/>