NLC INDIA LIMITED

("NAVRATNA" – A GOVERNMENT OF INDIAENTERPRISE)

NEYVELI – 607 801, TAMIL NADU

INTERNSHIP REPORT

ON

BASIC NETWORKING IN NLCIL

SUBMITTED BY

GANESH V

COMPUTER AND COMMUNICATION ENGINEERING

SRI SAIRAM INSTITUTE OF TECHNOLOGY

(AUTONOMOUS)

Sai Leo Nagar, West Tambaram, Chennai – 600 044.

NLC INDIA LIMITED

("NAVRATNA" – A GOVERNMENT OF INDIA ENTERPRISE)

NEYVELI – 607 801, TAMIL NADU

BONAFIDE CERTIFICATE

Certified that the Internship Training report titled **"BASIC NETWORKING IN NLCIL"** is the bonafide work of, **GANESH V (SIT22CO045)** Studying **COMPUTER AND COMMUNICATION ENGINEERING (B.E)** at **SRI SAIRAM INSTITUTEOF TECHNOLOGY** done during the period from 01-03-2024 to 15-03-2024 at **CORPORATE OFFICE**, NLC INDIA LIMITED, NEYVELI.

His performance, conduct and attendance during the period was outstanding

15/3/24

EXTERNAL GUIDE

SHALU MATHEWS JOHN

DCM/CS/CO

NLCIL NEYVELI

Permitted to submit the internship report to College Authorities

Dy.Chief Manager
Computer Serives,
corporate Office,
NLC India Ltd., Neyveli-1

15/3/24

CHIEF MANAGER,

LEARNING & DEVELOPMENT CENTRE

NLC INDIA LIMITED

DATE:15|03|2024

PLACE: NLCIL, NEYVELI, TAMIL NADU

Chief Manager
Learning & Development Centre
NLC India Limited, Neyveli-3.

DECLARATION

I hereby declare that the Internship training report titled **"BASIC NETWORKING IN NLCIL"** is the original work done by us under the guidance of **SHALU MATHEWS JOHN/DCM/CS/CO,** NLCIL, Neyveli.

This internship report is for reference only and no part of the report will be published copied anywhere without the written permission from officials of NLCIL, Neyveli.

Signature of the student

GANESH V

ACKNOWLEDGEMENT

I express my sincere thanks to **NLC INDIA LIMITED** for providing me the opportunity to carry out the Internship Training.

I also express my sincere thanks to **SHRI. SARAVANABHAVAN A KR, DGM/L&DC** and the staff of Learning & Development Centre for providing me the opportunity to carry out the Internship Training in NLC India Limited, Neyveli.

I also express my sincere thanks to Unit Head **SHRI. SOLOMON LUTHER KING D/ CGM CS/CO** and the staff of Corporate Office for providing me the opportunity to carry out the Internship Training in NLC India Limited, Neyveli.

I sincerely thank **SHRI. SHALU MATHEWS JOHN/DCM/CS/CO NLCIL NEYVELI,** for providing the guidance during the internship training programme from 01-03-2024 to 15-03-2024.

I sincerely thank **Dr. K. PALANIKUMAR, PRINCIPAL/ SRI SAIRAM INSTITUTE OF TECHNOLOGY** for providing me support and guidance for the Internship.

My heartfelt thanks **Dr. PAHHAIAMMAL ALIAS PRIYA.M HEAD OF THE DEPARTMENT/COMPUTER AND COMMUNICATION, SRI SAIRAM INSTITUTE OF TECHNOLOGY** for making it convenient to undertake an internship training in NLC India Limited, Neyveli.

CONTENT OF THE REPORT

ABSTRACT

Computer networks have a significant impact on the working of an organization. Organizations depend on the proper functioning and analysis of their networks for education, administration, communication, e-library block, 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 an organization.

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

i. Admin Blocks
ii. Software unit
iii. Hardware unit
iv. Conference hall
v. Trainee block
vi. Reception
vii. Server room

CHAPTER 1

1.0 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 industrial training organization plays an important role in this digitalization; hence the organization should adapt to digital means of networking as well and become a “digital organization”. 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.

organization networking via wireless connection becomes an important part of organization life and provides the main way for staffs and trainee 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 organization and wisdom organization. It provides an efficient way to explore the internet with a mobile terminal for staffs and trainee regardless of cables and places. This is an important mark of the modern organization as a supplement of a cable network. With the development of network and communication technology, cable networks on an organization 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 organization.

1.1 Project Statement

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

The major aim of this project is to show the wireless connectivity and simulation design that is used in organizations 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 (organization staff and trainee), we have added DNS, Email, and HTTP servers for the maximum utilization of resources.

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

CHAPTER 2

2.0 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 trainee as an educational tool for helping them learn fundamental CCNA concepts. Previously trainee 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.

1.1 Project Statement

In this mini-project, we defined a simulation of organization networks based on wireless networking. The network is divided into two sets: one for the organization area and the other for the staff area.The major aim of this project is to show the wireless connectivity and simulation design that is used in organizations 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 (organization staff and trainee), we have added DNS, Email, and HTTP servers for

the maximum utilization of resources.

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

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

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 an organization. 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 organization makes it easier for staffs and trainee to access educational resources, by enabling an important platform to exchange information.

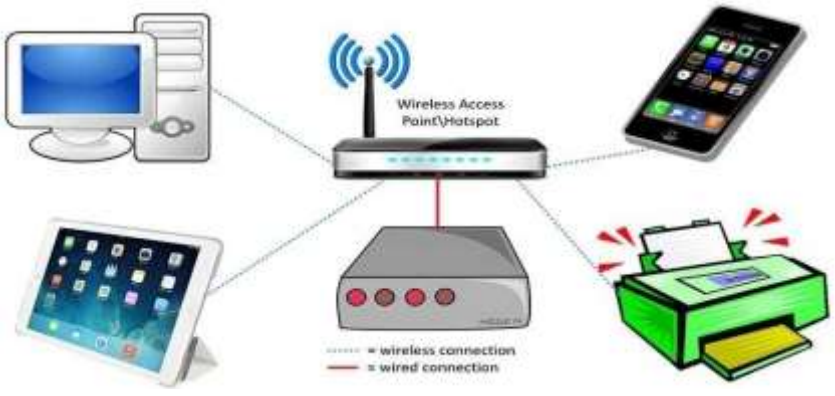


Figure 1: Shows the wireless connection access by various tool

3. Network Requirements

Ultratech's outline is considered for this wireless organization network.

The network is divided into 2 areas:

1. Main Organization Area

   The main Organization area is further divided into various accessing points like Admin/trainee building, Trainee block, Academic Blocks (SOFTWARE UNIT and HARDWARE UNIT), Server Center, and Admin block.

2. Trainee and guess Area

   The Staff area is further divided into Conference hall and Reception hall respectively.

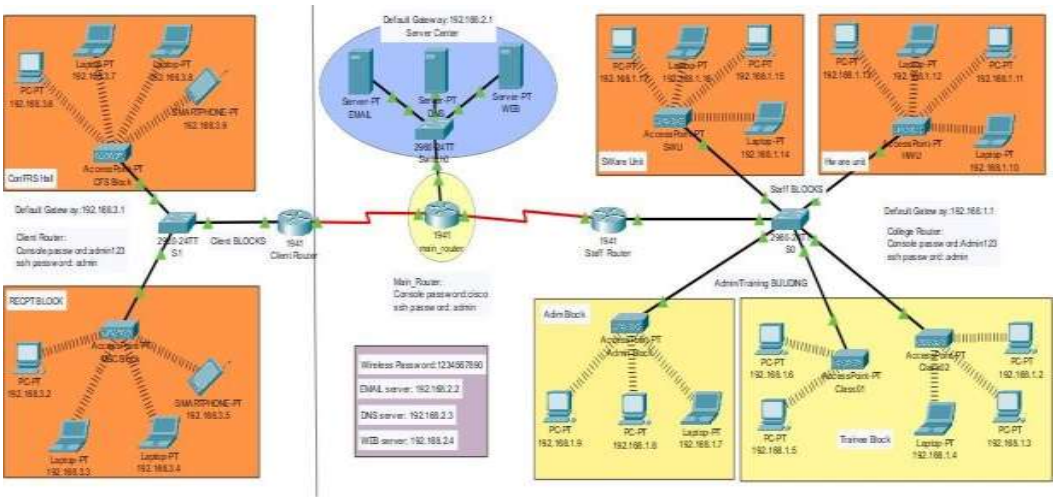


Figure 2: Basic layout of our wireless access points in Organization

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

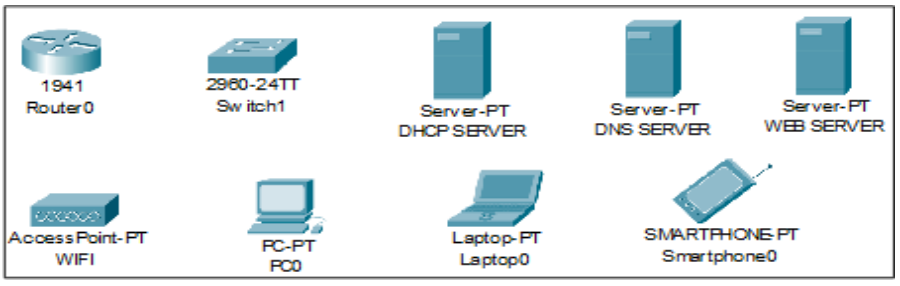


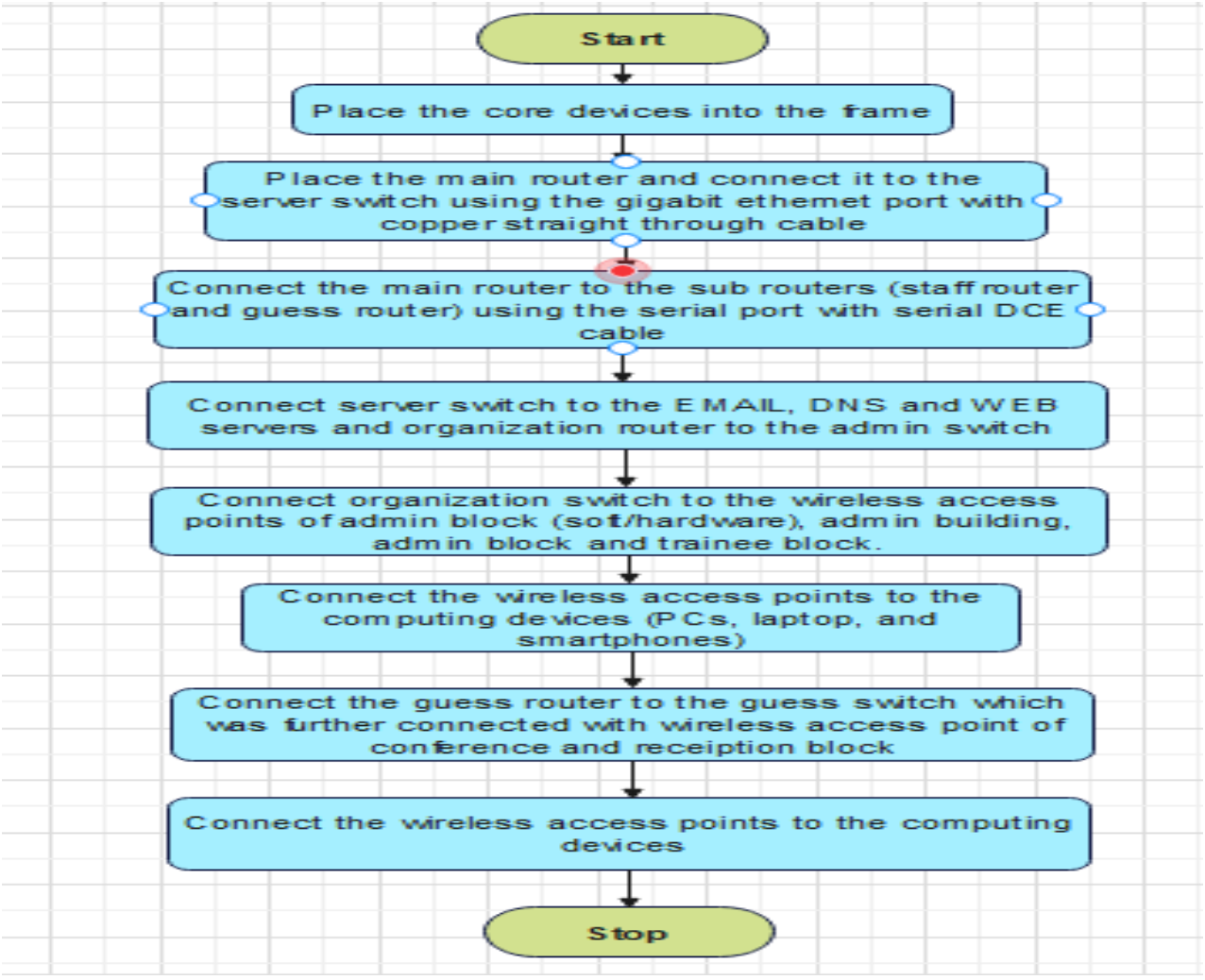
Figure 3: Devices used in the network

4. Implementation and Flow Diagram

- To design the wireless network of the organization 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 organization outline, which was further connected to the **server switch** using the gigabit ethernet port with copper straight-through cable and sub routers (**organization router and staff router**) using the serial port with serial DCE cable at the staff area and organization area respectively.
- The server switch was further connected to the **EMAIL, DNS, and WEB** servers respectively.
- Organization router was connected to the organization switch which was further connected with wireless access points of the software unit

(**SOFTWARE UNIT and HARDWARE UNIT**), **Admin/trainee building**, **trainee block,** and **Admin block.**

- The wireless access points were then connected to computing devices (PCs, laptops, and smartphones).
- Similarly, the staff router was connected to the staff 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.

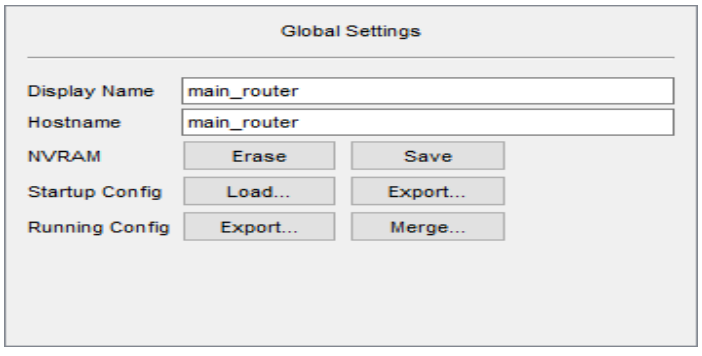


This is the flow diagram for a better understanding of the steps mentioned above.

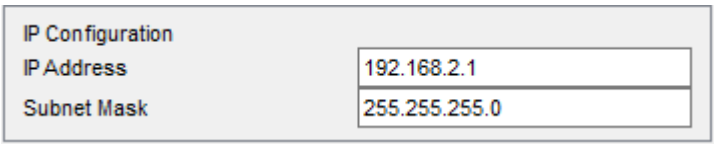
5. Configuring IP Addresses

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

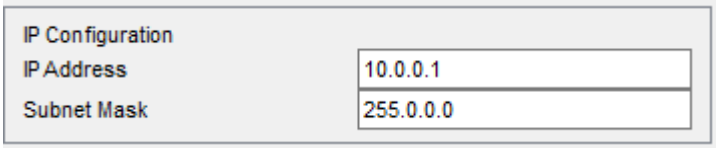
- Main Router configuration



GigabitEthernet0/1



Serial0/1/0



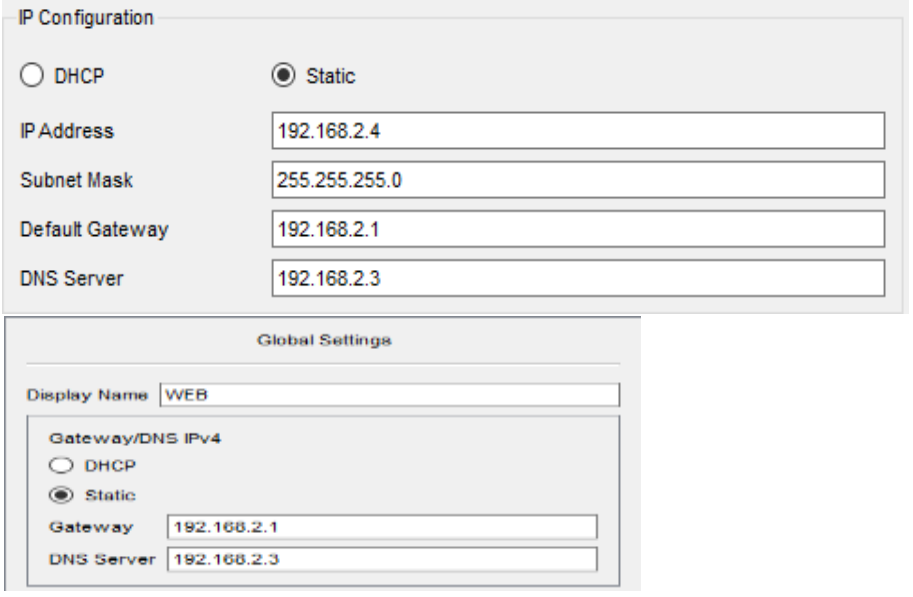
Serial0/1/1

RIP

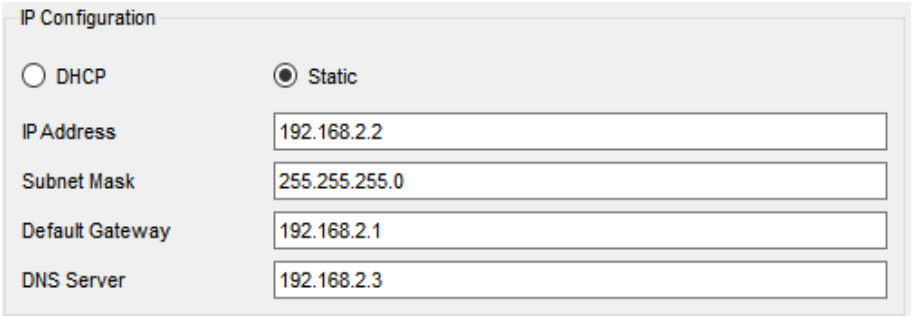
Network Address
10.0.0.0
11.0.0.0
192.168.1.0
192.168.2.0

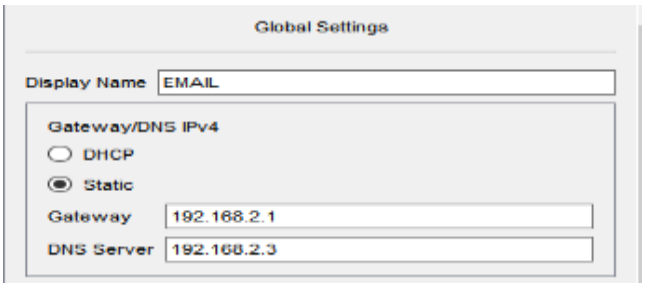
- DNS SERVER

- WEB SERVER

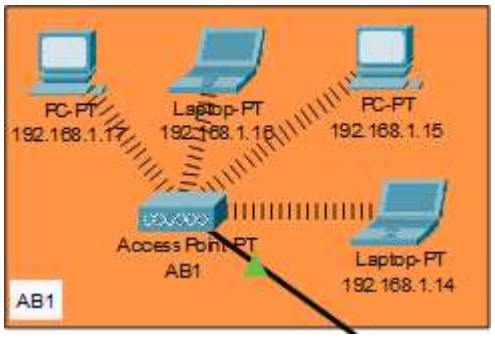


- EMAIL SERVER





- SOFTWARE UNIT 1



IP Address are as follows

192.168.1.14- Laptop

192.168.1.15- PC

192.168.1.16- Laptop

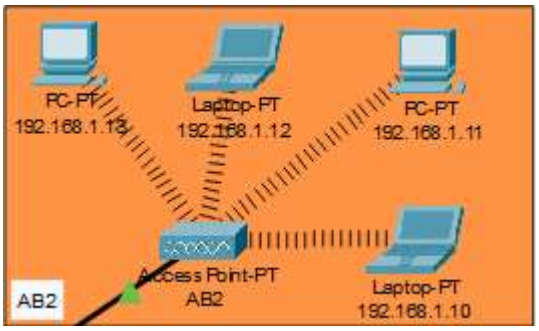
192.168.1.17- PC

Subnet Mask- 255.255.255.0

Default Gateway- 192.168.1.1

DNS Server- 192.168.2.3

- HARDWARE UNIT2



IP Address are as follows

192.168.1.10- Laptop

192.168.1.11- PC

192.168.1.12- Laptop

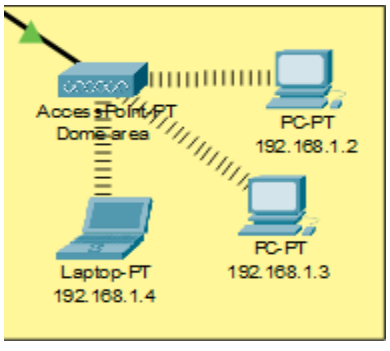
192.168.1.13- PC

Subnet Mask- 255.255.255.0

Default Gateway- 192.168.1.1

DNS Server- 192.168.2.3

- ADMIN/TRAINEE BUILDING



IP Addresses are as follows

192.168.1.2- PC

192.168.1.3- PC

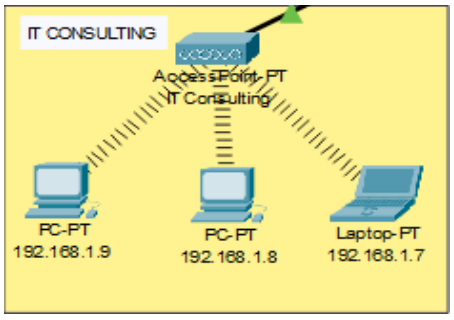
192.168.1.4- Laptop

Subnet Mask- 255.255.255.0

Default Gateway- 192.168.1.1

DNS Server- 192.168.2.3

- Admin block



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

- WIRELESS ACCESS POINT

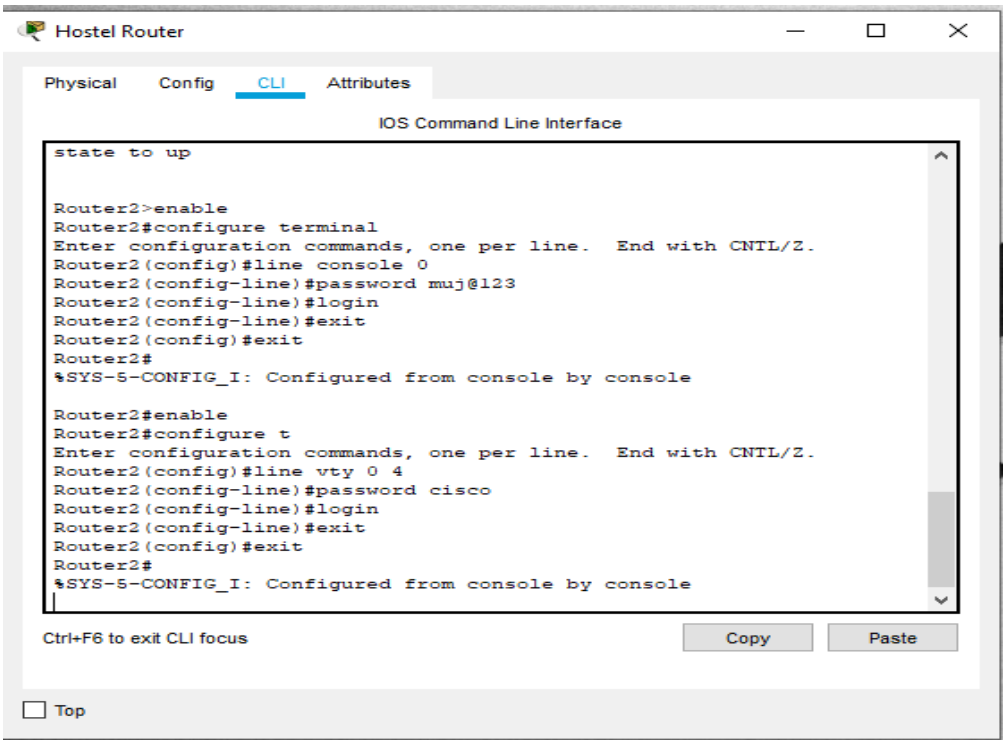
SSID	Password
1)muj_Admin/trainee	1234567890
2)muj_trainee block	1234567890
3)muj_ITC	1234567890
4)muj_SOFTWARE UNIT	1234567890
5)muj_HARDWARE UNIT	1234567890
6)muj_rec	1234567890
7)muj_conf	1234567890

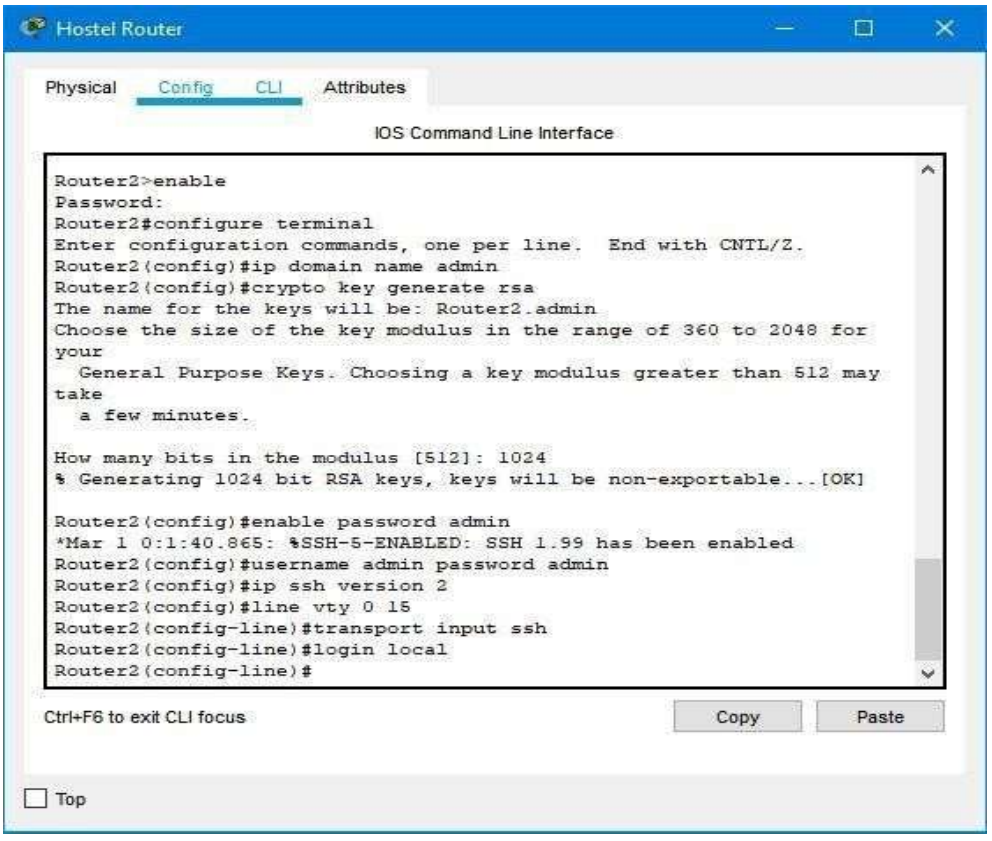
6. Securing the network

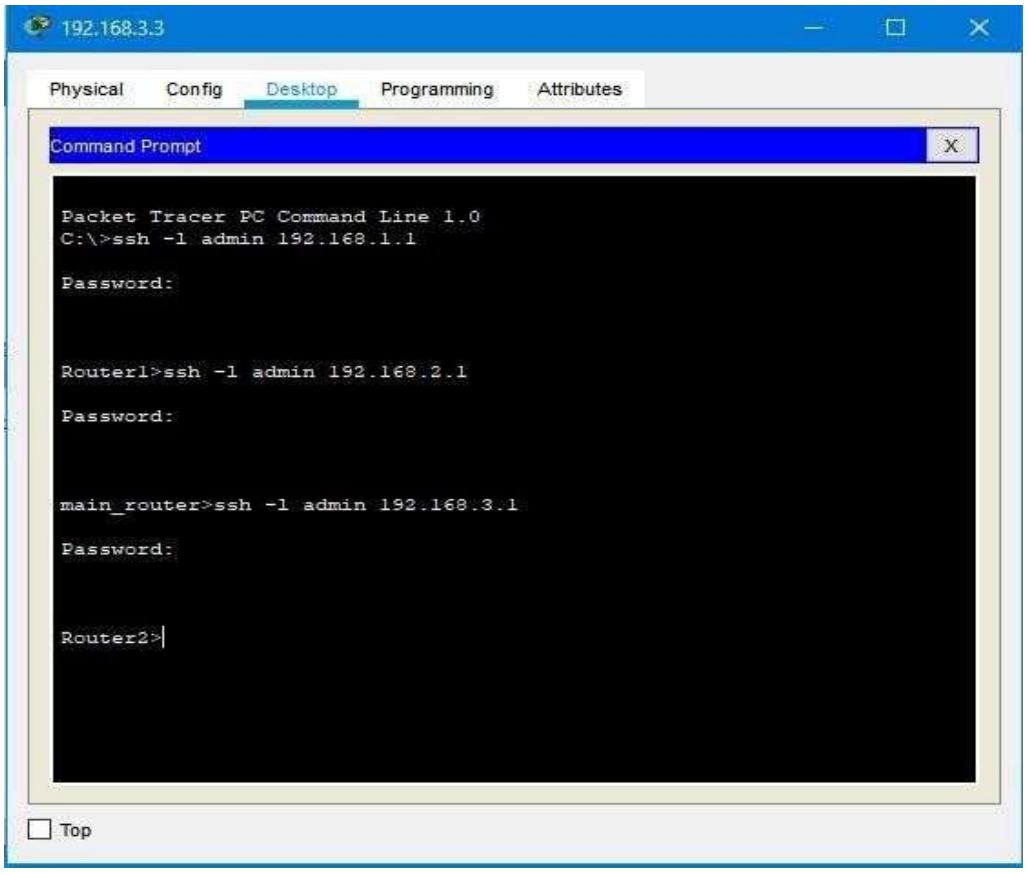
Passwords are used in accessing the router and all the wireless networks (mentioned in step 5 wireless access point) to make the access limited to Organization authorized users only.

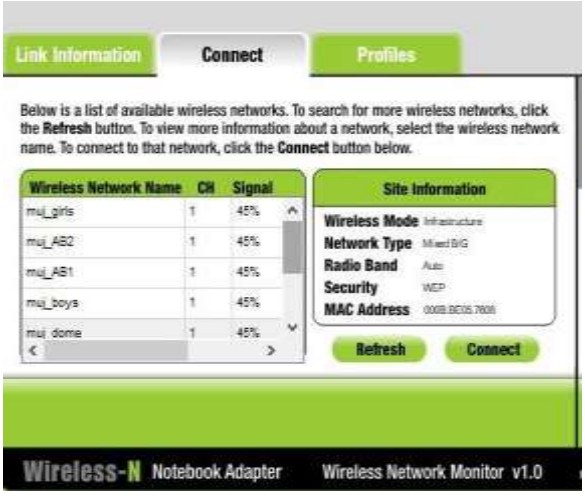
Routers are also secured with ssh (Secure Shell). Routers and their assigned passwords are mentioned below:

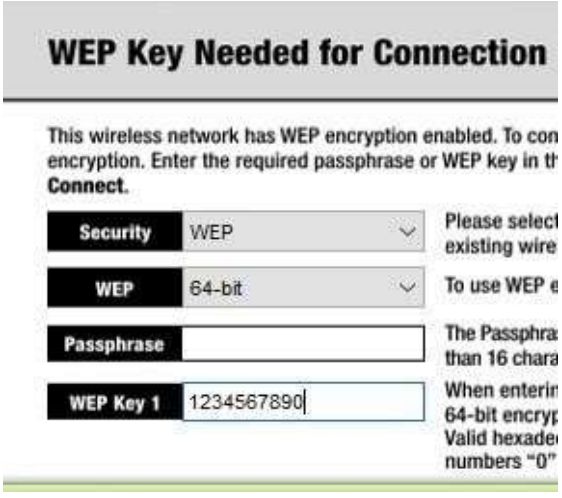
Router Name	Passwords
1)main_router	Console password: cisco ssh password: admin
2)Router1(Organization Router)	Console password:admin@123 ssh password: admin
3)Router2(Staff Router)	Console password:admin@123 ssh password: admin


Hostel Router
Physical
Config
CLI
Attributes
IOS Command Line Interface
state to up
Router2>enable
Router2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router2(config)#line console 0
Router2(config-line)#password muj@123
Router2(config-line)#login
Router2(config-line)#exit
Router2(config)#exit
Router2#
%SYS-5-CONFIG_I: Configured from console by console
Router2#enable
Router2#configure t
Enter configuration commands, one per line. End with CNTL/Z.
Router2(config)#line vty 0 4
Router2(config-line)#password cisco
Router2(config-line)#login
Router2(config-line)#exit
Router2(config)#exit
Router2#
%SYS-5-CONFIG_I: Configured from console by console
Ctrl+F6 to exit CLI focus
Copy
Paste
Top


Hostel Router
Physical
Config
CLI
Attributes
IOS Command Line Interface
Router2>enable
Password:
Router2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router2(config)#ip domain name admin
Router2(config)#crypto key generate rsa
The name for the keys will be: Router2.admin
Choose the size of the key modulus in the range of 360 to 2048 for
your
General Purpose Keys. Choosing a key modulus greater than 512 may
take
a few minutes.
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
Router2(config)#enable password admin
*Mar 1 0:1:40.865: %SSH-5-ENABLED: SSH 1.99 has been enabled
Router2(config)#username admin password admin
Router2(config)#ip ssh version 2
Router2(config)#line vty 0 15
Router2(config-line)#transport input ssh
Router2(config-line)#login local
Router2(config-line)#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top





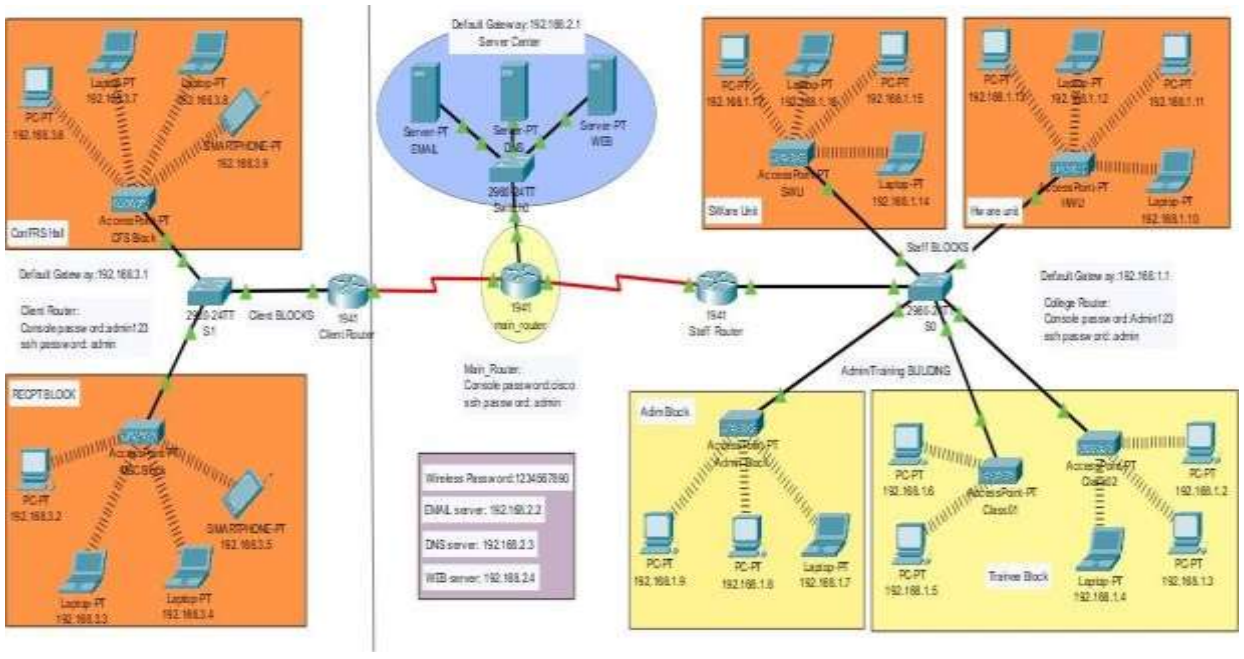


Connectivity of wireless network on computing devices

CHAPTER 4

RESULT & DISCUSSION

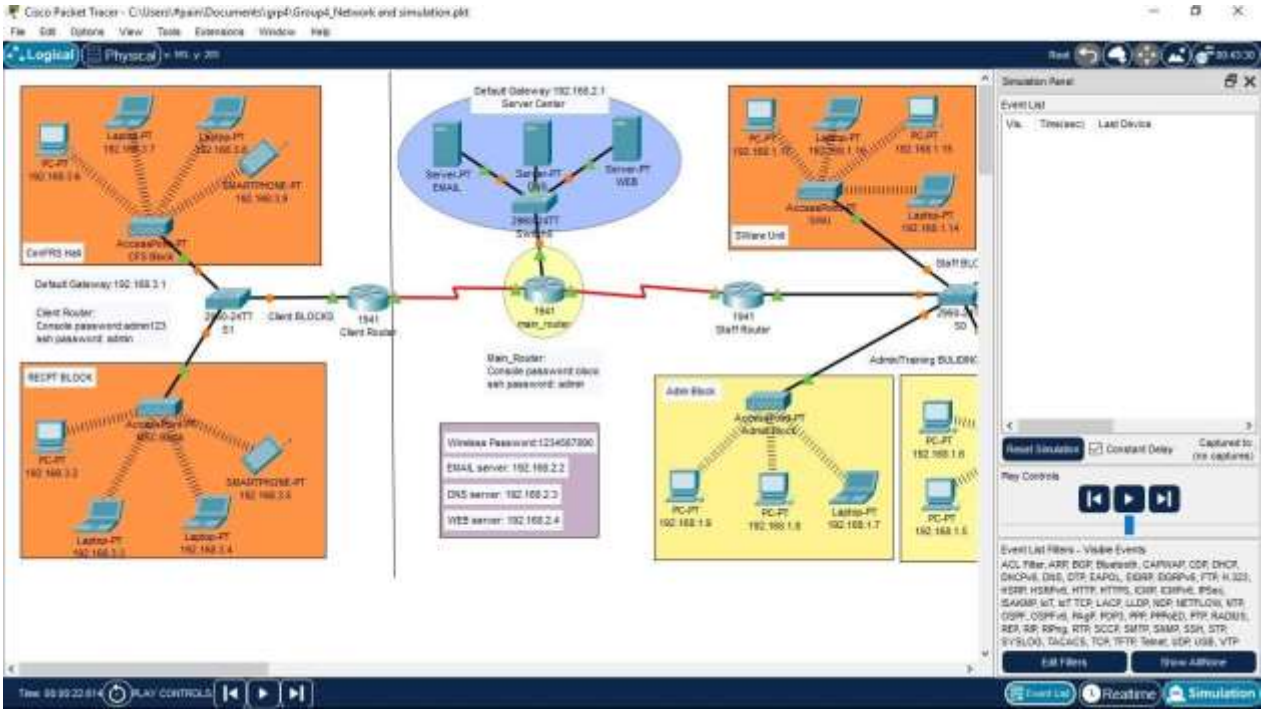
Finally, we have combined all the steps as mentioned in chapter 3 (work done) and implemented the desired wireless network for Organization. We have the complete network providing various facilities to the teaching staff, non-teaching staff, and trainee.



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

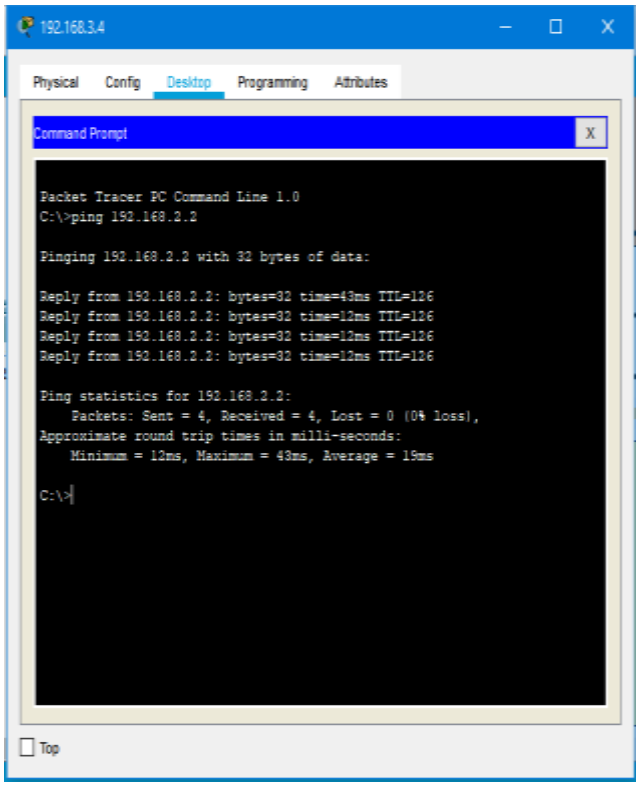
- **Final Simulation:**

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:

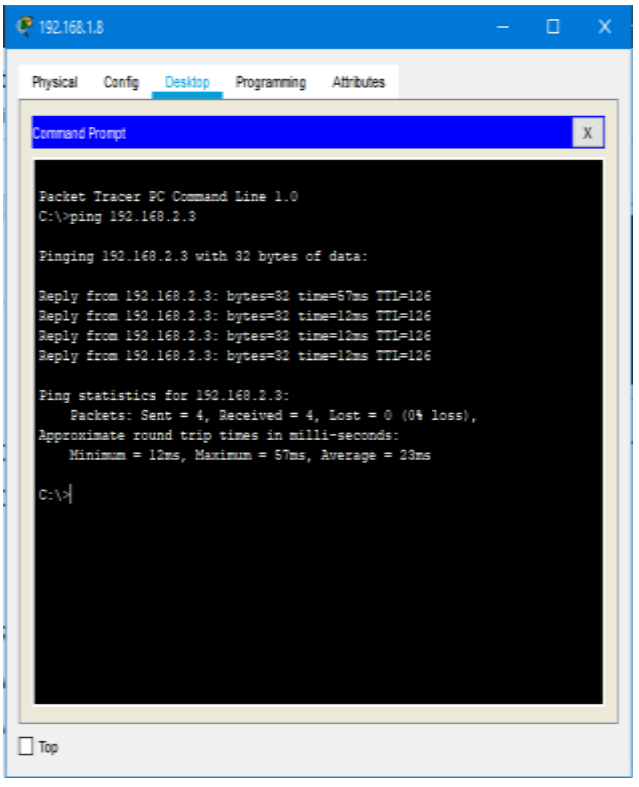


Final simulation for the network system to check all the connections

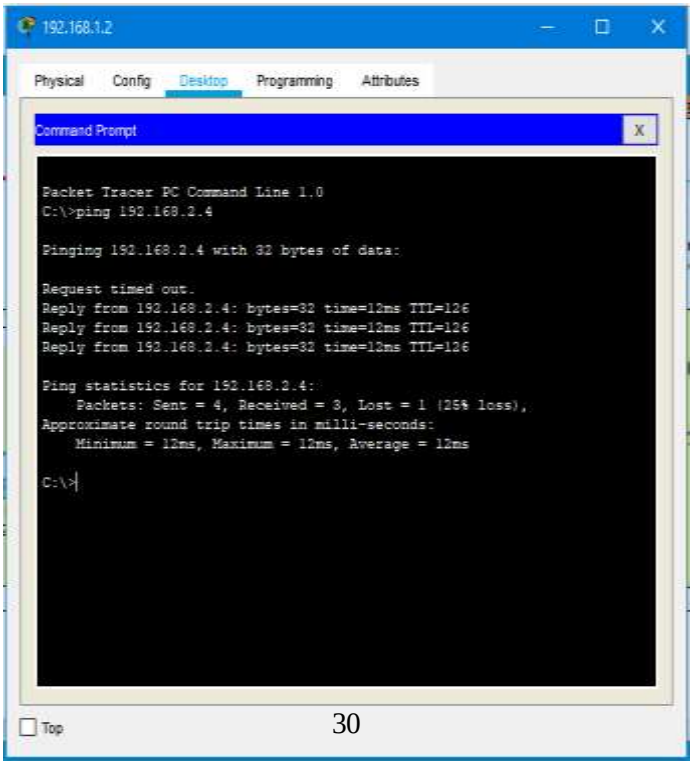
- **Ping Test**: Network connectivity and communication can be tested using the ping command, followed by the domain name or the IP address of the device (equipment) whose connectivity one wishes to verify.



Ping Test for EMAIL server



Ping Test for DNS server



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 Organization, 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 an Organization Network using Cisco Packet Tracer that uses a networking topology implemented using servers, routers, switches, and end devices in a multiple area network. 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 trainee and staffs. We have included an email server to facilitate intra organization 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.

CHAPTER 6

TENABLE NESSUS AUDIT:

Nessus is a powerful vulnerability scanning tool commonly used to audit network systems for security vulnerabilities. Here's a basic overview of how you might use Nessus to audit basic networking:

Installation and Setup: Start by installing Nessus on your system. Once installed, configure it to scan the network you want to audit. This typically involves providing the IP addresses or ranges of the systems you want to scan.

Scan Configuration: Define the parameters of your scan. Decide whether you want a basic scan or a more comprehensive one. Basic scans usually check for common vulnerabilities and misconfigurations, while more advanced scans can delve deeper into the system.

Initiate the Scan: Once the configuration is set up, initiate the scan. Nessus will start scanning the network and the systems within it based on the parameters you've defined.

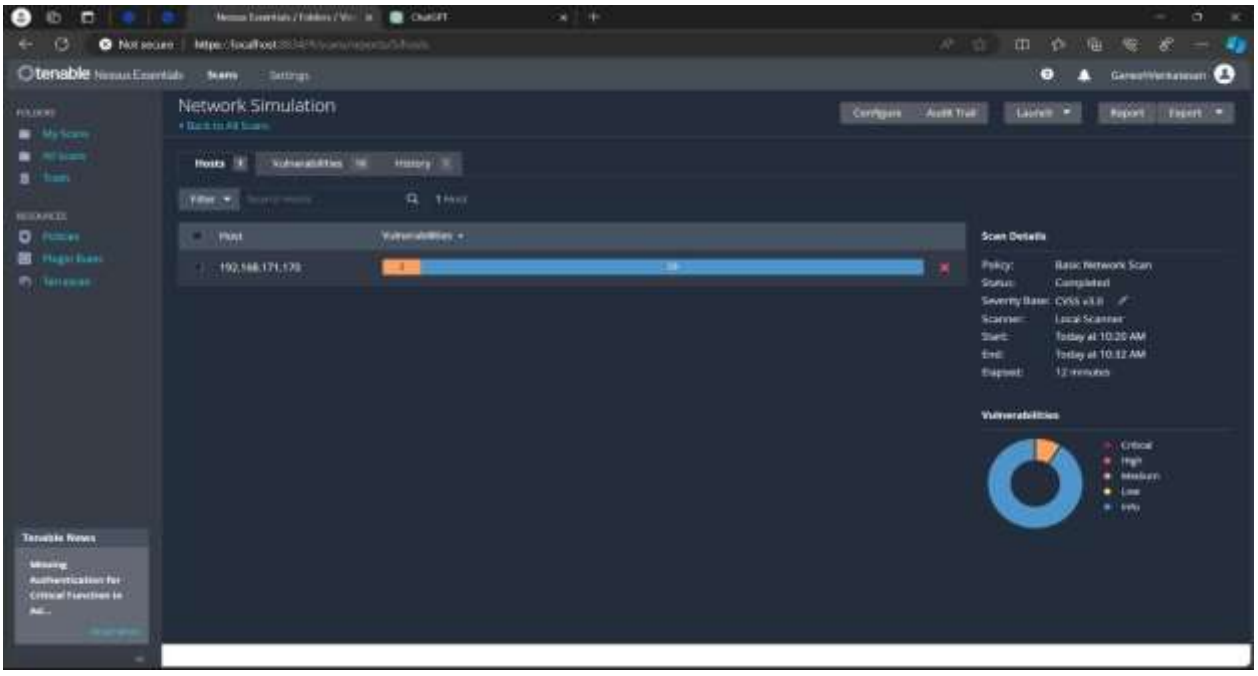
Analysis of Results: After the scan is complete, review the results. Nessus will provide a report detailing any vulnerabilities or issues it has found. It typically categorizes vulnerabilities by severity, making it easier to prioritize remediation efforts.

Remediation: Once vulnerabilities are identified, take appropriate action to address them. This might involve applying patches, reconfiguring systems, or implementing additional security measures.

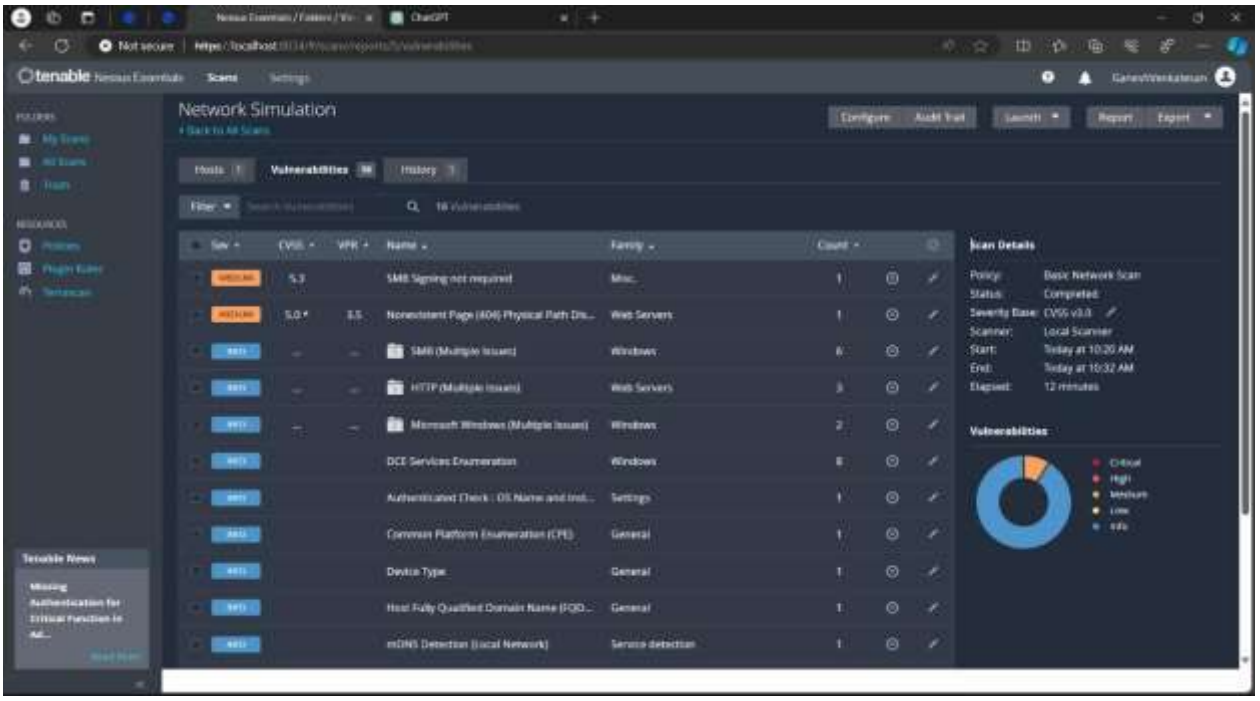
Regular Scanning: Network security is an ongoing process. Regularly schedule scans with Nessus to ensure that new vulnerabilities are promptly identified and addressed.

Remember, while Nessus is a powerful tool, it's just one part of a comprehensive security strategy. It's essential to combine vulnerability scanning with other security measures such as intrusion detection, firewall configuration, and user education to ensure the overall security of your network.

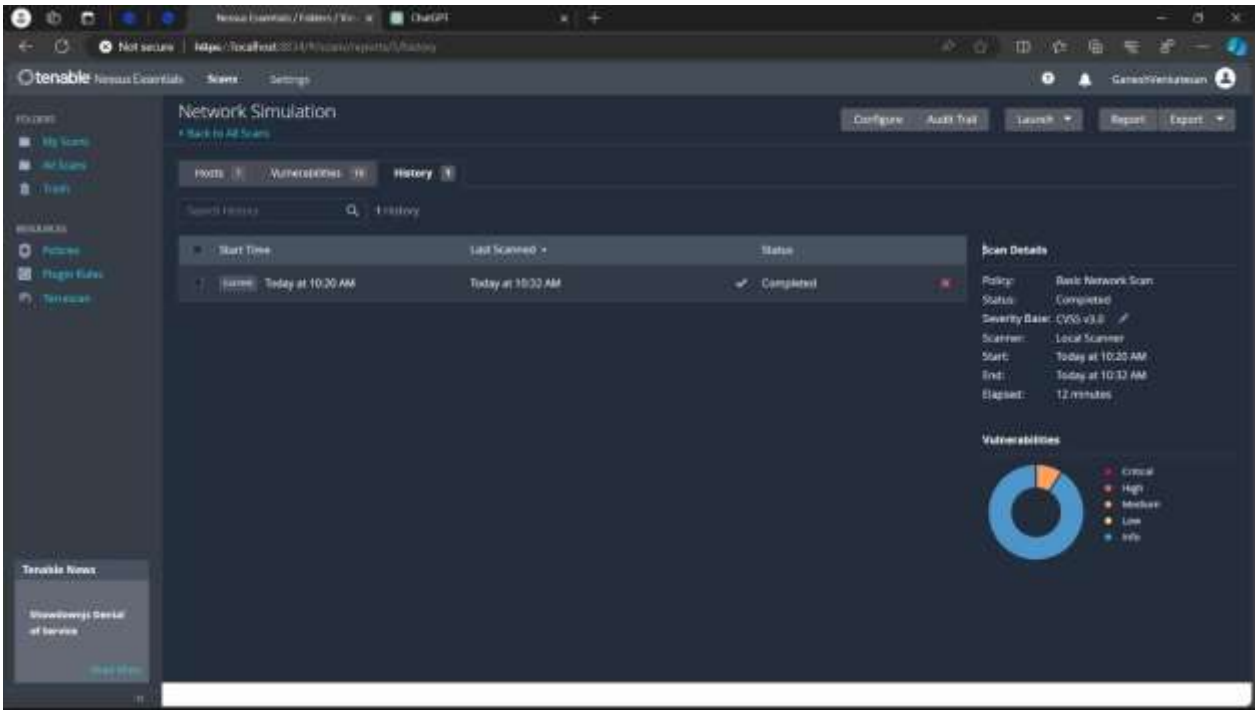
BASIC NETWORKING:



HOSTS



VULNERABILITIES



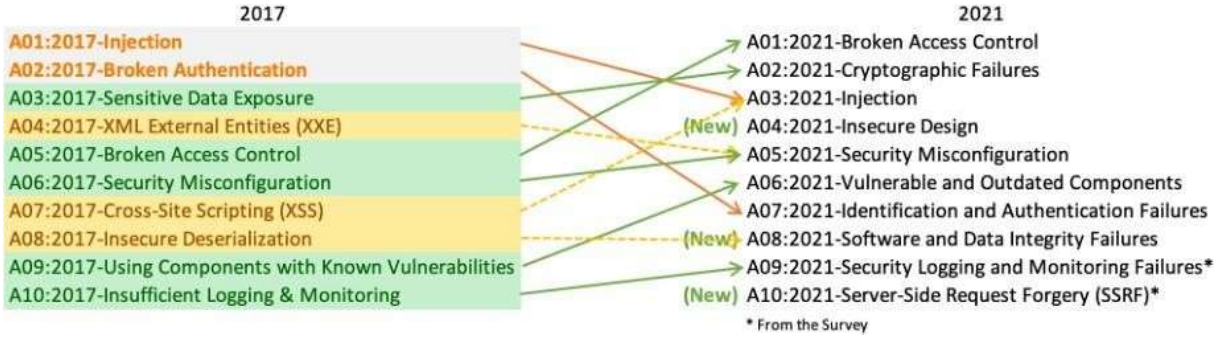
BASIC NETWORKING AUDIT

\

Chapter 7

STUDY OF TOP 10 VULNERABILITIES:

There are three new categories, four categories with naming and scoping changes, and some consolidation in the Top 10 for 2021.



- **A01:2021-Broken Access Control** moves up from the fifth position; 94% of applications were tested for some form of broken access control. The 34 Common Weakness Enumerations (CWEs) mapped to Broken Access Control had more occurrences in applications than any other category.
- **A02:2021-Cryptographic Failures** shifts up one position to #2, previously known as Sensitive Data Exposure, which was broad symptom rather than a root cause. The renewed focus here is on failures related to cryptography which often leads to sensitive data exposure or system compromise.
- **A03:2021-Injection** slides down to the third position. 94% of the applications were tested for some form of injection, and the 33 CWEs mapped into this category have the second most occurrences in applications. Cross-site Scripting is now part of this category in this edition.
- **A04:2021-Insecure Design** is a new category for 2021, with a focus on risks related to design flaws. If we genuinely want to "move left" as an industry, it calls for more use of threat modeling, secure design patterns and principles, and reference architectures.

- **A05:2021-Security Misconfiguration** moves up from #6 in the previous edition; 90% of applications were tested for some form of misconfiguration. With more shifts into highly configurable software, it's not surprising to see this category move up. The former category for XML External Entities (XXE) is now part of this category.
- **A06:2021-Vulnerable and Outdated Components** was previously titled Using Components with Known Vulnerabilities and is #2 in the Top 10 community survey, but also had enough data to make the Top 10 via data analysis. This category moves up from #9 in 2017 and is a known issue that we struggle to test and assess risk. It is the only category not to have any Common Vulnerability and Exposures (CVEs) mapped to the included CWEs, so a default exploit and impact weights of 5.0 are factored into their scores.
- **A07:2021-Identification and Authentication Failures** was previously Broken Authentication and is sliding down from the second position, and now includes CWEs that are more related to identification failures. This category is still an integral part of the Top 10, but the increased availability of standardized frameworks seems to be helping.
- **A08:2021-Software and Data Integrity Failures** is a new category for 2021, focusing on making assumptions related to software updates, critical data, and CI/CD pipelines without verifying integrity. One of the highest weighted impacts from Common Vulnerability and Exposures/Common Vulnerability Scoring System (CVE/CVSS) data mapped to the 10 CWEs in this category. Insecure Deserialization from 2017 is now a part of this larger category.

- **A09:2021-Security Logging and Monitoring Failures** was previously Insufficient Logging & Monitoring and is added from the industry survey (#3), moving up from #10 previously. This category is expanded to include more types of failures, is challenging to test for, and isn't well represented in the CVE/CVSS data. However, failures in this category can directly impact visibility, incident alerting, and forensics.
- **A10:2021-Server-Side Request Forgery** is added from the Top 10 community survey (#1). The data shows a relatively low incidence rate with above average testing coverage, along with above-average ratings for Exploit and Impact potential. This category represents the scenario where the security community members are telling us this is important, even though it's not illustrated in the data at this time.

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/