



Amity Institute of Information and Technology

Secure Protocol Design Lab

MCS145

Course: MSc Cyber Security

Semester: 1

LAB MANUAL

Submitted By:

Adnanmohammad Mugal

A217131524022

Sem – I , Batch – A

Submitted To:

Mr. Amit Kumar Singh

Assistant Professor

INDEX

| LAB No: | Practical Name | Page Numbers |
|----------------|---|---------------------|
| 1 | Designing Remote Connectivity | 3 |
| 2 | Designing IP Addressing | 7 |
| 3 | Selecting Routing Protocols | 11 |
| 4 | Wireless Network Design | 14 |
| 5 | Designing Security Solutions | 19 |
| 6 | Installation and Configuration of Linux | 25 |
| 7 | Linux Systems Administration | 29 |
| 8 | Understanding Shells and Scripting with Linux | 31 |
| 9 | Setting up Samba and a Window Linux network | 33 |
| 10 | Learn the fundamentals of wireless LAN | 36 |
| 11 | Learn the various standards related to wireless LANs | 39 |
| 12 | Learn about the security aspects of wireless LANs | 43 |

LAB 1

Designing Remote Connectivity

Aim: To design Remote connectivity using Cisco packet tracer.

Pre requisites:

- PC: Lenovo Thinkpad t480s
- RAM: 16 GB
- Tool: Cisco Packet Tracer (Version: 7.3.0.0838)
- OS: Windows 11

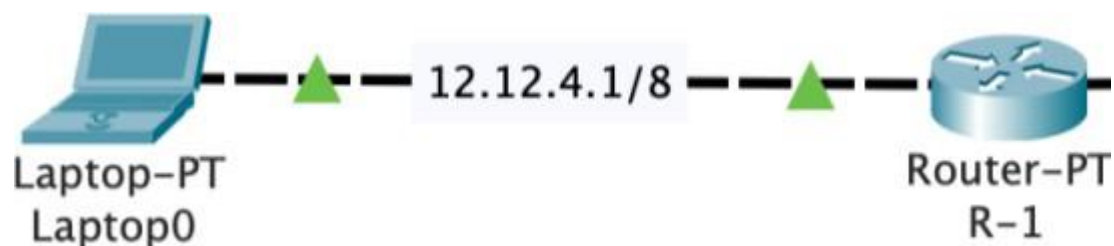
Theory:

Remote connectivity can be established using two methods:

- Telnet (Port 23): It is a network protocol that allows users to connect to remote devices over a network, primarily for command-line interface access. It transmits data in plaintext, making it insecure for sensitive data.
- SSH (Port 22): It provides a secure alternative by encrypting data during transmission, protecting credentials and commands. SSH is widely used for secure system administration and remote access in network environments.

Procedure:

TELNET



Configuring Router

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#banner login "Welcome to R1"
R1(config)#enable password 123
R1(config)#interface fastethernet0/0
R1(config-if)#ip address 12.12.4.1 255.0.0.0
R1(config-if)#no shut
```

Setting up Telnet

```
R1(config-if)#exit
R1(config)#line vty 0 15
R1(config-line)#password 123
R1(config-line)#login
R1(config-line)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#write memory
Building configuration...
[OK]
```

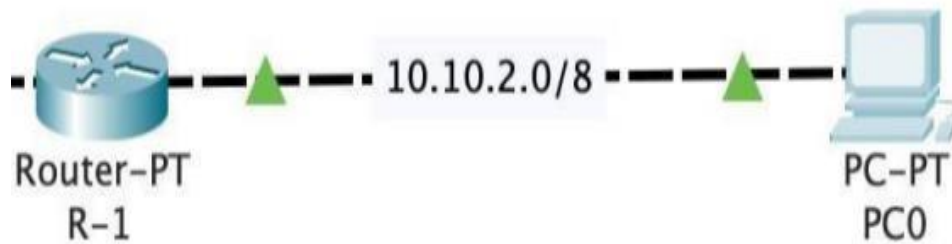
Testing Connection – Telnet

```
C:\>telnet 192.168.0.2
Trying 192.168.0.2 ...Open
Welcome to R1

User Access Verification

Password:
R1>
```

SSH



Configuring Router

```
R#configure Terminal
Enter configuration commands, one per line. End with CNTL/Z.
R(config)#int
R(config)#interface F
R(config)#interface FastEthernet 1/0
R(config-if)#ip address 10.10.2.1 255.0.0.0
R(config-if)#no shut
```

Setting up SSH

```
R(config-if)#enable password tim
R(config)#ip domain nam
R(config)#ip domain name testing
R(config)#username tim password password
R(config)#crypto key generate RSA 368
^
% Invalid input detected at '^' marker.

R(config)#crypto key generate RSA
The name for the keys will be: R.testing
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]: 362
% Generating 362 bit RSA keys, keys will be non-exportable...[OK]

R(config)#line vty 0 4
*Mar 1 0:31:8.321: RSA key size needs to be at least 768 bits for ssh version 2
*Mar 1 0:31:8.322: %SSH-5-ENABLED: SSH 1.5 has been enabled
```

Testing Connection SSH

```
C:\>ssh -l tim 10.10.2.1

Password:

R>show ?
  arp          Arp table
  cdp          CDP information
  class-map    Show QoS Class Map
  clock        Display the system clock
  controllers  Interface controllers status
  crypto       Encryption module
```

Conclusion:

Successfully designed remote connectivity by using both the methods Telnet and SSH and tested them as well.

LAB 2

Designing IP Addressing

Aim: To design IP addressing using cisco packet tracer

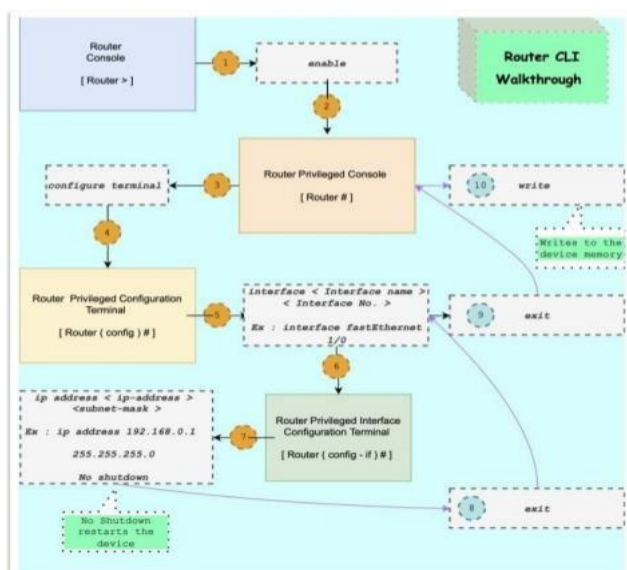
Pre requisites:

- PC: Lenovo Thinkpad t480s
- RAM: 16 GB
- Tool: Cisco Packet Tracer (Version: 7.3.0.0838)
- OS: Windows 11

Theory:

- An IP address uniquely identifies devices on a network, enabling data transfer.
- Types:
 - IPv4: 32-bit, limited addresses.
 - IPv6: 128-bit, vast address space.
- Static vs. Dynamic:
 - Static: Fixed, ideal for servers.
 - Dynamic: Changes, commonly used for consumer devices.
- IPs can reveal location and are crucial for managing network security and detecting threats.

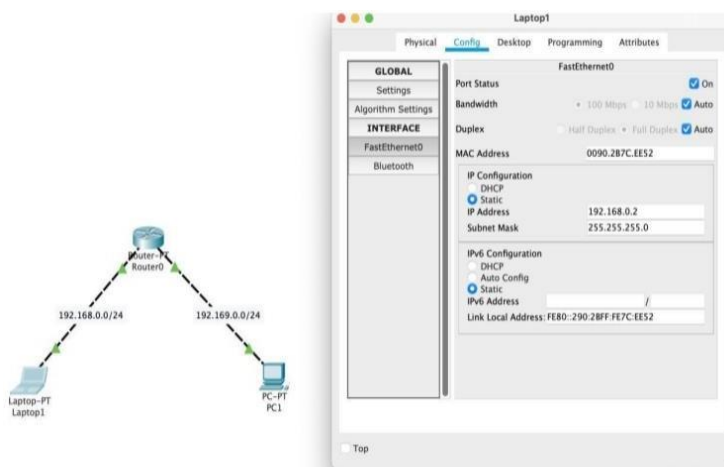
Procedure:



Router Configuration

```
Router> enable
Router# configure terminal
Router(config)# hostname R1
R1(config)# interface fastEthernet 0/0
R1(config-if)# ip address 192.168.0.1 255.255.255.0
R1(config-if)# no shut
R1(config-if)# exit
R1(config)# exit
R1# write memory
```

Do the same for Interface 1/0



Statically assigning IP Address to Laptop 1

Now go to global – Settings and set gateway as ‘Router Interface IP’

Do the same for PC1

Verifying the connection: Click on PC or Laptop – Desktop – Command Prompt

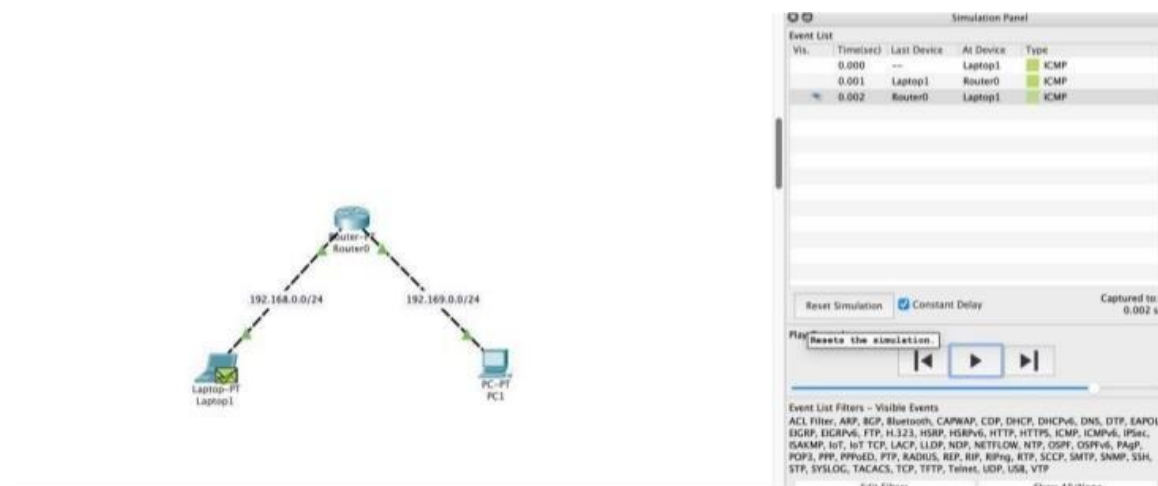
```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

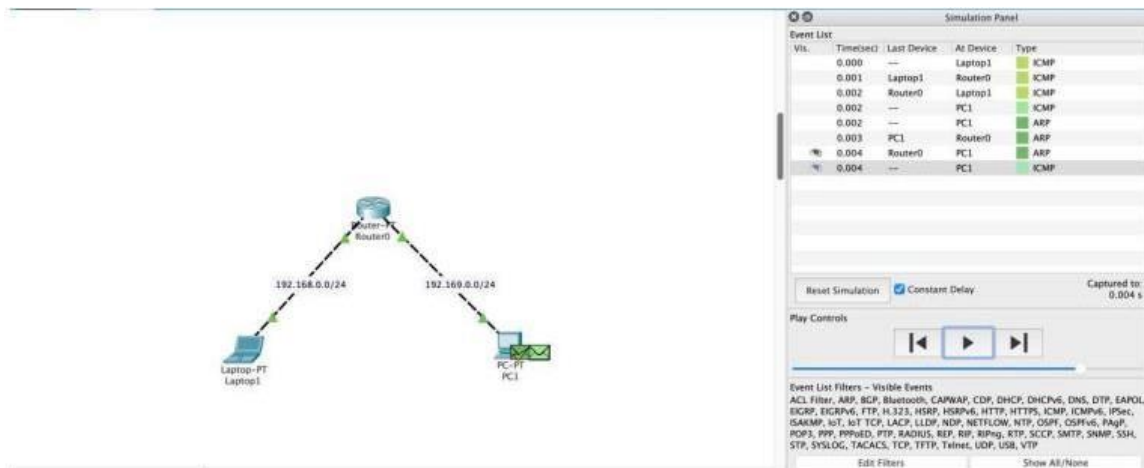
Reply from 192.168.0.1: bytes=32 time=1ms TTL=255
Reply from 192.168.0.1: bytes=32 time=3ms TTL=255
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0%
    loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 1ms
```

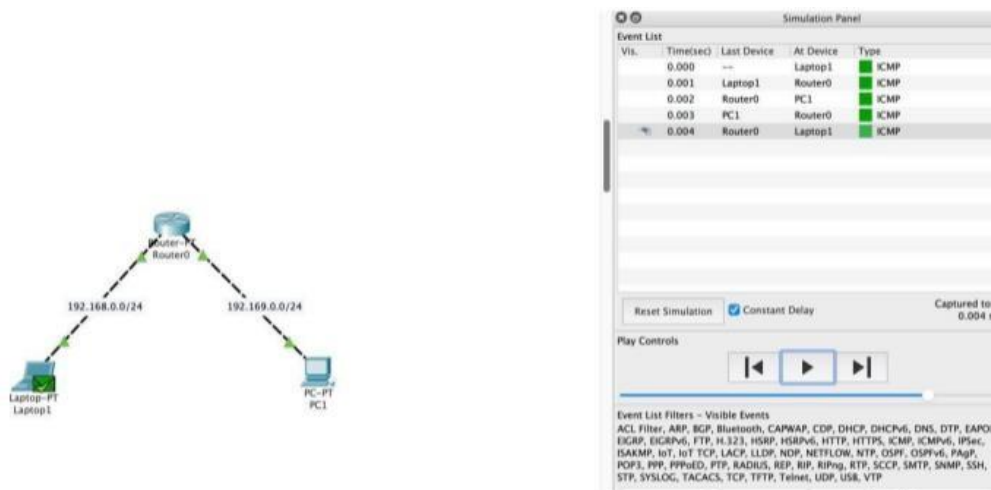
Simulating using ICMP Packets as Simple PDU



(Laptop 1 → Router 0)



(PC1 → Router 0)



(Laptop1 → PC1)

Conclusion:

Successfully Designed and Tested the Assigned IP addresses.

LAB 3

Selecting Routing Protocols

Aim: Selecting the Routing Protocol by using Cisco Packet tracer.

Pre requisites:

- PC: Lenovo Thinkpad t480s
- RAM: 16 GB
- Tool: Cisco Packet Tracer (Version: 7.3.0.0838)
- OS: Windows 11

Theory:

- Static routing involves manually setting routes in a network.
- Fixed Paths: Routes don't change unless manually updated.
- Simple and Secure: No automatic updates; reduces risk of errors.
- Low Overhead: Saves bandwidth since it doesn't use routing protocols.
- Best for Small Networks: Difficult to manage in large networks.

Procedure:



Layout

Router Configuration

```
Router> enable
Router# configure terminal
Router(config)# hostname R1
R1(config)# interface fastEthernet 0/0
R1(config-if)# ip address 192.168.0.1 255.255.255.0
R1(config-if)# no shut
R1(config-if)# exit
R1(config)# interface serial 2/0
R1(config-if)# ip address 10.10.0.1 255.0.0.0
R1(config-if)# no shut
R1(config)# exit
R1# write memory
```

Do the same for Router 1

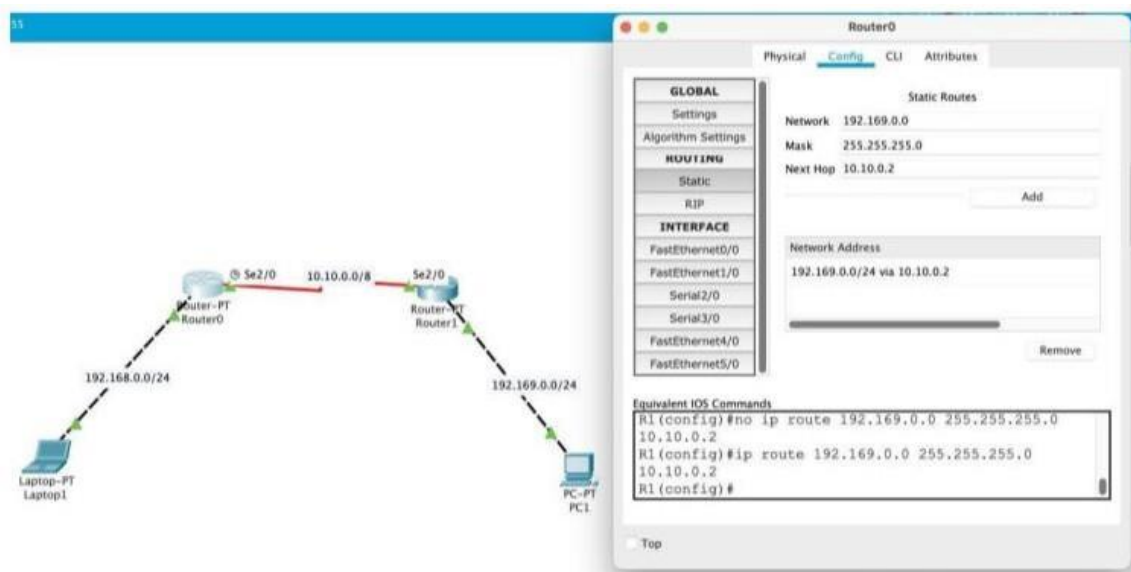
Assigning static Ips to the PC and Laptop

Method 1 – Using CLI

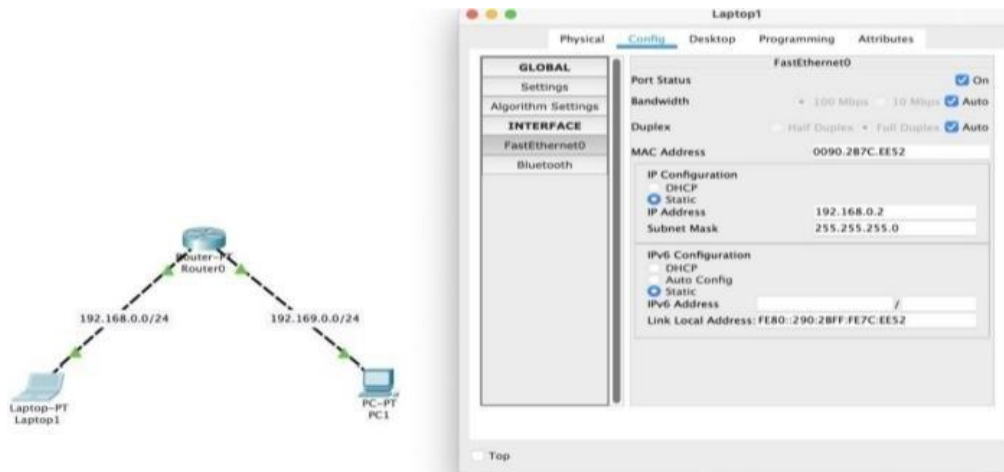
```
R1(config)#ip route 192.169.0.0 255.255.255.0 10.10.0.2
R1(config)# exit
R1#write
```

```
Router(config)#ip route 192.168.0.0 255.255.255.0 10.10.0.1
Router(config)# exit
Router#write
```

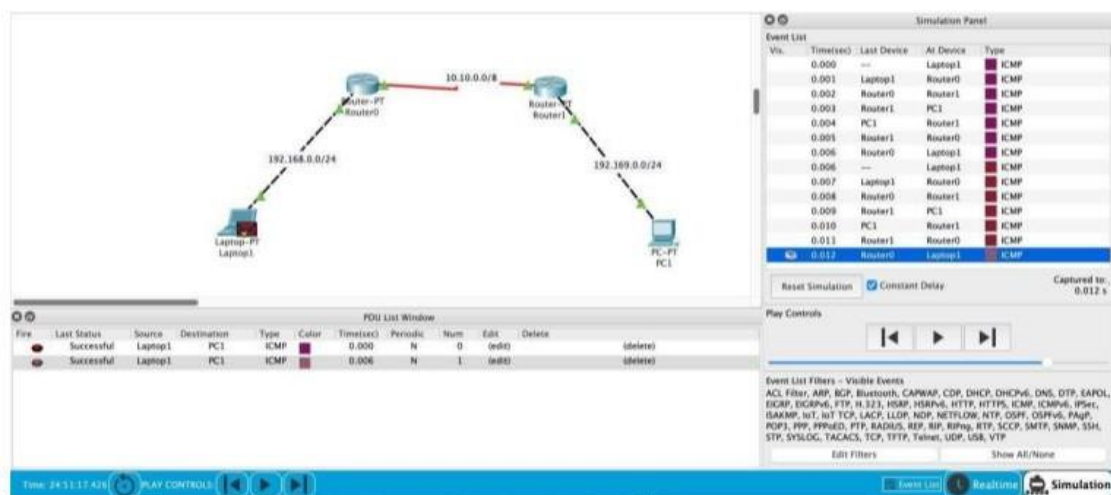
Method 2 – Using Config Tab



Click on router → Config Tab → Routing > Static → Write Route



Simulating using ICMP Packets as Simple PDU (Laptop → PC1)



Conclusion

Successfully designed selected routing protocol-Static Routing and simulated as well.

LAB 4

Wireless Network Design

Aim: To design wireless network by using Cisco Packet Tracer.

Pre requisites:

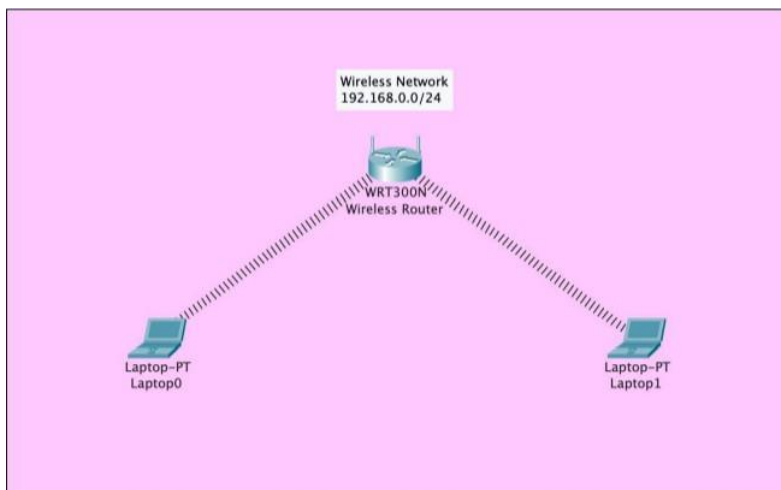
- PC: Lenovo Thinkpad t480s
- RAM: 16 GB
- Tool: Cisco Packet Tracer (Version: 7.3.0.0838)
- OS: Windows 11

Theory:

Wi-fi

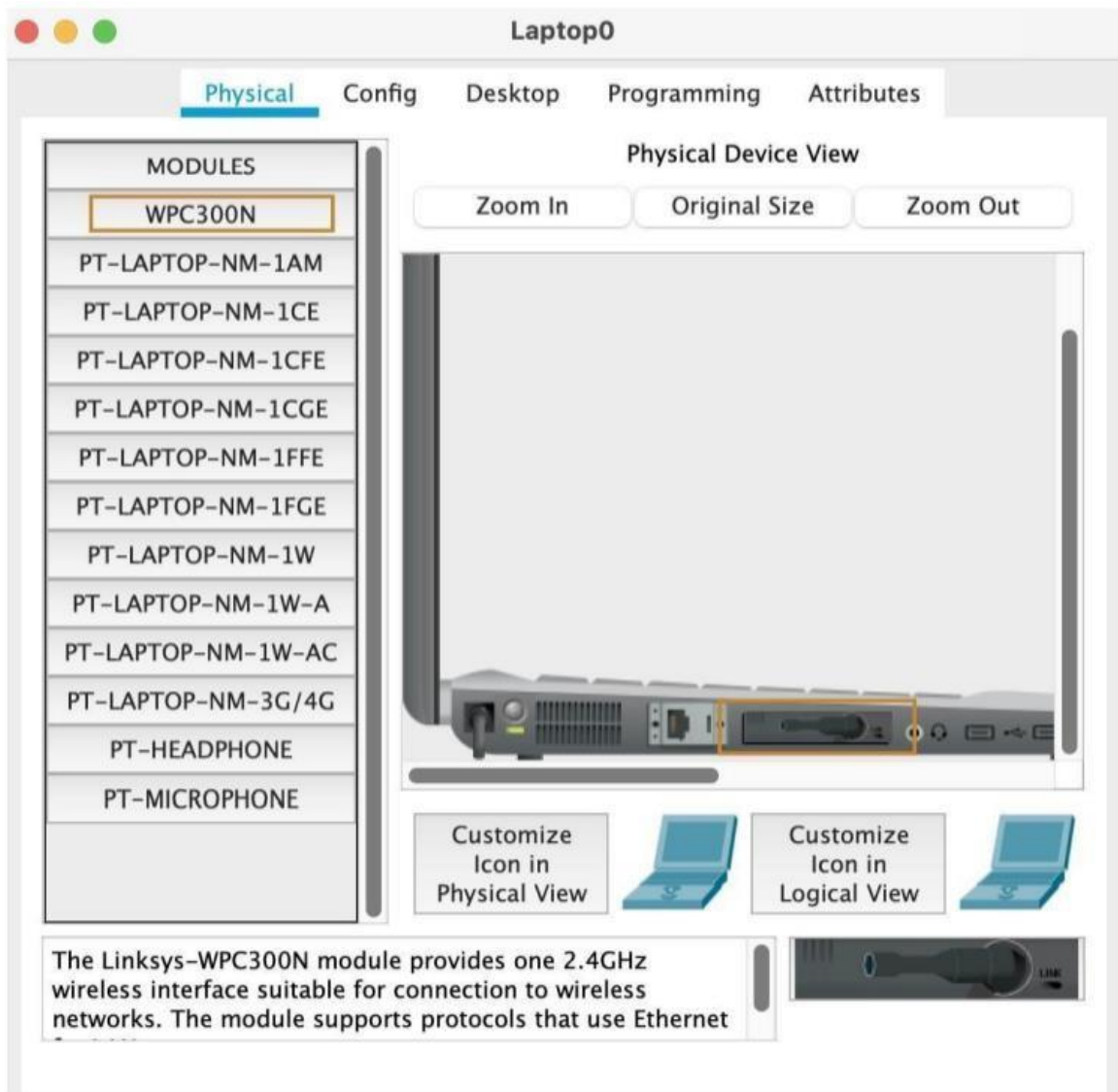
- **Wireless Connection:** Connects devices without cables.
- **Uses Radio Signals:** Transmits data through the air.
- **Local Range:** Usually covers homes or small businesses.
- **Needs Router:** Requires a router to create the network.

Procedure:



Layout

Click on the Device → Physical → Turn off the power button → drag and drop the “WPC300N” or “WMP300N” Module. → Click on Power button.



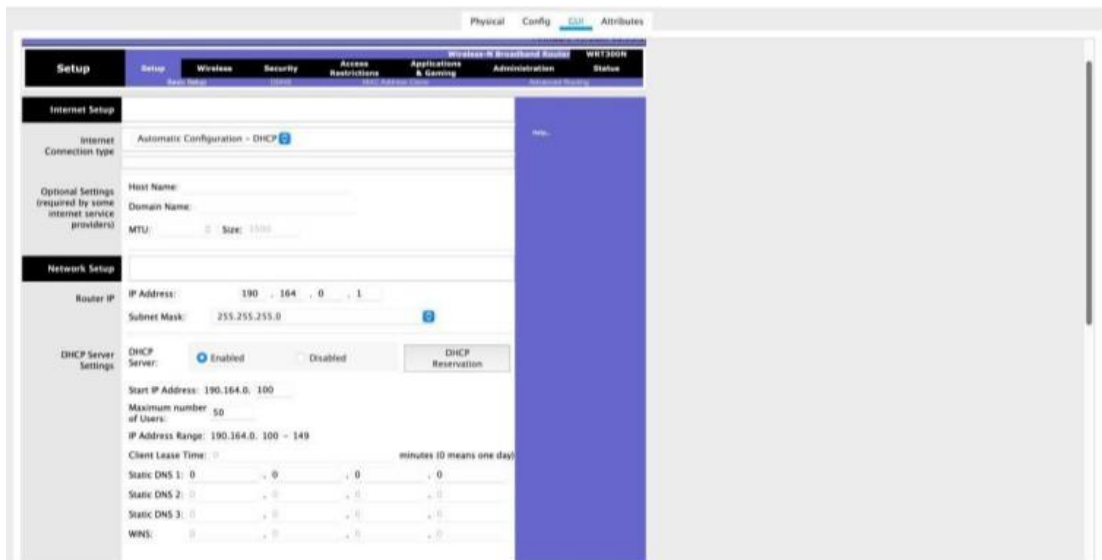
Check End Nodes

Now Configure the Router

Click on WRT300N Router → Config Tab → Interfaces > LAN → Set IP Address



Setting -Up the IP using Config Tab



GUI Tab

One can also setup Wi-Fi using “GUI tab” by setting Router IP and Selecting the Mask.

Also set the DHCP server:

Select “Enabled”

Set Range of IP Address that should be assigned (“IP Address Range”)


Maximum No. of Users

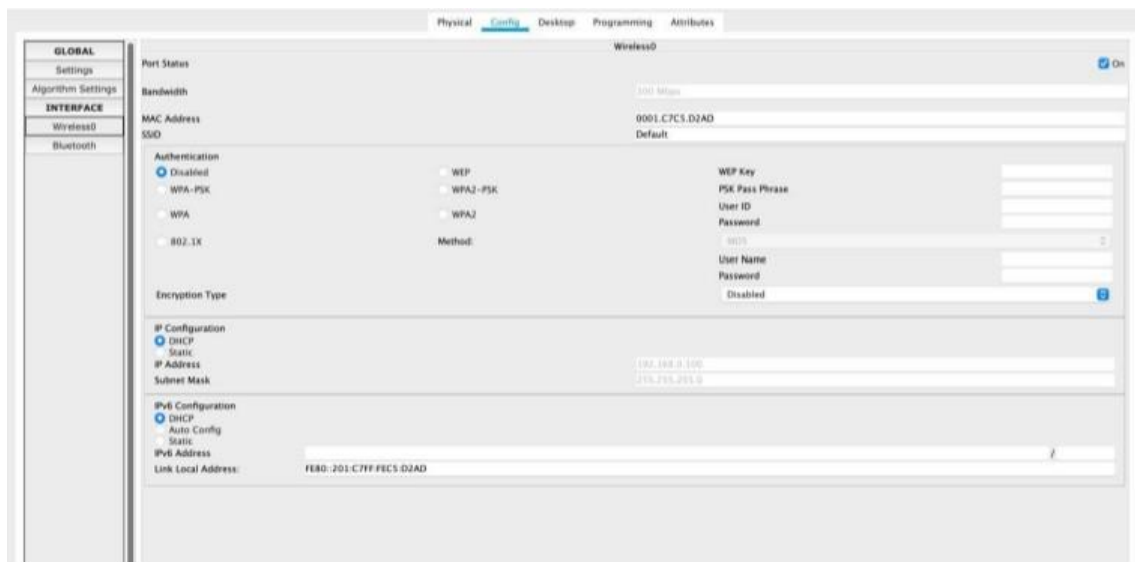
One Can even manually add Clients using “DHCP Reservation” → Add Client



Statically adding users to the network

In the End Nodes / Devices

 Click on the End Device → Config tab → Wireless 0

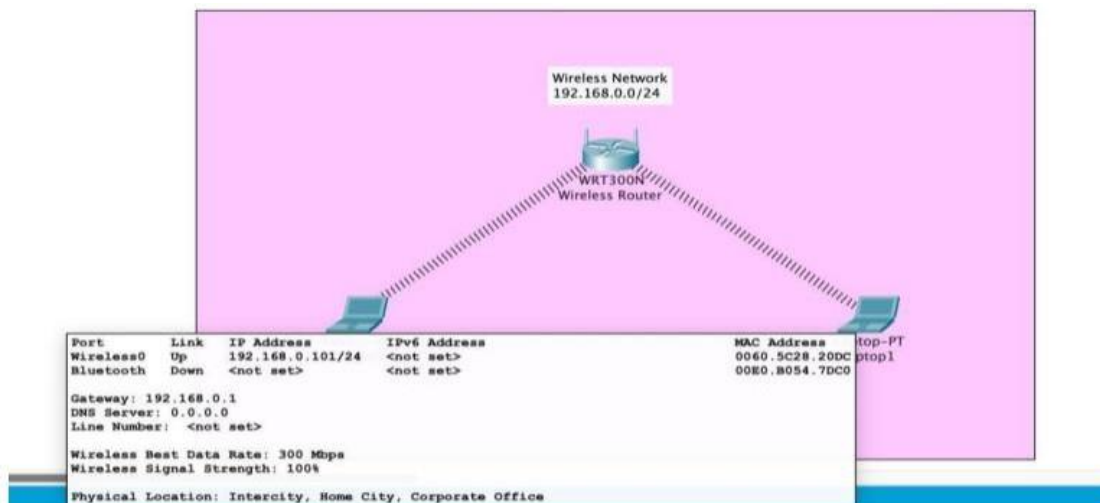


Setting Up Wireless Network

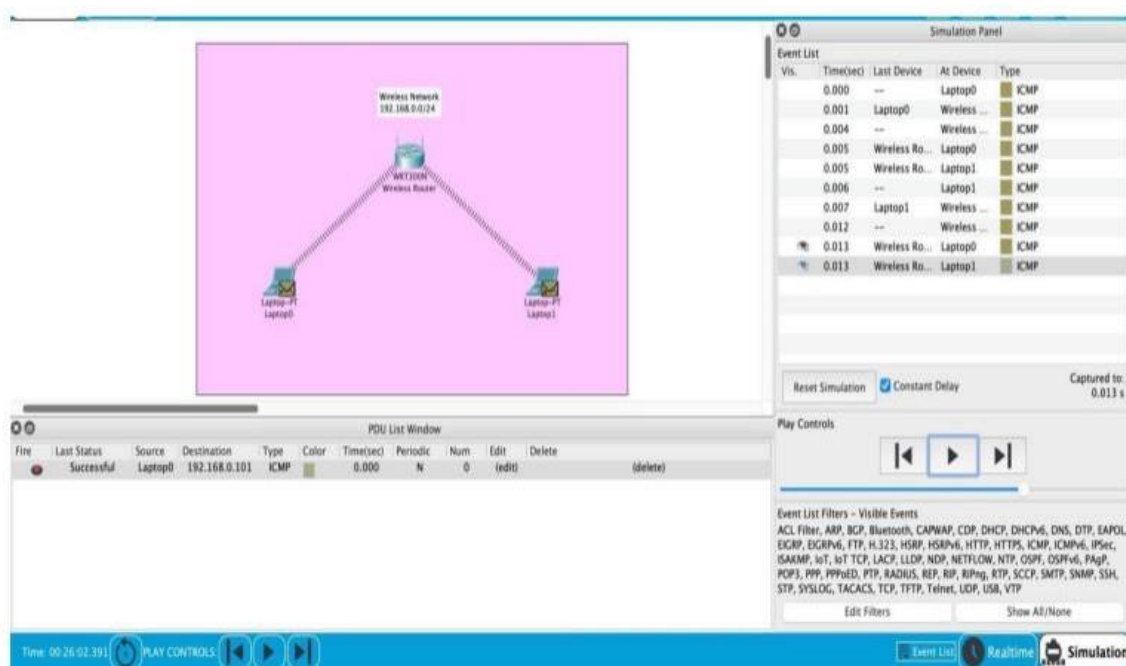
Set IP Configuration to DHCP

Now if you hover over the device, you can see IP address has been Assigned.

To verify it check the WRT300N's "DHCP Reservations".



Simulation



Simulating WiFi network using ICMP packet { Simple PDU }

Conclusion

Successfully designed, implemented and simulated Wireless network (Wi-fi) by using Cisco Packet tracer.

LAB 5

Designing Security Solution

Aim: To design Security Solution using Cisco Packet tracer.

Pre requisites:

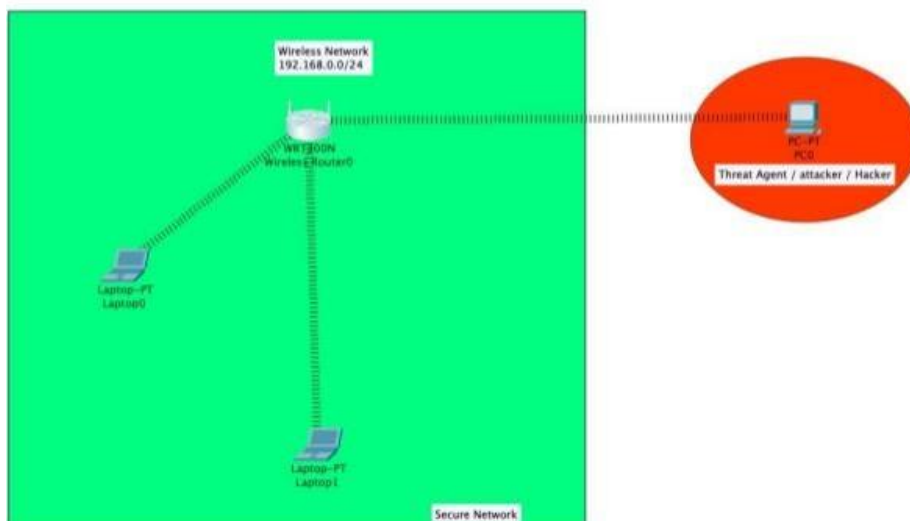
- PC: Lenovo Thinkpad t480s
- RAM: 16 GB
- Tool: Cisco Packet Tracer (Version: 7.3.0.0838)
- OS: Windows 11

Theory:

MAC Filtering

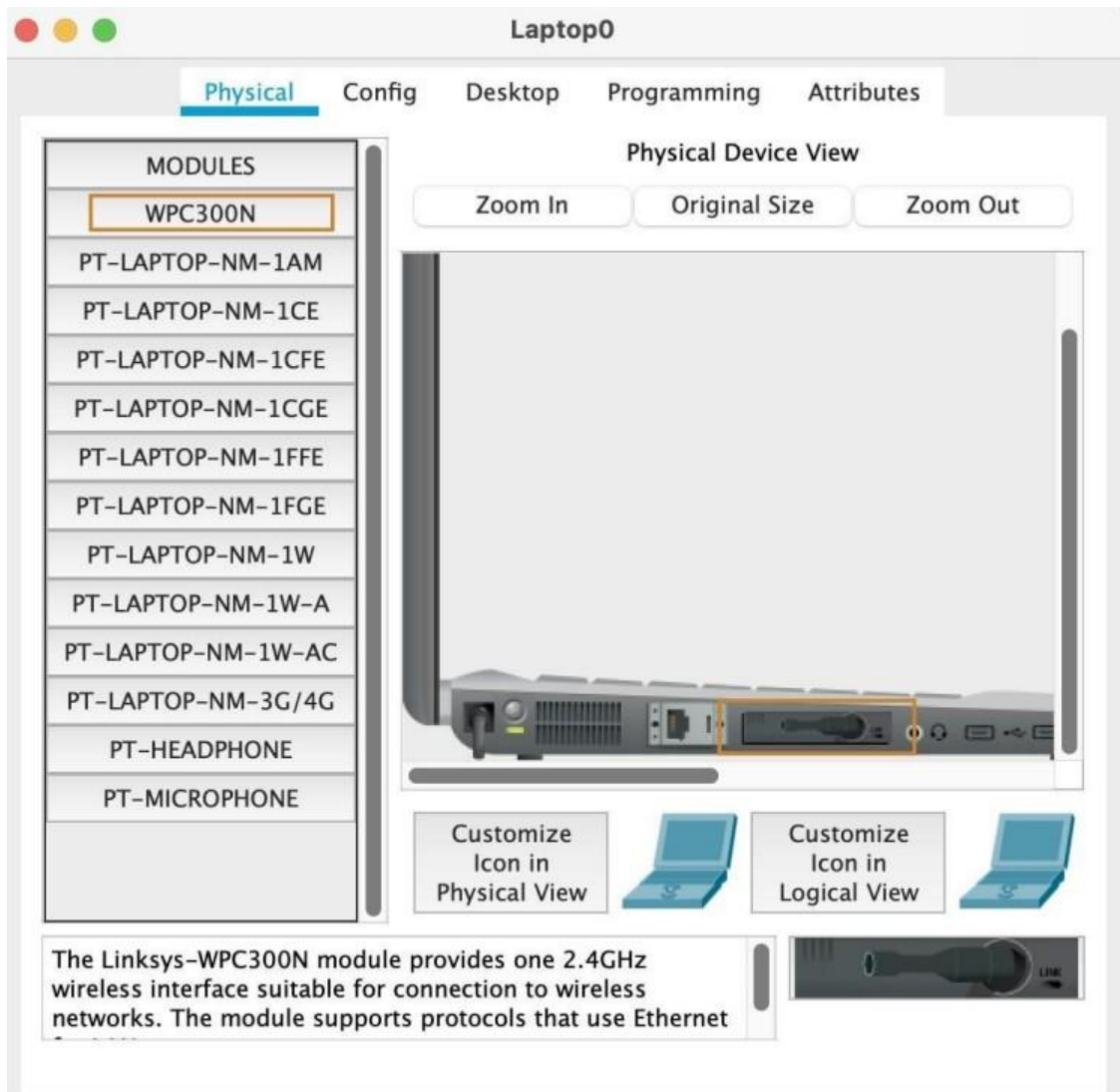
- Device Control: Allows or blocks devices based on their MAC address.
- Network Security: Helps secure networks by limiting access.
- Manual Setup: Requires adding MAC addresses to a list.
- Not Fully Secure: Can be bypassed by changing MAC addresses.

Procedure:



Layout

Click on the Device → Physical → Turn off the power button → drag and drop the “WPC300N” or “WMP300N” Module. → Click on Power button.



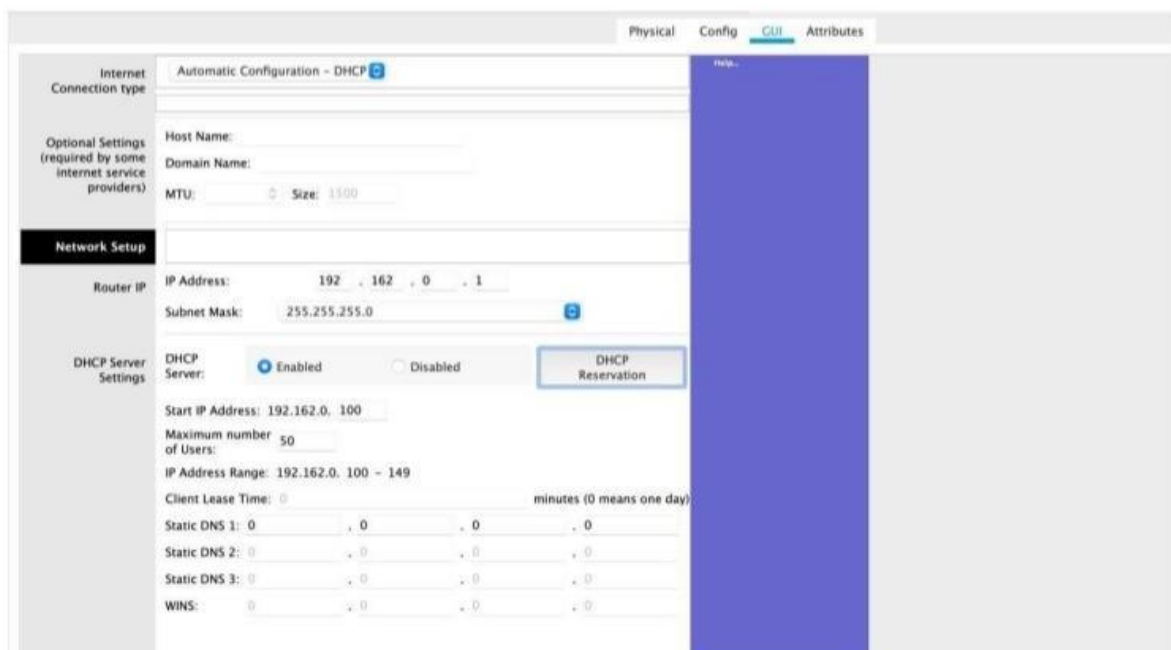
Check End Nodes

Now Configure the Router

Click on WRT300N Router → Config Tab → Interfaces > LAN → Set IP Address



Setting -Up the IP using Config Tab



GUI Tab

One can also setup Wi-Fi using “GUI tab “by setting Router IP and Selecting the

Mask.

Also set the DHCP server:

Select “Enabled”

Set Range of IP Address that should be assigned (“IP Address Range”)

Maximum No. of Users

One Can even manually add Clients using “DHCP Reservation” → Add Client

Bridge 10
Broadcast Power
Firmware Version: v0.91.0

DHCP Reservation

Select Clients from DHCP Tables

| Client Name | Interface | IP Address | MAC Address | Select |
|-------------|-----------|---------------|-------------------|--------------------------|
| | LAN | 192.168.0.100 | 00:01:C7:C5:D2:AD | <input type="checkbox"/> |
| | LAN | 192.168.0.101 | 00:60:5C:28:20:DC | <input type="checkbox"/> |
| | LAN | 192.168.0.102 | 00:60:2F:07:21:89 | <input type="checkbox"/> |

Add Client

Manually Adding Client

| 1 | 2 | 3 | 4 |
|-------------|-------------------|---|-----|
| 192.162.0.0 | 00:00:00:00:00:00 | | Add |

Statically adding users to the network

Click on the End Device → Config tab → Wireless 0

GLOBAL

Settings

Algorithm Settings

INTERFACE

Wireless0

Bluetooth

Physical

Config

Desktop

Programming

Attributes

Wireless0

On

Port Status

Bandwidth

MAC Address

SSID

Authentication

Encryption Type

IP Configuration

IPv6 Configuration

100 Mbps

0001.C7C5.D2AD

Default

Disabled

WPA-PSK

WPA

802.1X

WEP

WPA2-PSK

WPA2

Method:

WEP Key

PSK Pass Phrase

User ID

Password

WEP

User Name

Password

Disabled

Static

IP Address

Subnet Mask

192.168.0.100

255.255.255.0

Dynamic

Static

Auto Config

Static

IPv6 Address

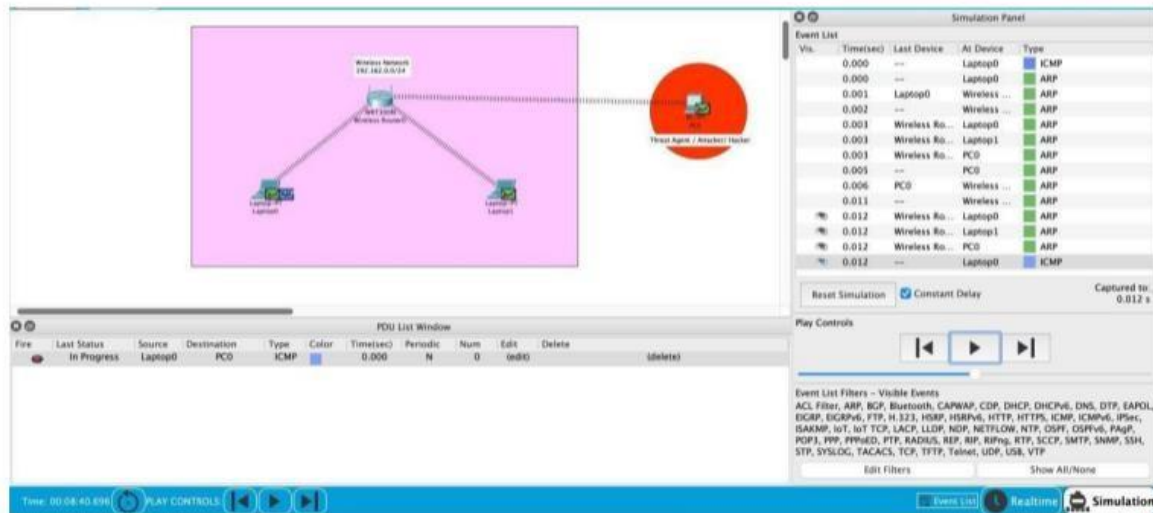
Link Local Address:

FE80::201:C7FF:FE05:D2AD

Setting Up Wireless Network

Set IP Configuration to DHCP

Now if you hover over the device, you can see IP address has been Assigned. To verify it check the WRT300N's "DHCP Reservations".

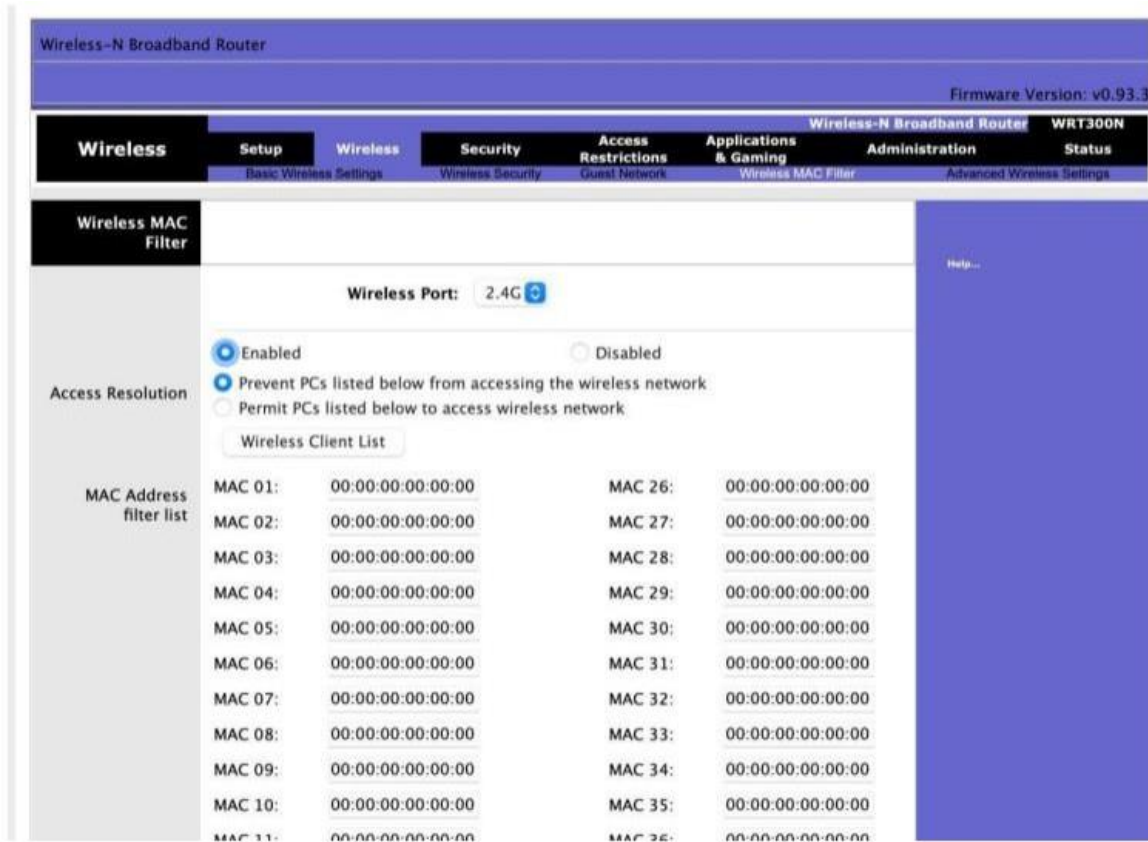


Testing Connectivity between devices by simulating

Adding Security

In the Wireless Router,

Go to GUI → Wireless → Wireless MAC Filter



Select Enable Option → Select 1st Option (Implicit Allow All except)

Wireless MAC Filter

Wireless Port: 2.4G

☒ Enabled
☐ Disabled

☒ Prevent PCs listed below from accessing the wireless network
☐ Permit PCs listed below to access wireless network

Wireless Client List

| | | | |
|---------|-------------------|---------|-------------------|
| MAC 01: | 00:50:0F:52:64:95 | MAC 26: | 00:00:00:00:00:00 |
| MAC 02: | 00:00:00:00:00:00 | MAC 27: | 00:00:00:00:00:00 |
| MAC 03: | 00:00:00:00:00:00 | MAC 28: | 00:00:00:00:00:00 |
| MAC 04: | 00:00:00:00:00:00 | MAC 29: | 00:00:00:00:00:00 |

Access Resolution

MAC Address filter list

Now Add the MAC Address. Save It.

The screenshot shows a network simulation environment. On the left, a diagram illustrates a wireless network with a central 'Wireless Router' connected to two 'Laptop PT' devices. A red circle labeled 'No Connection' is shown between the router and a 'Host Agent / Antenna Model'. The right side of the interface features a 'Simulation Panel' with an 'Event List' table. The table has columns for 'Vis.', 'Time(sec)', 'Last Device', 'AI Device', and 'Type'. The 'Event List' shows several entries for 'DTP' (Data Transfer Protocol) events occurring at various times (e.g., 10.747, 10.748, 40.748, 40.749, 70.751, 70.752, 100.752). Below the event list, there are 'Play Controls' (Reset Simulation, Constant Delay, Captured to: 100.752 s) and a list of 'Event List Filters - Visible Events' including ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPsec, ISAKMP, IoT, IoT TCP, LACP, LLDP, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgg, POP3, PPP, PPPoE, PTP, RADIUS, REP, RFP, RIPv2, RTP, SCCP, SHTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP.

Simulating Network Post Changes. {Filtering is Working}

Conclusion

Hence, we simulated one security mechanism.

LAB 6

Installation and Configuration of Linux

Aim: To Install Debian OS (Ubuntu) on a Virtual Machine (VMware)

Pre-requisites:

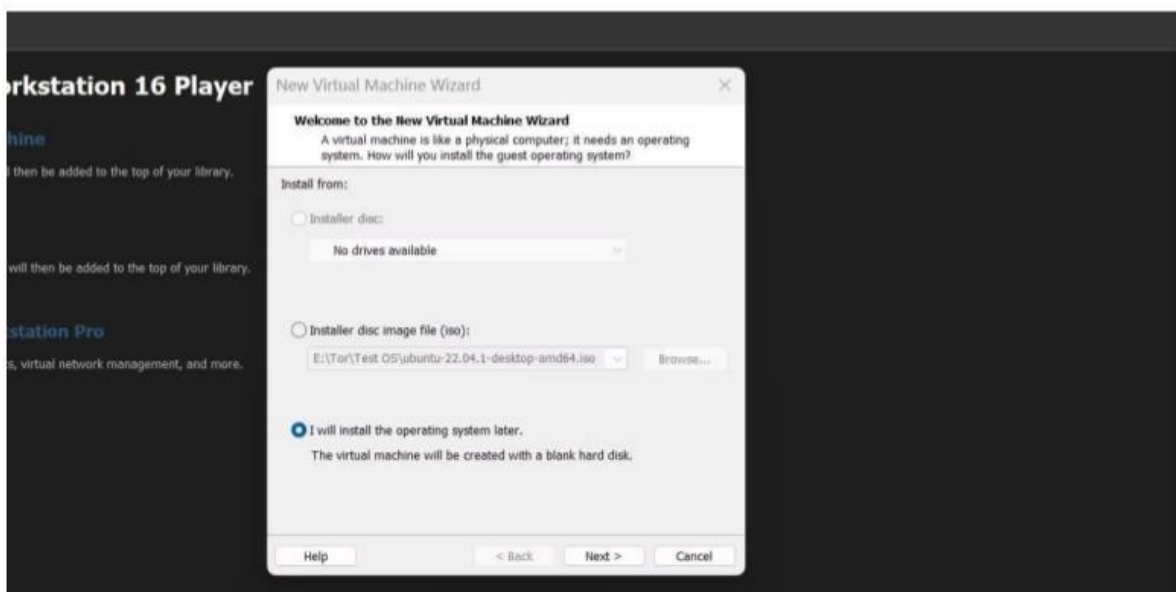
- Hardware
- Processor: i5 10300H
- Host OS (Windows)
- RAM: (Min) 4GB RAM
- ROM: (Min) 25 GB Software
- VMware
- Ubuntu iso (ARM)

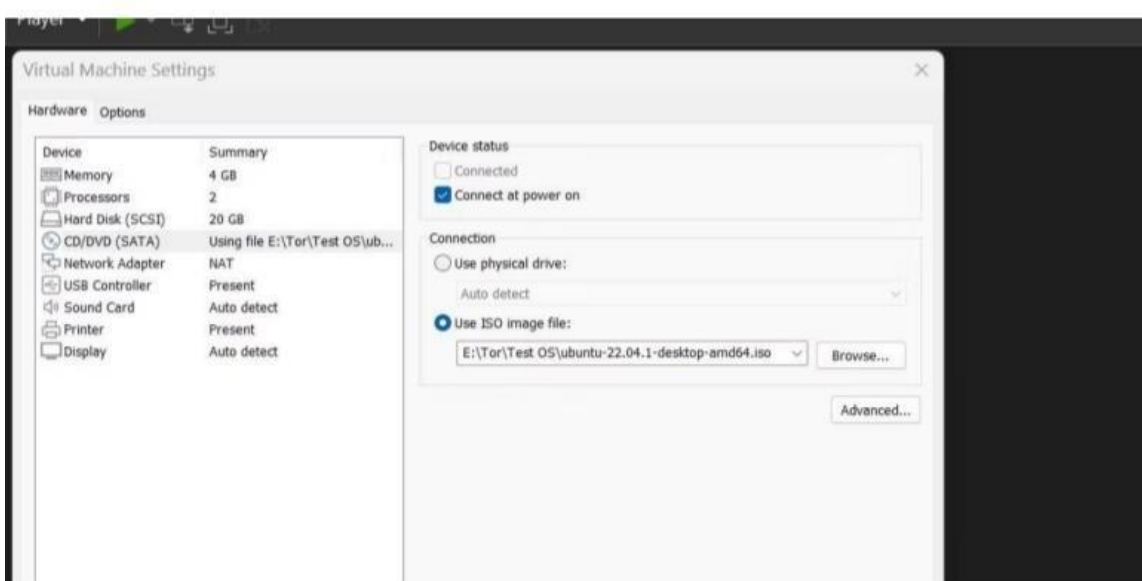
Theory:

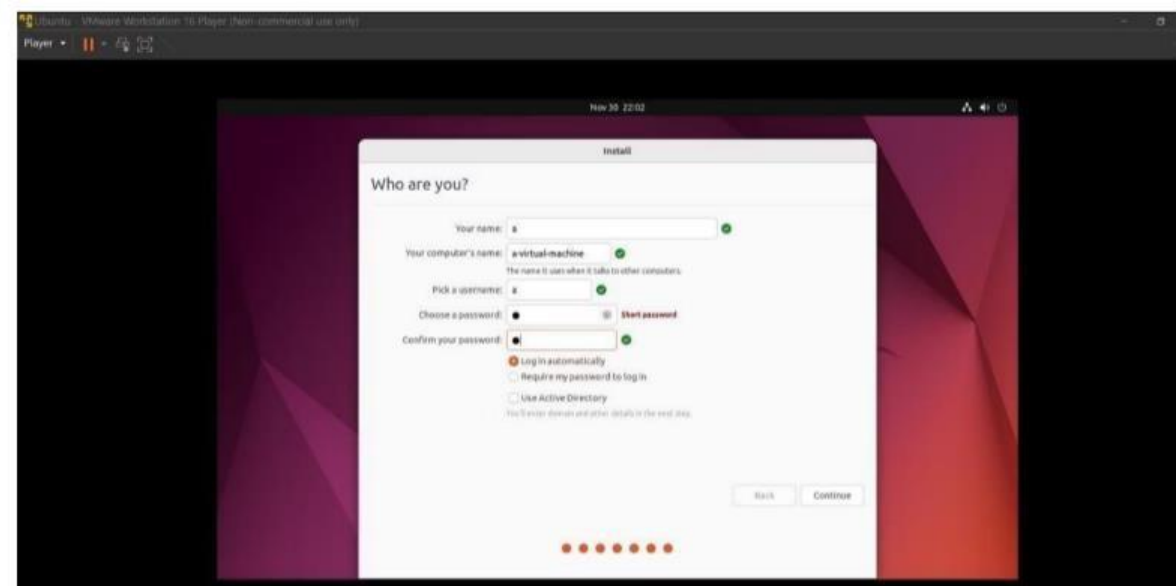
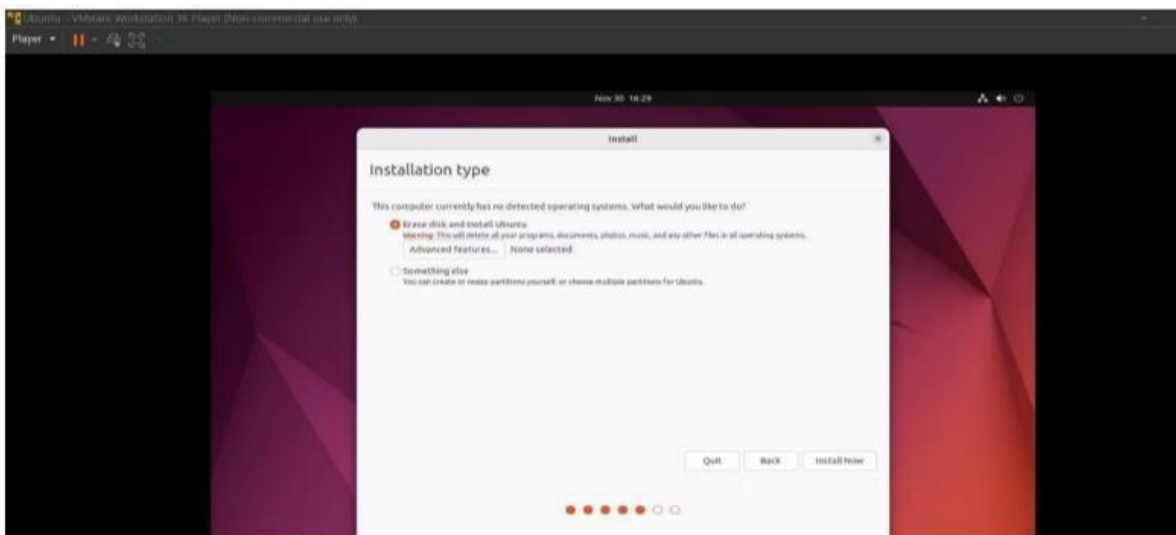
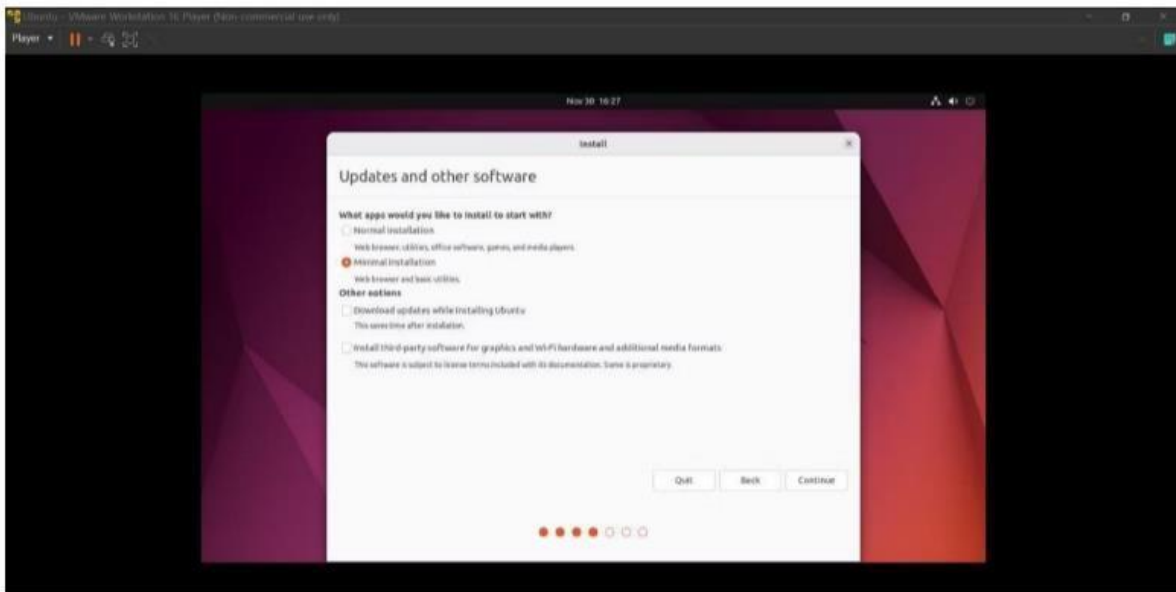
Linux Operating System

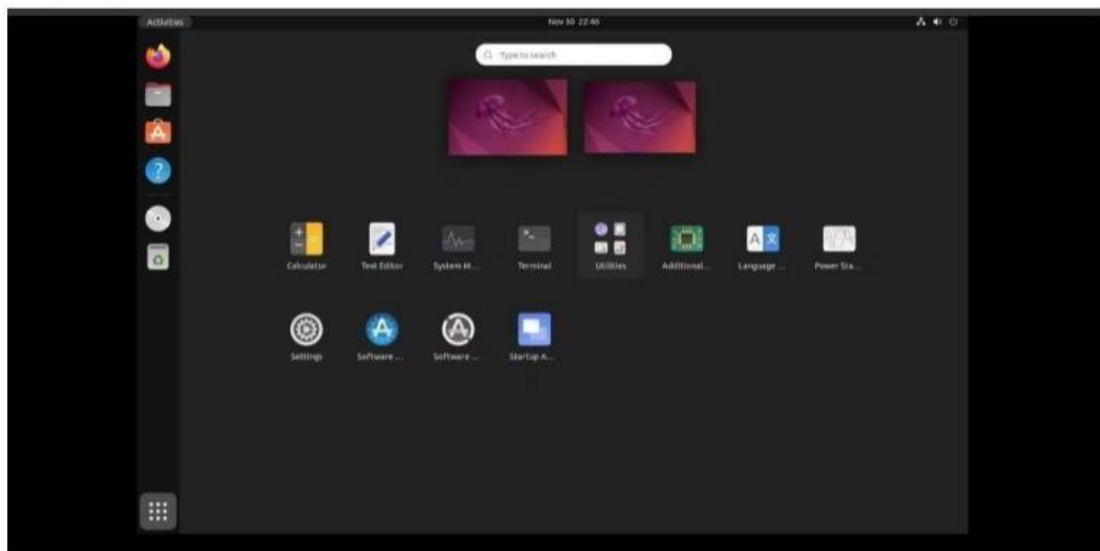
- Open-Source: Free to use and modify.
- Multi-User: Supports multiple users at once.
- Secure: Known for strong security features.
- Command-Line and GUI: Offers both text-based and graphical interfaces.

Procedure:









Conclusion:

We have successfully downloaded and configured Ubuntu on a Virtual Machine.

LAB 7

Linux System Administration

Aim: To use the basic Linux system administration commands.

Pre-requisites:

- Hardware
- Processor: i5 10300h
- Host OS (Windows)
- RAM: (Min) 4GB RAM
- ROM: (Min) 25 GB Software
- VMware
- Ubuntu iso (ARM)

Theory:

- System Configuration & Upkeep: Manages setup and ongoing maintenance of computer systems.
- Server Management: Handles servers, ensuring they run reliably and efficiently.
- System Performance & Security: Monitors and optimizes performance while ensuring security.
- Budget Management: Balances costs while meeting the needs of users and maintaining systems.
- Terminal Interface: Primarily works through the terminal, requiring mastery of commands for efficient operation and troubleshooting.

Procedure:

```
# > Listing
ls
# -a : Hidden Files ( start with '.' )
ls -a
# -l : Long Listing ( Information like, Date of creation, Size , Owner, permissions etc )
ls -l

# > Change Directory
cd

# > Present Working Directory
pwd

# > Creating Directory
mkdir < Directory Name >

# > Concatination of Contents
cat < File Name >

# > Creating File ( If it doesn't exist )/ Editing Time Stamp ( If it Exists )
touch < File Name >

# > Deleting File
rm < File Name >

# -r : delete directory
rm -r < Directory Name >
```

```

root@65b58ef0c819:/# ls
bin boot dev etc home lib media mnt opt proc root run sbin srv sys tmp usr var
root@65b58ef0c819:/# ls -la
. . . dockerenv bin boot dev etc home lib media mnt opt proc root run sbin srv sys tmp usr var
root@65b58ef0c819:/# ls -l
total 48
lrwxrwxrwx 1 root root 7 Aug 15 11:54 bin -> usr/bin
drwxr-xr-x 2 root root 4096 Apr 18 2022 boot
drwxr-xr-x 5 root root 360 Dec 21 00:03 dev
drwxr-xr-x 1 root root 4096 Dec 21 00:03 etc
drwxr-xr-x 2 root root 4096 Apr 18 2022 home
lrwxrwxrwx 1 root root 7 Aug 15 11:54 lib -> usr/lib
drwxr-xr-x 2 root root 4096 Aug 15 11:54 media
drwxr-xr-x 2 root root 4096 Aug 15 11:54 mnt
drwxr-xr-x 2 root root 4096 Aug 15 11:54 opt
dr-xr-xr-x 188 root root 0 Dec 21 00:03 proc
drwx----- 2 root root 4096 Aug 15 12:13 root
drwxr-xr-x 5 root root 4096 Aug 15 12:13 run
lrwxrwxrwx 1 root root 8 Aug 15 11:54 sbin -> usr/sbin
drwxr-xr-x 2 root root 4096 Aug 15 11:54 srv
dr-xr-xr-x 13 root root 0 Dec 21 00:03 sys
drwxrwxrwt 2 root root 4096 Aug 15 12:13 tmp
drwxr-xr-x 11 root root 4096 Aug 15 11:54 usr
drwxr-xr-x 11 root root 4096 Aug 15 12:13 var

```

> Listing (ls)

```

root@65b58ef0c819:/# cd /tmp
root@65b58ef0c819:/tmp# pwd
/tmp
root@65b58ef0c819:/tmp# mkdir test
root@65b58ef0c819:/tmp# ls
test

```

Changing Directory (cd), Viewing Present working Directory (pwd) & Creating Directory (mkdir)

```

root@65b58ef0c819:/tmp# cat test.txt
hello world
root@65b58ef0c819:/tmp# touch test
root@65b58ef0c819:/tmp# ls -l
total 8
-rw-r--r-- 1 root root 0 Dec 21 00:08 hi.txt
drwxr-xr-x 2 root root 4096 Dec 21 00:08 test
-rw-r--r-- 1 root root 12 Dec 21 00:07 test.txt
root@65b58ef0c819:/tmp# touch test.txt
root@65b58ef0c819:/tmp# ls -l
total 8
-rw-r--r-- 1 root root 0 Dec 21 00:08 hi.txt
drwxr-xr-x 2 root root 4096 Dec 21 00:08 test
-rw-r--r-- 1 root root 12 Dec 21 00:09 test.txt

```

> Concatenation of Strings (cat), Creating File (touch) & Modifying timestamp (touch)

```

root@65b58ef0c819:/tmp# ls
hi.txt test test.txt
root@65b58ef0c819:/tmp# rm hi.txt
root@65b58ef0c819:/tmp# ls
test test.txt
root@65b58ef0c819:/tmp# rm -r test
root@65b58ef0c819:/tmp# ls
test.txt

```

> Removing Files (rm) and Folders (rm -r)

Conclusion:

We have Successfully completed using the basic Linux administration commands.

LAB 8

Understanding Shells and Scripting with Linux

Aim: To understand the basics of the Linux shells and shell scripting.

Pre-Requisites:

- A Linux-based system (e.g., Ubuntu, CentOS, or a virtual machine).
- Basic familiarity with the terminal.
- A text editor for writing scripts (such as nano, vim, or gedit).

Theory:

What is a Shell?

A shell is a command-line interpreter that provides a user interface for the operating system. It allows users to execute commands, run programs, and perform various tasks.

Common shells in Linux include:

- Bash (Bourne Again Shell) - Default for many Linux distributions.
- Zsh (Z Shell) - Known for features like theme customization and plugins.
- Ksh (Korn Shell) - Popular in some Unix systems.

Shells execute commands and control input/output in Linux. Each shell can run scripts to automate tasks.

What is Shell Scripting?

Shell scripting involves writing a sequence of commands in a file, called a script, to perform repetitive tasks.

Shell scripts typically have .sh extensions but can be executed without it.

Shell scripting is useful for:

Task automation (backups, system updates).

System administration (managing users, files, processes).

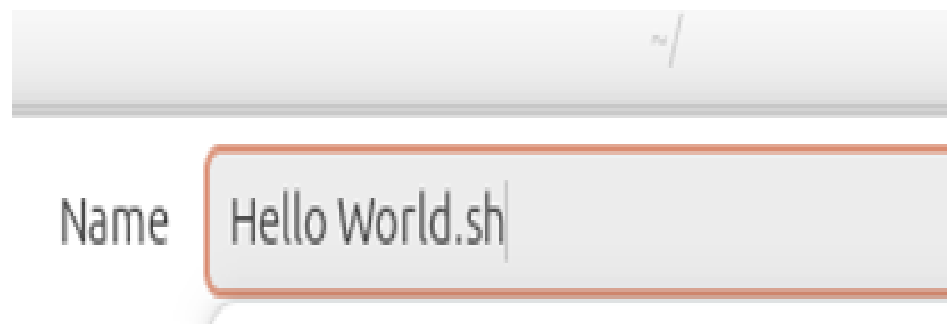
Customizing user environments.

Procedure:

Write the script in the text editor as shown in the below


```
#!/bin/bash  
echo "Hello World"
```

Save this file as any file name with extension with .sh (example: Hello world.sh)

A screenshot of a file manager interface. At the top, there is a breadcrumb path showing '~/'. Below it, there is a search bar. Under the search bar, the text 'Name' is followed by a text input field containing 'Hello World.sh'.

Set the script executable permission by running chmod command as shown below:

```
(root@kali)-[/home/kali]  
# chmod 777 helloworld.sh
```

Run or execute the file with the following syntax:

```
(root@kali)-[/home/kali]  
# ./helloworld.sh  
Hello World
```

Conclusion:

We have understood the basics of the shells and shell scripting. We also got to know about how to write, save, set permissions and execute the shell script.

LAB 9

Setting up Samba in Linux Network

Aim: To set up the Samba Server in Linux Network

Pre-requisites:

- Hardware
- Processor: i5 10300h
- Host OS (Windows)
- RAM: (Min) 4GB RAM
- ROM: (Min) 25 GB Software
- VMware
- Ubuntu iso (ARM)

Theory:

- Windows Interoperability: Samba enables Linux and Unix systems to work seamlessly with Windows systems.
- File and Print Services: Provides secure, stable, and fast file and print services using the SMB/CIFS protocol.
- Cross-Platform Compatibility: Supports various clients, including DOS, Windows, OS/2, and Linux.
- Active Directory Integration: Allows Linux/Unix systems to integrate into Active Directory environments as domain controllers or domain members.
- Flexibility: Offers network administrators flexibility in setup, configuration, and equipment choices.

Procedure:

Install Samba

```
# Update Libraries and Upgrade System
sudo apt update && sudo apt upgrade -y

# Install Samba
sudo apt install samba

# Reboot
reboot
```

```
thenc@th3nc:~$ sudo apt install samba
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libflashrom1 libftdi1-2
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  attr ibverbs-providers libavahi-client3 libavahi-common-data libavahi-common3 libboost-iostreams1.74.0 libboost-thread1.74.0 libcephfs2 libcupst2 libgfrp10
  libgfrpc0 libgfsxdr0 libglusterfs0 libibverbs1 libldb2 libnl-route-3-200 librados2 librdmacm1 libtalloc2 libtdb1 libtevent0 liburing2 libwbclient0
  python3-dnspython python3-gpg python3-ldb python3-markdown python3-pygments python3-requests-toolbelt python3-samba python3-talloc python3-tdb samba-common
  samba-common-bin samba-dsdb-modules samba-libs samba-vfs-modules tdb-tools
Suggested packages:
  cups-common python3-sniffio python3-trio python-markdown-doc python-pygments-doc ttf-bitstream-vera bind9 bind9utils ctdb ldb-tools ntp | chrony
  smbldap-tools winbind heimdal-clients
The following NEW packages will be installed:
  attr ibverbs-providers libavahi-client3 libavahi-common-data libavahi-common3 libboost-iostreams1.74.0 libboost-thread1.74.0 libcephfs2 libcupst2 libgfrp10
  libgfrpc0 libgfsxdr0 libglusterfs0 libibverbs1 libldb2 libnl-route-3-200 librados2 librdmacm1 libtalloc2 libtdb1 libtevent0 liburing2 libwbclient0
  python3-dnspython python3-gpg python3-ldb python3-markdown python3-pygments python3-requests-toolbelt python3-samba python3-talloc python3-tdb samba
  samba-common samba-common-bin samba-dsdb-modules samba-libs samba-vfs-modules tdb-tools
0 upgraded, 35 newly installed, 0 to remove and 0 not upgraded.
Need to get 19.6 MB of archives.
After this operation, 103 MB of additional disk space will be used.
Do you want to continue? (Y/n) Y
Get:1 http://ports.ubuntu.com/ubuntu-ports jammy/main arm64 libtalloc2 arm64 2.3.3-2build1 [24.8 kB]
Get:2 http://ports.ubuntu.com/ubuntu-ports jammy/main arm64 libtevent0 arm64 0.11.0-1build1 [38.0 kB]
Get:3 http://ports.ubuntu.com/ubuntu-ports jammy-updates/main arm64 libwbclient0 arm64 2:4.15.3+dfsg-0ubuntu0.3 [267 kB]
Get:4 http://ports.ubuntu.com/ubuntu-ports jammy/main arm64 python3-dnspython all 2.1.0-1ubuntu1 [123 kB]
Get:5 http://ports.ubuntu.com/ubuntu-ports jammy/main arm64 libtdb1 arm64 1.4.5-2build1 [47.3 kB]
Get:6 http://ports.ubuntu.com/ubuntu-ports jammy-updates/main arm64 libldb2 arm64 2:2.4.4-0ubuntu0.1 [152 kB]
Get:7 http://ports.ubuntu.com/ubuntu-ports jammy-updates/main arm64 python3-ldb arm64 2:2.4.4-0ubuntu0.1 [41.8 kB]
Get:8 http://ports.ubuntu.com/ubuntu-ports jammy/main arm64 python3-tdb arm64 1.4.5-2build1 [15.2 kB]
```

Installation of SAMBA using Advance Packaging Tool (APT)

```
thenc@th3nc:~$ systemctl status smbd
● smbd.service - Samba SMB Daemon
   Loaded: loaded (/lib/systemd/system/smbd.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2022-12-21 00:44:59 UTC; 2min 24s ago
     Docs: man:smbd(8)
           man:samba(7)
           man:smb.conf(5)
  Process: 732 ExecStartPre=/usr/share/samba/update-apparmor-samba-profile (code=exited, status=0/SUCCESS)
 Main PID: 750 (smbd)
   Status: "smbd: ready to serve connections..."
    Tasks: 4 (limit: 2188)
  Memory: 18.0M
     CPU: 70ms
   CGroup: /system.slice/smbd.service
           └─750 /usr/sbin/smbd --foreground --no-process-group
             └─791 /usr/sbin/smbd --foreground --no-process-group
               └─792 /usr/sbin/smbd --foreground --no-process-group
                 └─793 /usr/lib/aarch64-linux-gnu/samba/samba-bgqd --ready-signal-fd=45 --parent-watch-fd=11 --debuglevel=0 -F

Dec 21 00:44:59 th3nc systemd[1]: Starting Samba SMB Daemon...
Dec 21 00:44:59 th3nc systemd[1]: Started Samba SMB Daemon.
```

Checking if Samba is up and running or not.

Do the following

```
# Creating a shareable Directory
mkdir /tmp/sambashare

# Now go to " /etc/samba/smb.conf " and Edit
sudo vi /etc/samba/smb.conf

# Add Following Line
[sambashare]
    comment=Samba on Linux ( Ubuntu 22.04 )
    path=/tmp/sambashare
    browsable=yes
    read only=no

# esc + :wq ~ Write and Quit

# Restart SMB service to see the changes.
systemctl restart smbd
```

```
# Uncomment to allow remote administration of Windows print drivers.
# You may need to replace 'lpadmin' with the name of the group your
# admin users are members of.
# Please note that you also need to set appropriate Unix permissions
# to the drivers directory for these users to have write rights in it
; write list = root, @lpadmin
[smbashare]
comment = Samba on Linux ( Ubuntu 22.04 )
path = /tmp/smbashare/
browsable = yes
read only = no

"/etc/samba/smb.conf" 247L, 9064B written
```

Modification to smb.conf

```
thenc@th3nc:~$ sudo systemctl restart smbd
thenc@th3nc:~$ systemctl status smbd
• smbd.service - Samba SMB Daemon
   Loaded: loaded (/lib/systemd/system/smbd.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2022-12-21 01:06:39 UTC; 13s ago
     Docs: man:smbd(8)
           man:samba(7)
           man:smb.conf(5)
  Process: 1268 ExecStartPre=/usr/share/samba/update-apparmor-samba-profile (code=exited, status=0/SUCCESS)
 Main PID: 1278 (smbd)
   Status: "smbd: ready to serve connections..."
    Tasks: 4 (limit: 2188)
  Memory: 8.0M
     CPU: 76ms
   CGroup: /system.slice/smbd.service
           └─1278 /usr/sbin/smbd --foreground --no-process-group
             └─1280 /usr/sbin/smbd --foreground --no-process-group
               └─1281 /usr/sbin/smbd --foreground --no-process-group
                 └─1282 /usr/lib/aarch64-linux-gnu/samba/samba-bgqd --ready-signal-fd=45 --parent-watch-fd=11 --debuglevel=0 -F

Dec 21 01:06:39 th3nc systemd[1]: Starting Samba SMB Daemon...
Dec 21 01:06:39 th3nc systemd[1]: Started Samba SMB Daemon.
```

Restarting Service / Daemon

```
sudo smbpasswd -a < username >
# -a : add
```

```
thenc@th3nc:~$ sudo smbpasswd -a thenc
New SMB password:
Retype new SMB password:
Added user thenc.
```

Conclusion:

We have Successfully setup Samba File Server.

LAB 10

Learn the fundamentals of wireless Lan

Aim: To Learn the fundamentals of wireless LAN.

Theory:

- **Definition:** WLAN (Wireless Local Area Network), also known as LAWN (Local Area Wireless Network), allows mobile users to connect to a LAN wirelessly.
- **Standards:** Defined by the IEEE 802.11 group of standards.
- **Path Sharing:** Uses the Ethernet protocol and CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance).
- **Encryption:** Employs the Wired Equivalent Privacy (WEP) algorithm for secure data transmission.
- **High-Speed Communication:** Provides fast data communication within small areas like buildings or offices.
- **Mobility:** Allows users to stay connected while moving around within a confined area.

Advantages of WLANs

➤ Flexibility:

Within radio coverage, nodes can communicate without further restriction. Radio waves can penetrate walls, senders and receivers can be placed anywhere (also non-visible, e.g., within devices, in walls etc.)

➤ Planning:

Only wireless ad-hoc networks allow for communication without previous planning, any wired network needs wiring plans.

➤ Design:

Wireless networks allow for the design of independent, small devices which can for example be put into a pocket. Cables not only restrict users but also designers of small notepads, PDAs, etc.

➤ Robustness:

Wireless networks can handle disasters, e.g., earthquakes, flood etc. whereas, networks requiring a wired infrastructure will usually break down completely in

disasters.

➤ **Cost:**

The cost of installing and maintaining a wireless LAN is on average lower than the cost of installing and maintaining a traditional wired LAN, for two reasons. First, after providing wireless access to the wireless network via an access point for the first user, adding additional users to a network will not increase the cost. And second, wireless LAN eliminates the direct costs of cabling and the labor associated with installing and repairing it.

➤ **Ease of Use:**

Wireless LAN is easy to use and the users need very little new information to take advantage of WLANs.

Disadvantages of WLANs

➤ **Quality of Services:**

Quality of wireless LAN is typically lower than wired networks. The main reason for this is the lower bandwidth due to limitations in radio transmission, higher error rates due to interference and higher delay/delay variation due to extensive error correction and detection mechanisms.

➤ **Proprietary Solutions:**

Due to slow standardization procedures, many companies have come up with proprietary solutions offering standardization functionality plus many enhanced features. Most components today adhere to the basic standards IEEE 802.11a or 802.11b.

➤ **Restrictions:**

Several govt. and non-govt. institutions world-wide regulate the operation and restrict frequencies to minimize interference.

➤ **Global operation:**

Wireless LAN products are sold in all countries so, national and international frequency regulations have to be considered.

➤ **Low Power:**

Devices communicating via a wireless LAN are typically power consuming, also wireless devices running on battery power. Whereas the LAN design should take this into account and implement special power saving modes and power management functions.

➤ **License free operation:**

LAN operators don't want to apply for a special license to be able to use the product. The equipment must operate in a license free band, such as the 2.4 GHz ISM band.

➤ **Robust transmission technology:**

If wireless LAN uses radio transmission, many other electrical devices can interfere with them (such as vacuum cleaner, train engines, hair dryers, etc.). Wireless LAN transceivers cannot be adjusted for perfect transmission in a standard office or production environment.

Conclusion:

We have successfully learnt about fundamentals of the WLAN.

LAB 11

Learn various standard related to wireless LANs

Aim: To learn various standards related to wireless LANs.

Theory:

The Wireless Local Area Network (WLAN) technology is defined by the IEEE 802.11 family of specifications. There are currently four specifications in the family: 802.11, 802.11a, 802.11b, and 802.11g. All four use the Ethernet protocol and CSMA/CA (carrier sense multiple access with collision avoidance instead of CSMA/CD) for path sharing.

- 802.11 — applies to wireless LANs and provides 1 or 2 Mbps transmission in the 2.4 GHz band using either frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS).
- 802.11a — an extension to 802.11 that applies to wireless LANs and provides up to 54 Mbps in the 5GHz band. 802.11a uses an orthogonal frequency division multiplexing (OFDM) encoding scheme rather than FHSS or DSSS. The 802.11a specification applies to wireless ATM systems and is used in access hubs.
- 802.11b (also referred to as 802.11 High Rate or Wi-Fi) — an extension to 802.11 that applies to wireless LANs and provides 11 Mbps transmission (with a fallback to 5.5, 2 and 1 Mbps) in the 2.4 GHz band. 802.11b uses only DSSS. 802.11b was a ratification to the original 802.11 standard, allowing wireless functionality comparable to Ethernet.
- 802.11g — offers wireless transmission over relatively short distances at 20 – 54 Mbps in the 2.4 GHz band. The 802.11g also uses the OFDM encoding scheme.
- 802.11n – builds upon previous 802.11 standards by adding MIMO (multiple- input multiple-output). IEEE 802.11n offers high throughput wireless transmission at 100Mbps – 200 Mbps.

| Name | Band (GHz) | Maximum Transmission Rate (Mbit/s) | Note |
|---------------|--------------|------------------------------------|--|
| 802.11 Legacy | 2.4 | 2 | Outdated, virtually no end devices available |
| 802.11a | 5 | 54 | Less interference-prone |
| 802.11b | 2.4 | 11 | Less common |
| 802.11g | 2.4 | 54 | Widespread, backwards compatible with 11b |
| 802.11n | 2.4 and/or 5 | 300 | Common |

- The main problem of radio networks acceptance in the market place is that there is not one unique standard like Ethernet with a guaranteed compatibility between all devices, but many proprietary standards pushed by each independent vendor and incompatible between themselves. Because corporate customers require an established unique standard, most of the vendors have joined the IEEE in an effort to create a standard for radio LANs. This is IEEE 802.11 (like Ethernet is IEEE 802.3, Token Rings IEEE 802.5 and 100vg is IEEE 802.12).
- Once in the 802.11 committee, each vendor has pushed its own technologies and specificities in the standard to try to make the standard closer to its product. The result is a standard which took far too much time to complete, which is overcomplicated and bloated with features, and might be obsoleted before products come to market by newer technologies. But it is a standard based on experience, versatile and well designed and including all of the optimizations and clever techniques developed by the different vendors.
- The 802.11 standard specifies one MAC protocol and 3 physical layers: Frequency Hopping 1 Mb/s (only), Direct Sequence 1 and 2 Mb/s and diffuse infrared (can we really call it a “standard” when it includes 3 incompatible physical layers?). Since then, it has been extended to support 2 Mb/s for Frequency Hopping and 5.5 and 11 Mb/s for Direct Sequence (802.11b). The MAC has two main standards of operation, a distributed

mode (CSMA/CA), and a coordinated mode (polling mode – not much used in practice). 802.11 of course uses MAC level retransmissions, and also RTS/CTS and fragmentation.

- The optional power management features are quite complex. The 802.11 MAC protocol also includes optional authentication and encryption (using the WEP, Wired Equivalent Privacy, which is RC4 40 bits – some vendors do offer 128 bits RC4 as well). On the other hand, 802.11 lacks to defines some area (multi-rate, roaming, inter AP communication...), that might be covered by future developments of the standard or complementary standards. Some 802.11 products also implement proprietary extensions (bit-rate adaptation, additional modulation schemes, stronger encryption...), those extensions may or may not be added to the standard over time.
- When 802.11 was finalized (September 97), most vendors were slow to implement 802.11 products because of the complexity of the standard and the number of mandatory features (and in some cases they also need to provide backward compatibility with their own previous line of products). Some of the optional features (encryption and power saving) did only appear months after the initial release of the product. But things seem to be sorted out and we now have fully featured products on the market. The complexity of the specification, the tightness of the requirements and the level of investment required made 802.11 products expensive compared to the previous generation of wireless LANs, but because of the higher standardization and higher volumes, prices are now dropping.
- Even if vendors eventually have launched 802.11 products, the standard doesn't fully guarantee inter-operability: the products have to use at least the same physical layer, the same bit rate and the same mode of operation (and there is so many other little important details...). The most cooperative vendors have been busy lately sorting out interoperability issues with independent testing labs, but it is still a touchy subject...
- After 7 years of arguing in sub-committees making 802.11, you would think that most people would have enough of it. In fact, no, the 802.11 committee is now busy pushing a new standard at 5 GHz, and also higher speed at 2.4 GHz (by tweaking the Direct Sequence physical layer). Each standard makes changes only to the physical layer, so that the 802.11 MAC can be reused totally unmodified, saving costs.
- 802.11-a (802.11 at 5 GHz) was standardized first (spring 99), based on OFDM, and using the UNII band (so it won't be available in Europe and Japan). The OFDM physical layer is a very close copy of the one used in Hyper-Lan II (so they might be some sort of compatibility), using 52

subcarriers in a 20 MHz channel, offering 6, 12 and 24 Mb/s and optional 9, 18, 36, 48 and 54 Mb/s bitrates. No products are yet on the market.

- Very soon after, 802.11 did standardize 802.11-b (802.11 HR), based on a modified DS physical layer. The goal was to extend the life of the 2.4 GHz band by overcoming the major drawback: low speed. On top of the original 802.11- DS standard, 802.11-b offer additional 5.5 Mb/s and 11 Mb/s bit rates. It was approved by the FCC and they are now products on the market (which are quite popular).

Conclusion:

We have successfully learnt about the various standards of WLAN.

LAB 12

Learn about the security aspects of wireless LANs.

Aim: To learn about the security aspects of wireless LANs.

Theory:

➤ Cyber Attacks Piggybacking

If you fail to secure your wireless network, anyone with a wireless-enabled computer in range of your access point can use your connection. The typical indoor broadcast range of an access point is 150–300 feet. Outdoors, this range may extend as far as 1,000 feet. So, if your neighborhood is closely settled, or if you live in an apartment or condominium, failure to secure your wireless network could open your internet connection to many unintended users. These users may be able to conduct illegal activity, monitor and capture your web traffic, or steal personal files.

➤ Wardriving

Wardriving is a specific kind of piggybacking. The broadcast range of a wireless access point can make internet connections available outside your home, even as far away as your street. Savvy computer users know this, and some have made a hobby out of driving through cities and neighborhood's with a wireless-equipped computer— sometimes with a powerful antenna—searching for unsecured wireless networks. This practice is known as “wardriving.”

➤ Evil Twin Attacks

In an evil twin attack, an adversary gathers information about a public network access point, then sets up their system to impersonate it. The adversary uses a broadcast signal stronger than the one generated by the legitimate access point; then, unsuspecting users connect using the stronger signal. Because the victim is connecting to the internet through the attacker's system, it's easy for the attacker to use specialized tools to read any data the victim sends over the internet. This data may include credit card numbers, username and password combinations, and other personal information. Always confirm the name and password of a public Wi-Fi hotspot prior to use. This will ensure you are connecting to a trusted access point.

➤ Wireless Sniffing

Many public access points are not secured and the traffic they carry is not encrypted. This can put your sensitive communications or transactions at risk.

Because your connection is being transmitted “in the clear,” malicious actors could use sniffing tools to obtain sensitive information such as passwords or credit card numbers. Ensure that all the access points you connect to use at least WPA2 encryption.

➤ **Unauthorized Computer Access**

An unsecured public wireless network combined with unsecured file sharing could allow a malicious user to access any directories and files you have unintentionally made available for sharing. Ensure that when you connect your devices to public networks, you deny sharing files and folders. Only allow sharing on recognized home networks and only while it is necessary to share items. When not needed, ensure that file sharing is disabled. This will help prevent an unknown attacker from accessing your device’s files.

➤ **Shoulder Surfing**

In public areas malicious actors can simply glance over your shoulder as you type. By simply watching you, they can steal sensitive or personal information. Screen protectors that prevent shoulder-surfers from seeing your device screen can be purchased for little money. For smaller devices, such as phones, be cognizant of your surroundings while viewing sensitive information or entering passwords.

➤ **Theft of Mobile Devices**

Not all attackers rely on gaining access to your data via wireless means. By physically stealing your device, attackers could have unrestricted access to all of its data, as well as any connected cloud accounts. Taking measures to protect your devices from loss or theft are important, but should the worst happen, a little preparation may protect the data inside. Most mobile devices, including laptop computers, now have the ability to fully encrypt their stored data—making devices useless to attackers who cannot provide the proper password or personal identification number (PIN). In addition to encrypting device content, it is also advisable to configure your device’s applications to request login information before allowing access to any cloud-based information. Last, individually encrypt or password-protect files that contain personal or sensitive information. This will afford yet another layer of protection in the event an attacker is able to gain access to your device.

Minimize Risks

Change default passwords.

Most network devices, including wireless access points, are pre-configured with default administrator passwords to simplify setup. These default passwords are easily available to obtain online, and so provide only marginal protection. Changing default passwords makes it harder for attackers to access a device. Use and periodic changing of complex passwords is your first line of defense in protecting your device.

Restrict access.

Only allow authorized users to access your network. Each piece of hardware connected to a network has a media access control (MAC) address. You can restrict access to your network by filtering these MAC addresses. Consult your user documentation for specific information about enabling these features. You can also utilize the “guest” account, which is a widely used feature on many wireless routers. This feature allows you to grant wireless access to guests on a separate wireless channel with a separate password, while maintaining the privacy of your primary credentials.

Encrypt the data on your network.

Encrypting your wireless data prevents anyone who might be able to access your network from viewing it. There are several encryption protocols available to provide this protection. Wi-Fi Protected Access (WPA), WPA2, and WPA3 encrypt information being transmitted between wireless routers and wireless devices. WPA3 is currently the strongest encryption. WPA and WPA2 are still available; however, it is advisable to use equipment that specifically supports WPA3, as using the other protocols could leave your network open to exploitation.

Protect your Service Set Identifier (SSID).

To prevent outsiders from easily accessing your network, avoid publicizing your SSID. All Wi-Fi routers allow users to protect their device’s SSID, which makes it more difficult for attackers to find a network. At the very least, change your SSID to something unique. Leaving it as the manufacturer’s default could allow a potential attacker to identify the type of router and possibly exploit any known vulnerabilities.

Conclusion:

We have successfully learnt about security aspects of WLANs.

