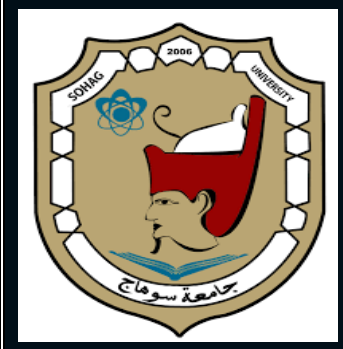


Sohag University

Faculty of computer and Artificial Intelligence

Network Department

Enterprise Composite Network Model

(ECNM)

Submitted by:

- **Abdelrahman Nasser**
- **Joy Anis**
- **Mariam Nasim**
- **Mariam Sameh**
- **Martha Talaat**

Supervised By

Prof.Dr. Mahmoud abou El-majd

2023 – 2024

Network Department committee

Prof.Dr. Hamdy Hasan Prof.Dr. Mahmoud abou El-majd Prof.Dr. Ahmed Abdelhakem

Contents

Project Idea: 5

Infrastructure of network 6

Chapter 1 7

Infrastructure of network 7

Basic configuration 8

Interface IPs 8

Active router 9

An Introductory Guide to Routing & Switching 10

Types of Routing 10

- Static Routing 10
- Default Routing 10
- Dynamic Routing 10

Default Routing 10

Dynamic Routing 11

Open Shortest Path First (OSPF) 11

OSPF Terms 12

FHRP-First Hop Redundancy Protocol 16

Common FHRPs include: 16

HSRP 16

EtherChannel 19

Wireless Network 20

Chapter 2 22

VPN +GRE 22

What is VPN ? 23

VPN function 23

GRE tunnels 24

Introduction: 25

2.12.4. disadvantage of GRE: 27

VOIP 30

KEY TAKEAWAYS 31

Understanding Voice-Over-Internet Protocol (VoIP) 31

What is a VoIP Number? 32
Essential components for VoIP calling 32
Chapter 4 36
Data center 36
Servers implemented on Linux OS: - 37
(1) File Transfer Protocol (FTP) Server: 37
(2) Network File System (NFS) Server: - 38
(3) Apache Web Server :- 40
(4) MariaDB Server: - 41
Network Interface Card (NIC) Teaming: - 42
Windows server 44
1- Computer name: 45
2- groups 46
3- Group Policy: 47
4- DHCP Server: 50
5- DNS Server: 51
6- PRINT Server: 52
Chapter 5 57
security 57
Introduction 58
Design network security 58
External network zone 59
Internal network zone 59
DMZ (Demilitarized zone) 59
Attacks 59
What is Denial-of-services (DOS)? 59
How can you tell if a computer is experiencing a DoS attack? 61
What is the difference between a DDoS attack and a DOS attack? 61
Protection from DOS attack 62
Standard defensive-oriented technologies 63
Intrusion Detection System (IDS): 63

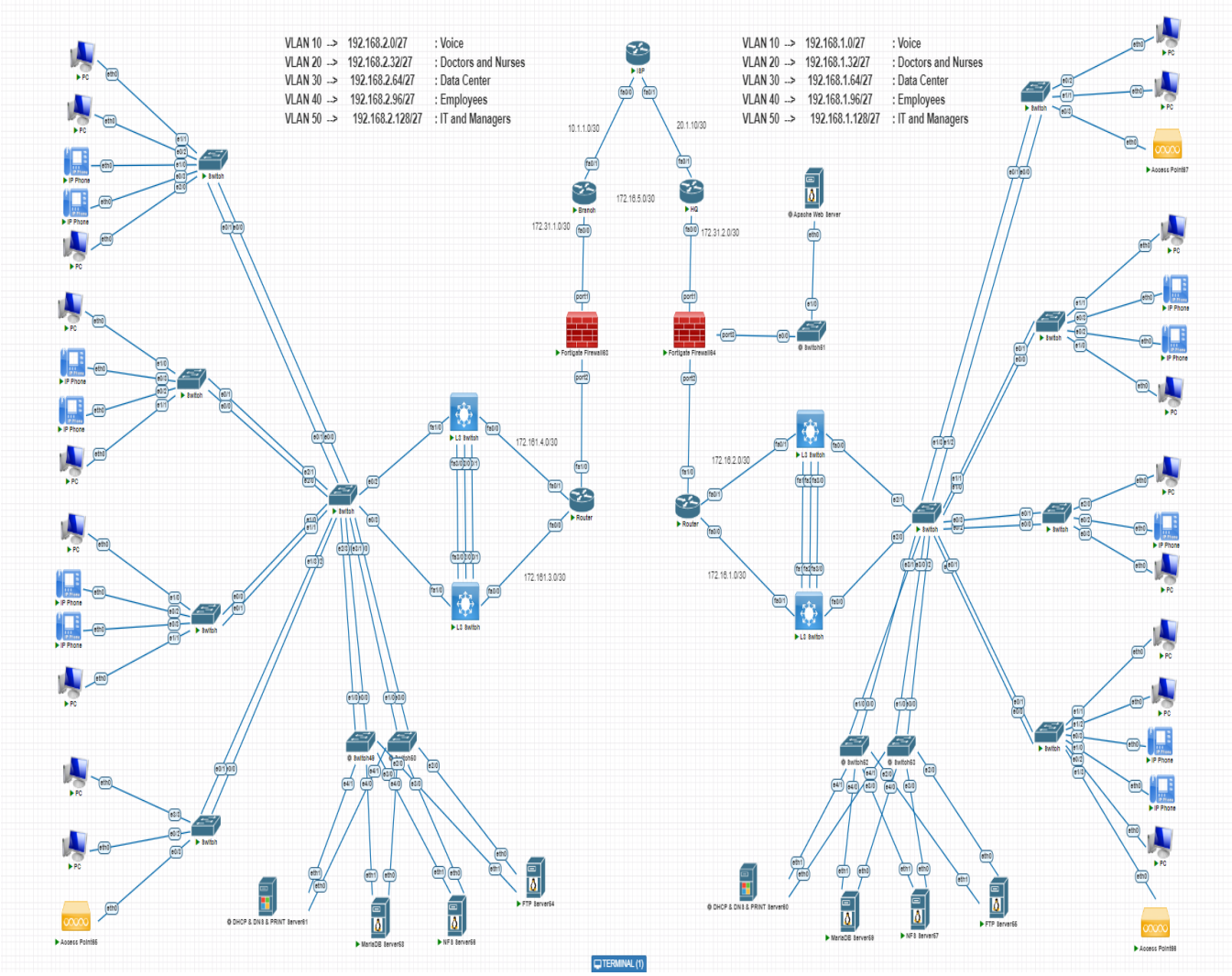
Intrusion Prevention System (IPS): 63
Firewall **64**
What is a firewall? 64
Types of firewalls 64
How Firewalls Work 64
Advantages of a Firewal 64
Disadvantages of using Firewall 65
Policy applied to firewall 66
Chapter 6 ..... **67**
Bill of Materials **69**
Circuit Diagram: IOT Based Biometric Fingerprint Attendance System **70**
Setting Up the Website **70**
Source Code/Program **72**
Results **72**
Sources: **75**

Project Idea:

The idea is to create a model to connect various branches of any entity, unrestricted by a specific number of branches or geographical locations. This concept has been applied in the medical field to link a hospital branch in Cairo with the main branch in Berlin.The main branch includes a data center with various operating systems, providing high security for the room.The hospital's website is hosted on a server in the main branch in Berlin,as well as a server for patient data storage. Any computer in any branch can access it, including through mobile devices due to the building's wireless coverage.Additionally, it provides cameras to monitor patients' conditions, fire alarms throughout the building, and fingerprint recognition for tracking employee attendance. The branches are interconnected through an encrypted channel via VPN. This comprehensive approach enhances both security and efficiency in managing the medical facilities.

Infrastructure of network

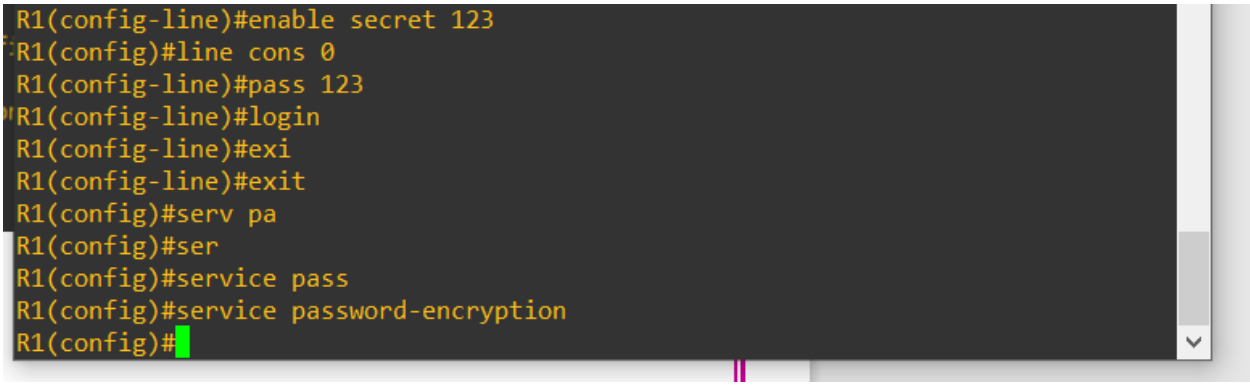
the communication between geographically distant branches occurs over the internet using a secure and encrypted channel for data transmission. Additionally, the network enables voice calls over the Internet instead of analog telephones. The ability of the public to access the hospital's website without affecting the private network is ensured. Additionally, there is a shared printer on each floor for common use. Maintaining network uptime is achieved through high availability and EtherChannel. Additionally, ensuring that traffic is always encrypted. preventing capturing, is done using IPsec.



Chapter 1

Infrastructure of network Routing & Switching

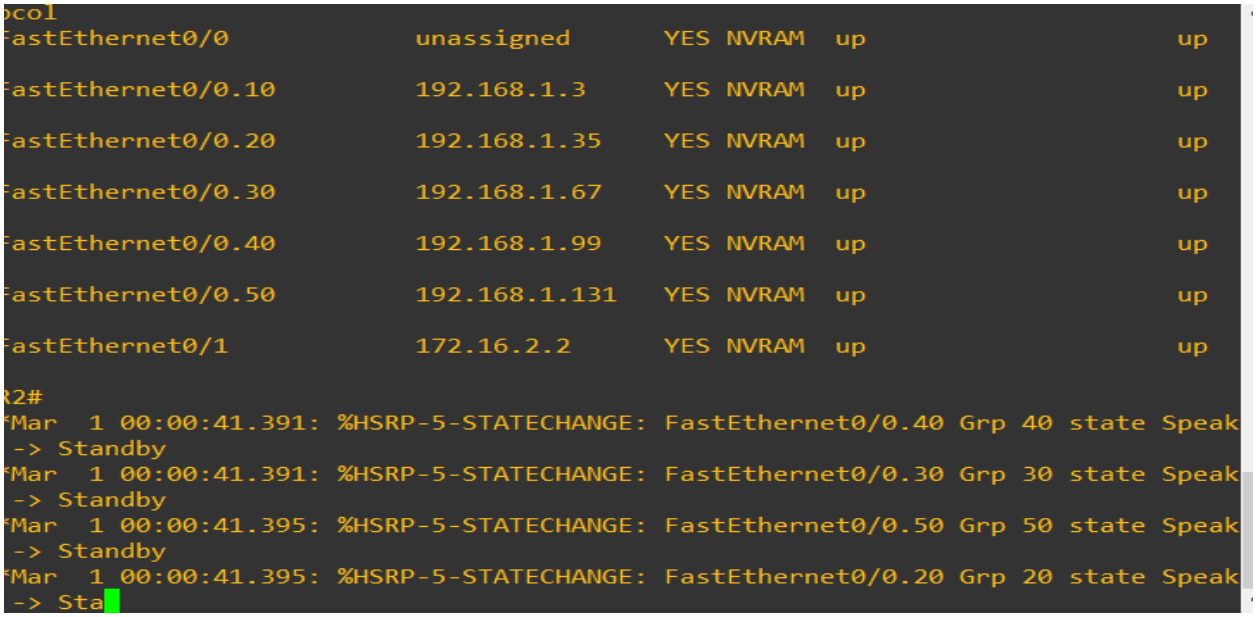
1.1. Basic configuration



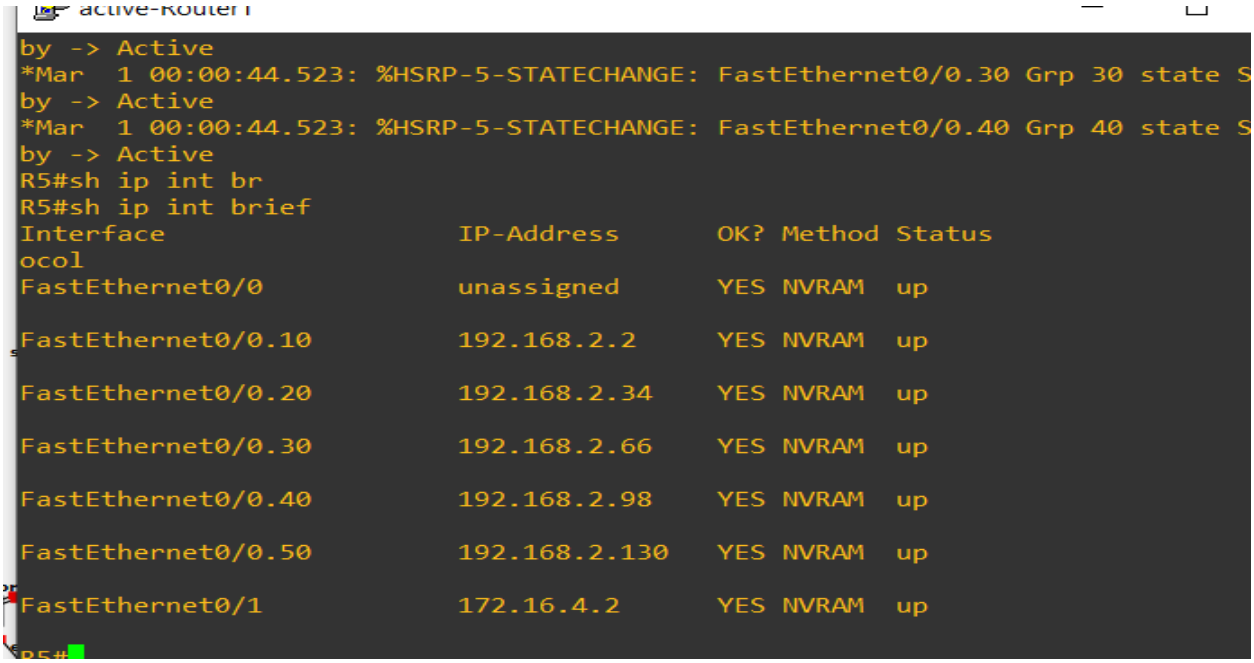
1.2. Interface IPs

ISP router		F0/1 **20.1.1.1/30**				
HQ-Router	F0/0 10.1.1.2/30	F0/1 172.31.1.1/30	Int tunnel1 172.16.5.1			
Branch-Router	F0/0 20.1.1.2/30	F0/1 172.31.2.1/30	Int tunnel1 172.16.5.2			
core-router1	F1/0 172.31.1.2/30	F0/0 172.16.3.1/30	F0/1 172.16.4.1/30			
core-router	F1/0 172.31.2.2/30	F0/0 172.16.1.1/30	F0/1 172.16.2.1/30			
standby-router	F0/1 172.16.1.2/30	F0/0.10 192.168.1.2	F0/0.20 192.168.1.34	F0/0.30 192.168.1.66	F0/0.40 192.168.1.98	F0/0.50 192.168.1.130
active-Router	F0/1 172.16.2.2/30	F0/0.10 192.168.1.3	F0/0.20 192.168.1.35	F0/0.30 192.168.1.67	F0/0.40 192.168.1.99	F0/0.50 192.168.1.131
standby-router-1	F0/1 172.16.3.2/30	F0/0.10 192.168.2.3	F0/0.20 192.168.2.35	F0/0.30 192.168.2.67	F0/0.40 192.168.2.99	F0/0.50 192.168.2.131
active-Router-1	F0/1 172.16.3.2/30	F0/0.10 192.168.2.2	F0/0.20 192.168.2.34	F0/0.30 192.168.2.66	F0/0.40 192.168.2.98	F0/0.50 192.168.2.130

1.3. Active Router interfaces



1.4. Active-Router-1 interfaces



1.4. An Introductory Guide to Routing & Switching

Routing and switching are the basic functions of computer networking. Routing refers to finding a path between two or more networks and switching refers to moving data from one device to another within a network.
These two concepts are the building blocks of all communications, from data to voice and video to wireless access. Businesses and organizations use routing and switching to share applications, speed access to information, enhance customer service, reduce operating costs, improve security, and enable remote connections.

1.4.1. Types of Routing

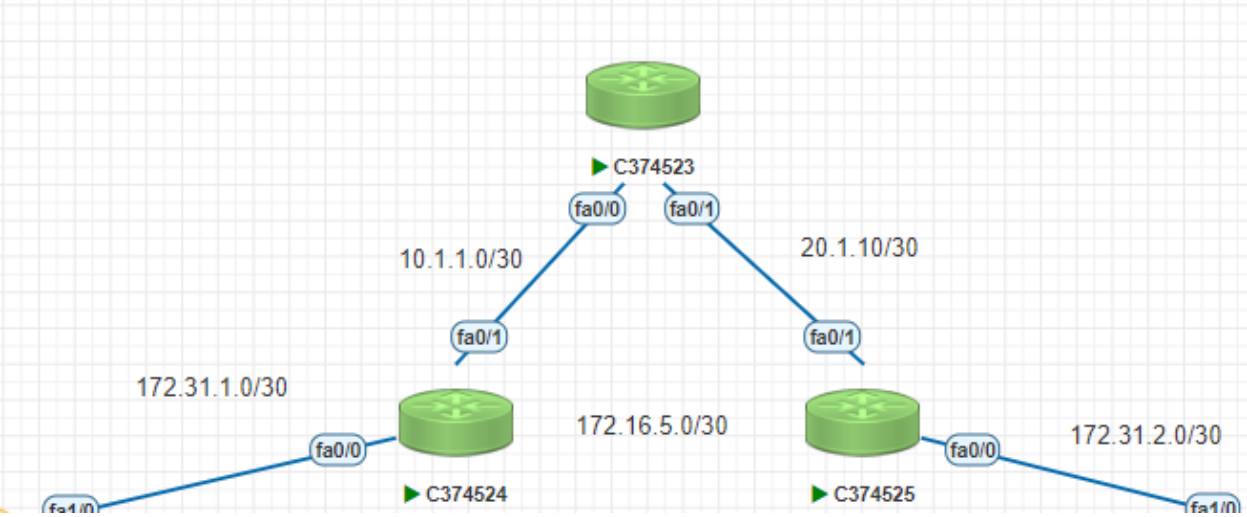
There are 3 types of routing that are described below.

- **Static Routing**
- **Default Routing**
- **Dynamic Routing**

1.4.2. Default Routing

This is the method where the router is configured to send all packets toward a single router (next hop). It doesn't matter to which network the packet belongs, it is forwarded out to the router which is configured for default routing. It is generally used with stub routers. A stub router is a router that has only one route to reach all other networks.

Configuration



HQ-router

```
hanged state to up
R9(config)#ip rou
R9(config)#ip route 0.0.0.0 0.0.0.0 10.1.1.1
```

Branch-router

```
hanged state to up
R9(config)#ip rou
R9(config)#ip route 0.0.0.0 0.0.0.0 20.1.1.1
```

1.5. Dynamic Routing

Dynamic routing makes automatic adjustments of the routes according to the current state of the route in the routing table. Dynamic routing uses protocols to discover network destinations and the routes to reach them. RIP and OSPF are the best examples of dynamic routing protocols. Automatic adjustments will be made to reach the network destination if one route goes down.

1.5.1. Open Shortest Path First (OSPF)

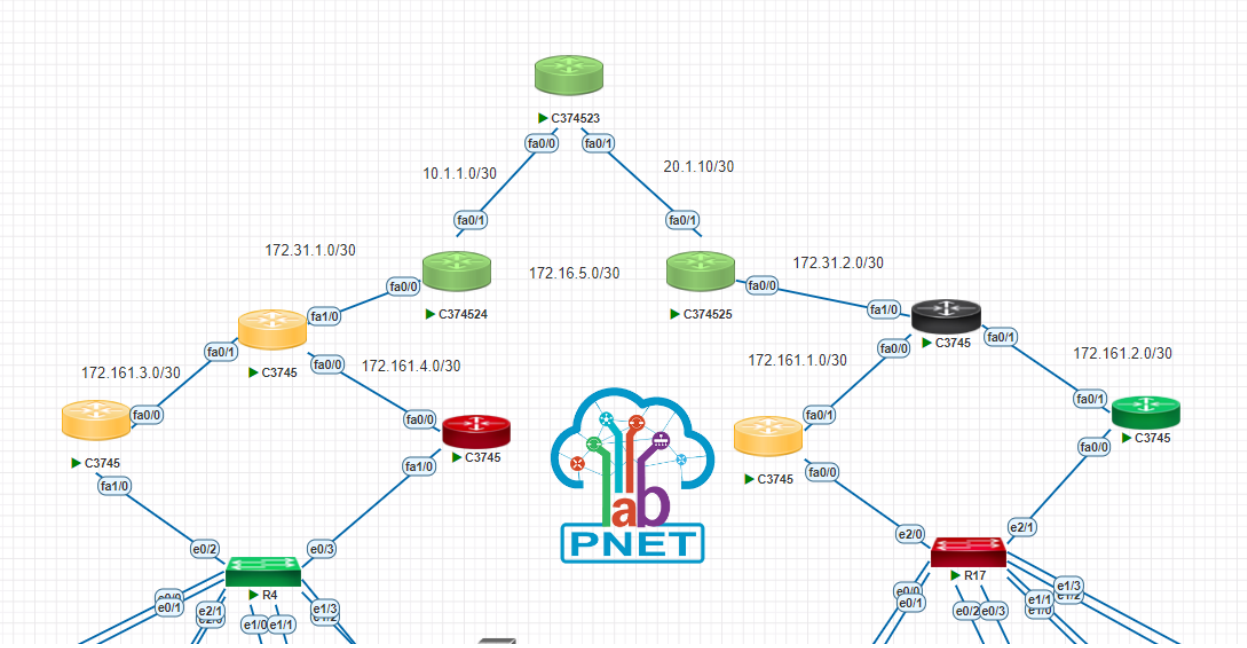
is a link-state routing protocol that is used to find the best path between the source and the destination router using its own Shortest Path First). OSPF is developed by Internet Engineering Task Force (IETF) as one of the Interior Gateway Protocol (IGP), i.e, the protocol which aims at moving the packet within a large autonomous system or routing domain. It is a network layer protocol which works on protocol

number 89 and uses AD value 110. OSPF uses multicast address 224.0.0.5 for normal communication and 224.0.0.6 for update to designated router(DR)/Backup Designated Router (BDR).

1.5.2. OSPF Terms

1. **Router Id**
2. **Router priority**
3. **Designated Router (DR)**
4. **Backup Designated Router (BDR)**
5. **DR and BDR election**

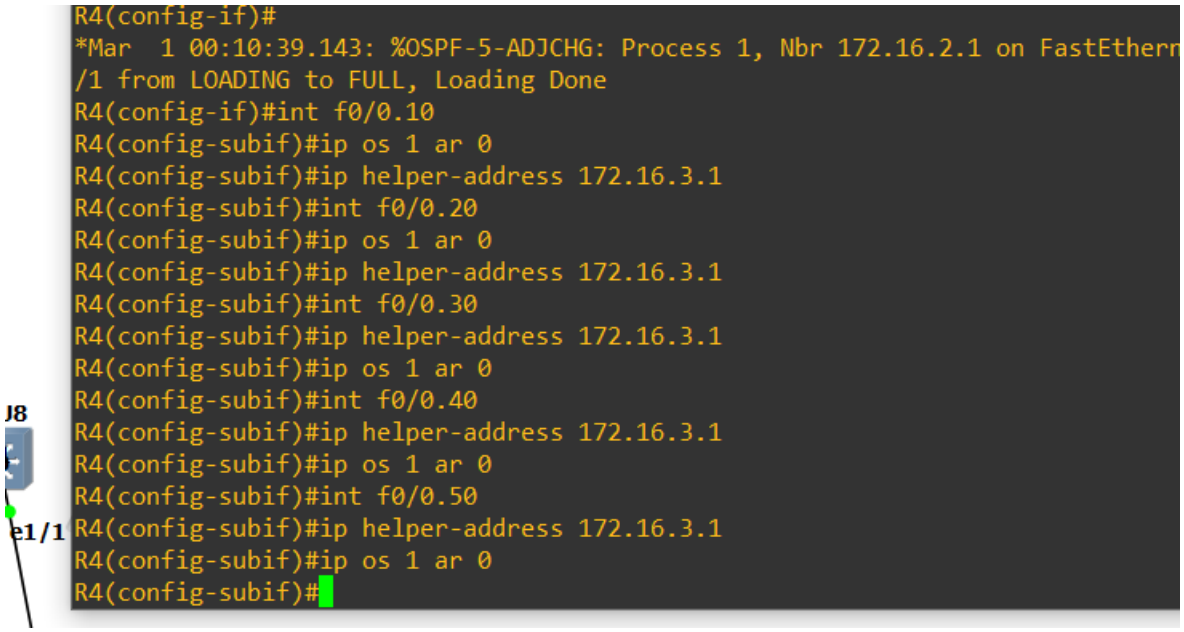
1.5.3. OSPF topology



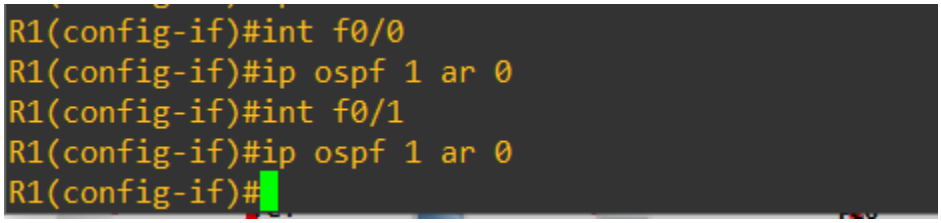
1.5.4. OSPF configuration

Configuring OSPF Enabling OSPF Router(config)#router OSPF ? Process ID Process ID: is value in the range from 1 to 65,535 identifies the OSPF.

Active and standby routers **configuration**

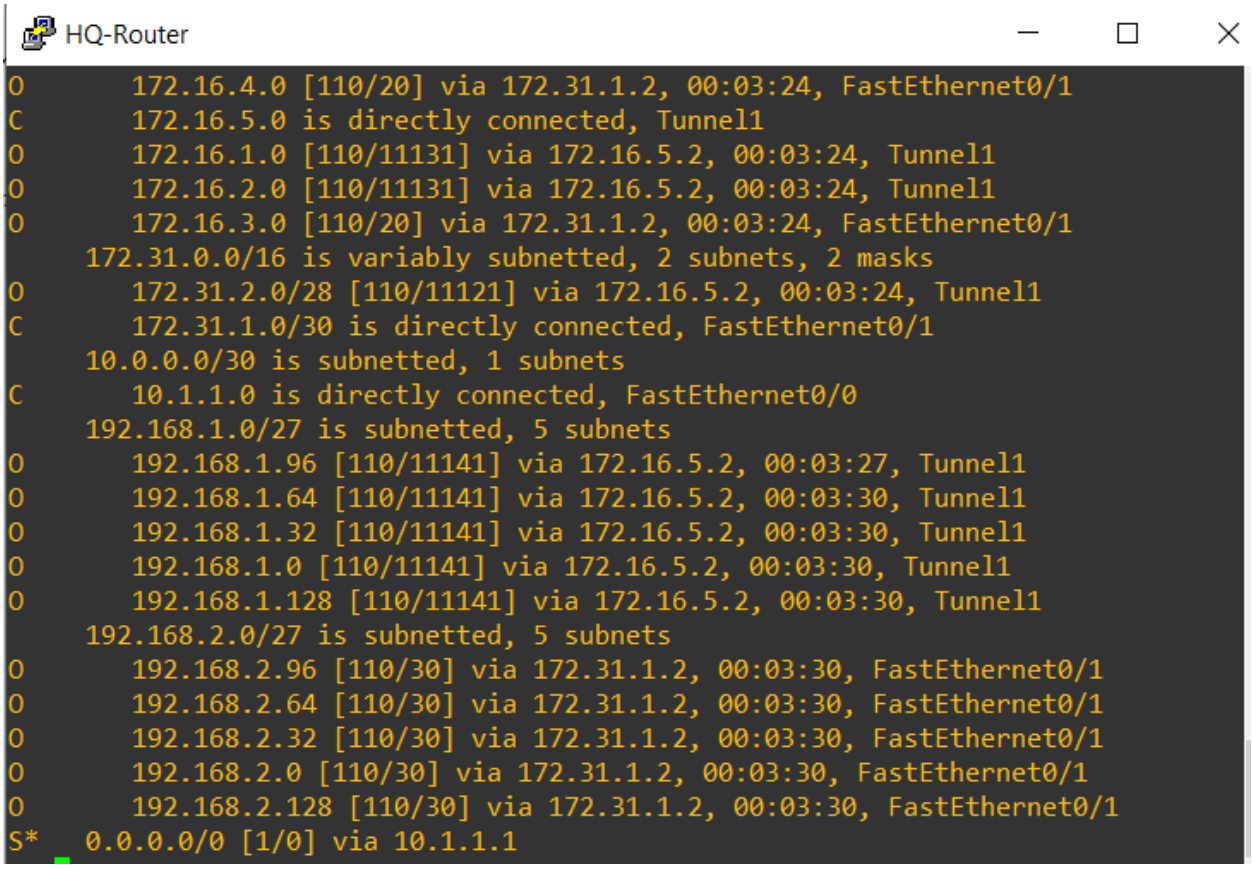


Core router



1.5.5. Routing table.

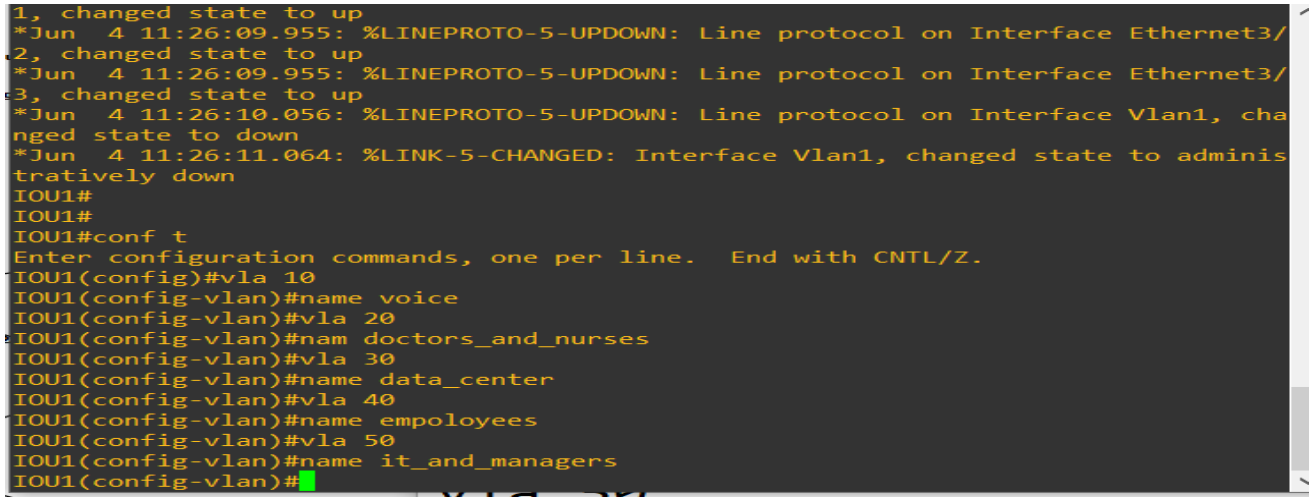
base (RIB), is a data table stored in a router or a network host that lists the routes to particular network destinations, and in some cases, metrics (distances) associated with those routes



1.6. Switch vlan configuration

In each branch there are four floors, and each floor contains a different group of doctors, trained nurses, and VoIP devices, so each floor contains a switch divided into four VLANs, and the fourth floor contains data center

1.6.1. Switch configuration in every branch



1.6.2. Assign ports to each VLAN

```
IOU1(config-if-range)#sw voic vl 10
IOU1(config-if-range)#int ran e1/1-3
IOU1(config-if-range)#sw mo acc
IOU1(config-if-range)#sw ac vl 20
IOU1(config-if-range)#int ran e2/0-3
IOU1(config-if-range)#sw mo acc
IOU1(config-if-range)#sw ac vl 50
IOU1(config-if-range)#int ran e3/0-3
IOU1(config-if-range)#sw mo acc
IOU1(config-if-range)#sw ac vl 40
IOU1(config-if-range)#int ran e0/0-1
IOU1(config-if-range)#switchport trunk encapsulation dot1q
IOU1(config-if-range)#sw mo tru
IOU1(config-if-range)#
*Jun  4 11:29:03.628: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/
0, changed state to down
*Jun  4 11:29:03.629: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/
1, changed state to down
IOU1(config-if-range)#
*Jun  4 11:29:06.638: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/
0, changed state to up
*Jun  4 11:29:06.639: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/
1, changed state to up
IOU1(config-if-range)#
```

1.6.2. Inter-VLAN routing configuration

Inter-VLAN routing is the ability to route, or send, traffic between VLANs that are normally blocked by default. Switches and VLANs work at the MAC address Layer (Layer 2). Traffic can't be routed between VLANs at Layer 2 based on MAC addresses.

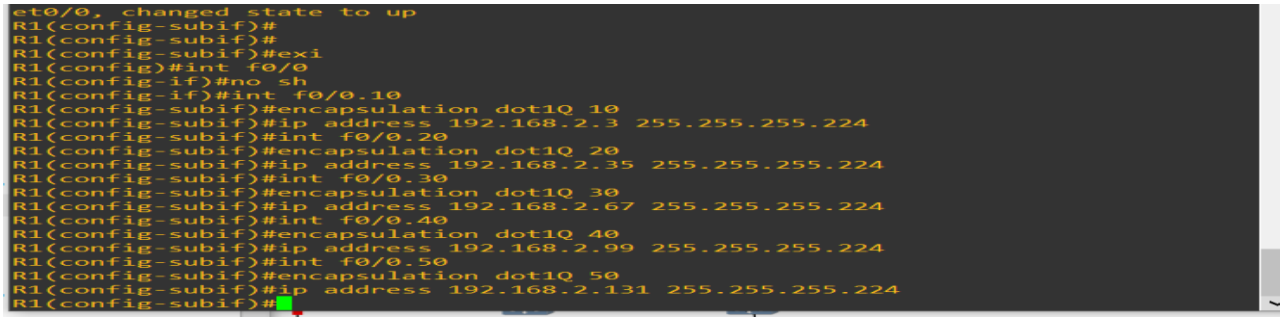
```
R1(config)#int f0/0
R1(config-if)#no sh
R1(config-if)#int f0/0.10
R1(config-subif)#encapsulation dot1Q 10
R1(config-subif)#ip address 192.168.2.2 255.255.255.224
R1(config-subif)#int f0/0.20
R1(config-subif)#encapsulation dot1Q 20
R1(config-subif)#ip address 192.168.2.34 255.255.255.224
R1(config-subif)#int f0/0.30
R1(config-subif)#encapsulation dot1Q 30
R1(config-subif)#ip address 192.168.2.66 255.255.255.224
R1(config-subif)#int f0/0.40
R1(config-subif)#encapsulation dot1Q 40
R1(config-subif)#ip address 192.168.2.98 255.255.255.224
R1(config-subif)#int f0/0.50
R1(config-subif)#encapsulation dot1Q 50
R1(config-subif)#ip address 192.168.2.130 255.255.255.224
R1(config-subif)#
R1(config-subif)#
*Mar  1 00:01:35.743: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state t
o up
*Mar  1 00:01:36.743: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/0, changed state to up
R1(config-subif)#
```

1.6.3. Router on a stick

A **router on a stick**, also known as a **one-armed router**,[1][2] is a router that has a single physical or logical connection to a network. It is a method of inter-VLAN routing where one router is connected to a switch via a single cable. The router has physical connections to the broadcast domains where one or more VLANs require the need for routing between them.

Devices on separate VLANs or in a typical local area network are unable to communicate with each other. Therefore, it is often used to forward traffic between locally attached hosts on separate logical routing domains or to facilitate routing table administration, distribution and relay.

Configuration



1.7. FHRP-First Hop Redundancy Protocol

FHRP typically stands for "First Hop Redundancy Protocol." First Hop Redundancy Protocols are network protocols used to provide high availability and fault tolerance for network hosts' default gateway or first hop. The default gateway is the router that network devices use to forward traffic to destinations outside their own subnet.

1.7.1. Common FHRPs include:

- ✓ Hot Standby Router Protocol (HSRP)
- ✓ Virtual Router Redundancy Protocol (VRRP)
- ✓ Gateway Load Balancing Protocol (GLBP)

1.7.2. HSRP

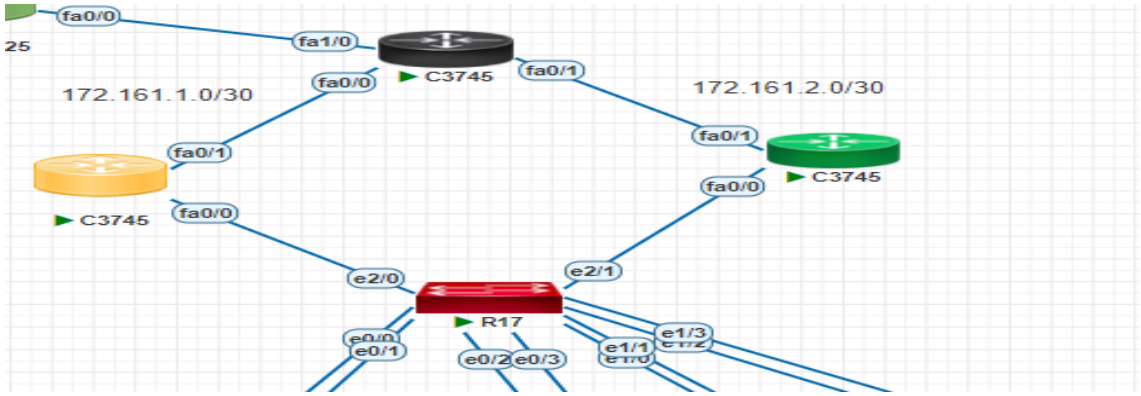
FHRP typically stands for "First Hop Redundancy Protocol." First Hop Redundancy Protocols are network protocols used to provide high availability and fault tolerance for network hosts' default gateway or first hop. The default

gateway is the router that network devices use to forward traffic to destinations outside their own subnet

With **Hot Standby Router Protocol** mechanism, even if a failure occurs on one device in the **HSRP Group**, then the traffic goes through on another device in that Group, through an alternative path.

Hot Standby Router Protocol provides this by using a Virtual IP address and a MAC address as a Gateway of multiple path alternatives. The traffic is always go to the Virtual IP address, Virtual Gateway. So, the traffic flow is independant from a device. This avoids single point of failure on the networks.

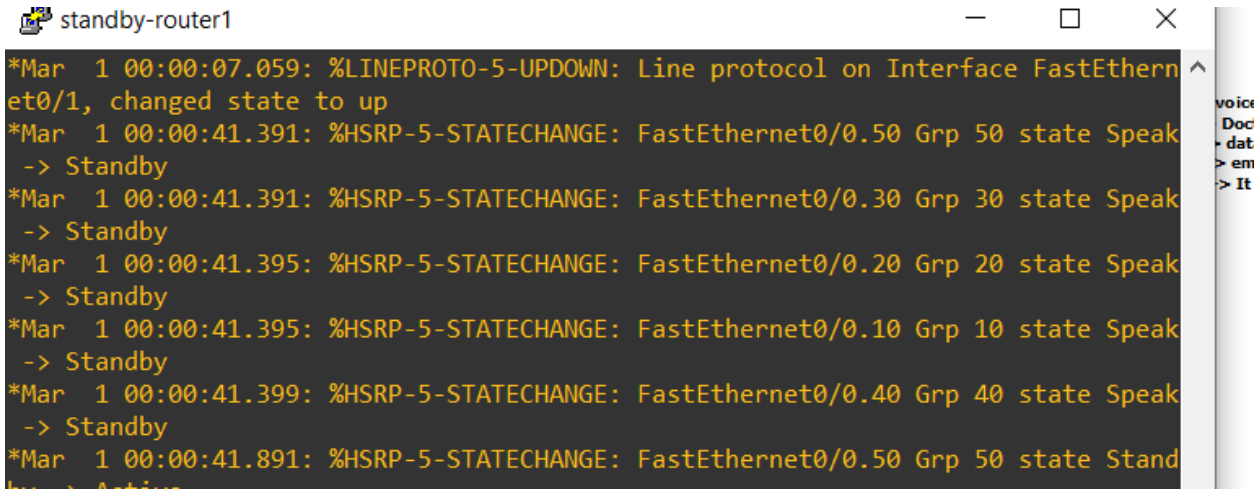
Configuration



Standby Router configuration

R1

```
*Mar  1 00:00:06.947: %LINK-5-CHANGED: Interface FastEthernet
to administratively down
*Mar  1 00:00:07.735: %LINEPROTO-5-UPDOWN: Line protocol on I
et0/1, changed state to down
*Mar  1 00:00:07.947: %LINEPROTO-5-UPDOWN: Line protocol on I
et0/0, changed state to down
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int f0/0.10
R1(config-subif)#standby 10 ip 192.168.2.1
R1(config-subif)#standby 10 priority 200
R1(config-subif)#int f0/0.20
R1(config-subif)#standby 20 ip 192.168.2.33
R1(config-subif)#standby 20 priority 200
R1(config-subif)#int f0/0.30
R1(config-subif)#standby 30 ip 192.168.2.65
R1(config-subif)#standby 30 priority 200
R1(config-subif)#int f0/0.40
R1(config-subif)#standby 40 ip 192.168.2.97
R1(config-subif)#standby 40 priority 200
R1(config-subif)#int f0/0.50
R1(config-subif)#standby 50 ip 192.168.2.129
R1(config-subif)#standby 50 priority 200
R1(config-subif)#
```



Active Router configuration

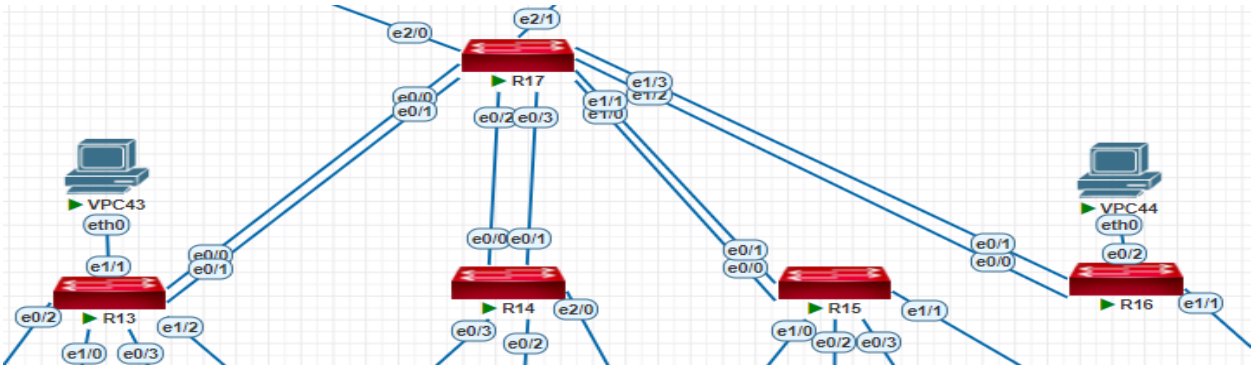
```
R1(config-subif)#int f0/0.10
R1(config-subif)#standby 10 ip 192.168.2.1
R1(config-subif)#int f0/0.20
R1(config-subif)#standby 20 ip 192.168.2.33
R1(config-subif)#int f0/0.30
R1(config-subif)#standby 30 ip 192.168.2.65
R1(config-subif)#int f0/0.40
R1(config-subif)#standby 40 ip 192.168.2.97
R1(config-subif)#int f0/0.50
R1(config-subif)#standby 50 ip 192.168.2.129
R1(config-subif)#
```

```
*Mar  1 00:00:41.891: %HSRP-5-STATECHANGE: FastEthernet0/0.50 Grp 50 state Stand
by -> Active
*Mar  1 00:00:41.895: %HSRP-5-STATECHANGE: FastEthernet0/0.30 Grp 30 state Stand
by -> Active
*Mar  1 00:00:41.895: %HSRP-5-STATECHANGE: FastEthernet0/0.20 Grp 20 state Stand
by -> Active
*Mar  1 00:00:41.895: %HSRP-5-STATECHANGE: FastEthernet0/0.10 Grp 10 state Stand
by -> Active
*Mar  1 00:00:41.895: %HSRP-5-STATECHANGE: FastEthernet0/0.40 Grp 40 state Stand
by -> Active
*Mar  1 00:00:46.523: %OSPF-5-ADJCHG: Process 1, Nbr 172.31.1.2 on FastEthernet0
/1 from LOADING to FULL, Loading Done
```

1.8. EtherChannel

EtherChannel is a port link aggregation technology or port-channel architecture used primarily on Cisco switches. It allows grouping of several physical Ethernet links to create one logical Ethernet link for the purpose of providing fault-tolerance and high-speed links between switches, routers and servers. An EtherChannel can be created from between two and eight active Fast

Configuration



Switch 1 configuration

```
Creating a port-channel interface Port-channel 1

IOU1(config-if-range)#int range e0/2-3
IOU1(config-if-range)#channel-Group 2 MOde active
IOU1(config-if-range)#int range e1/0-1
IOU1(config-if-range)#channel-Group 3 MOde active
Creating a port-channel interface Port-channel 3

IOU1(config-if-range)#int range e1/2-3
IOU1(config-if-range)#channel-Group 4 MOde active
Creating a port-channel interface Port-channel 4

IOU1(config-if-range)#int range e2/0-1
IOU1(config-if-range)#channel-Group 5 MOde active
Creating a port-channel interface Port-channel 5

IOU1(config-if-range)#
*Jun  4 14:30:13.856: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet
0, changed state to down
*Jun  4 14:30:13.865: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet
1, changed state to down
*Jun  4 14:30:13.865: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet
2, changed state to down
```

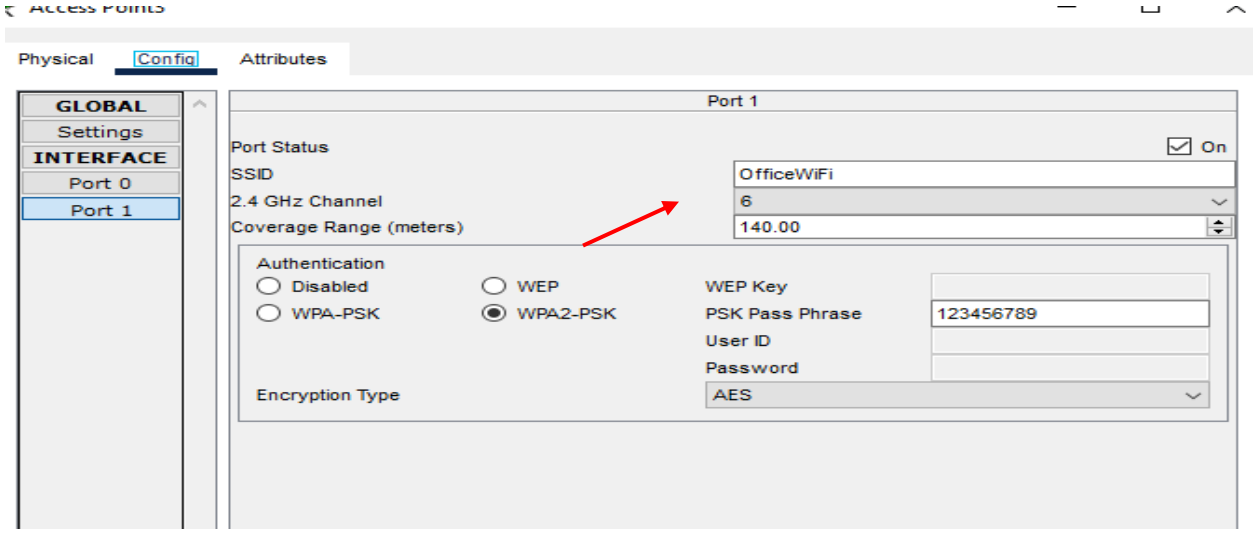
Four ether channels

configuration

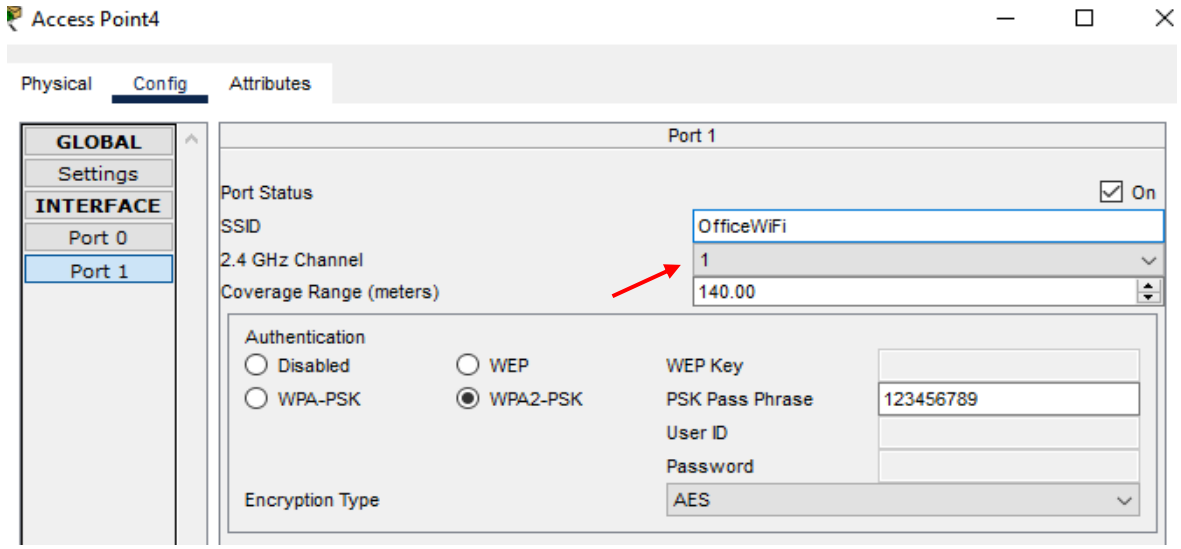
```
        A - formed by Auto LAG


Number of channel-groups in use: 4
Number of aggregators:           4

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)         LACP      Et0/0(P)    Et0/1(P)
2      Po2(SU)         LACP      Et0/2(P)    Et0/3(P)
3      Po3(SU)         LACP      Et1/0(P)    Et1/1(P)
4      Po4(SU)         LACP      Et1/2(P)    Et1/3(P)

IOU7#
```

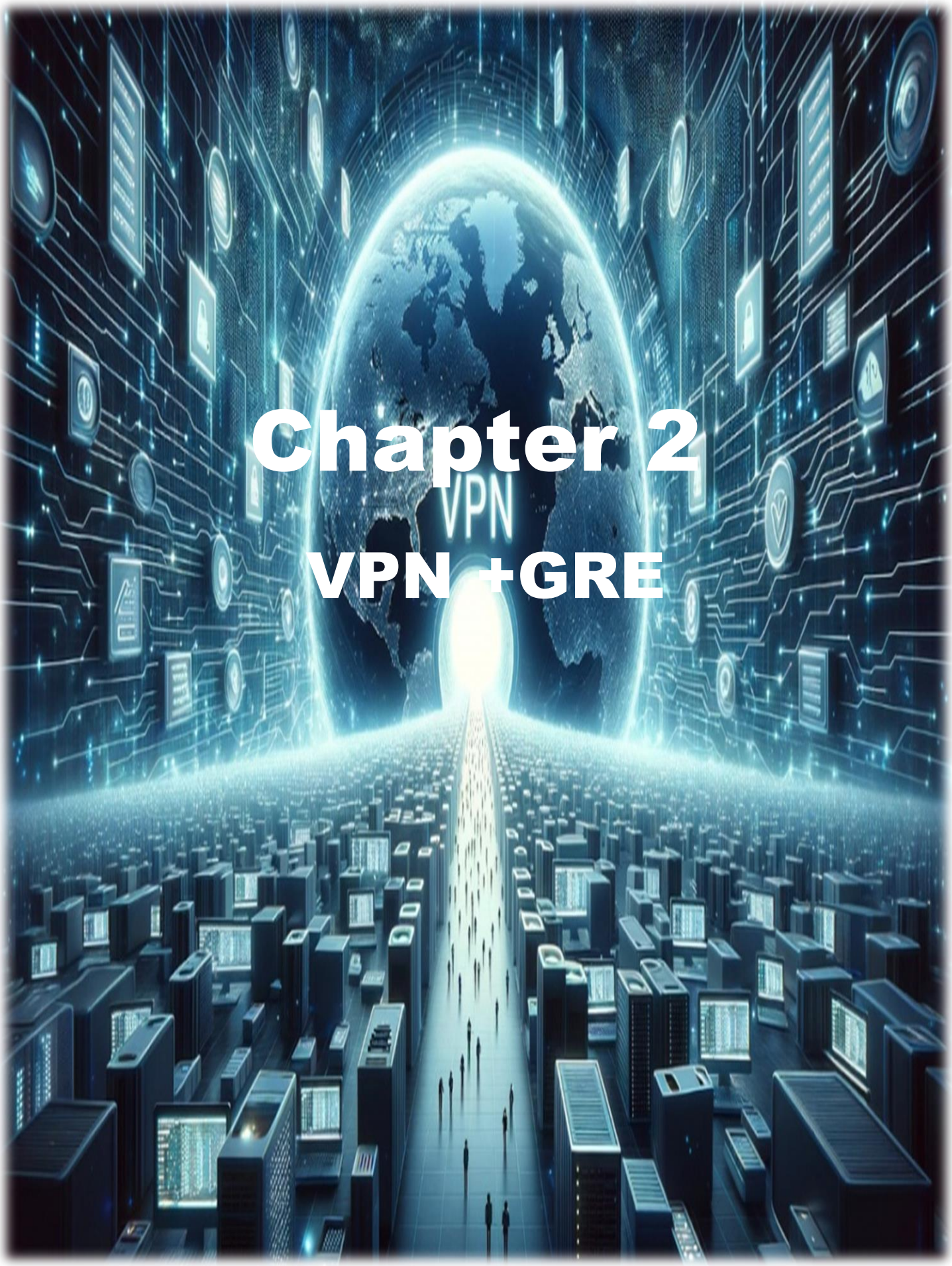
1.9. Wireless Network

In this project, we used multiple Access Points (APs) on each floor, each with the same settings, so that a device can automatically connect to the network on any floor. However, we changed the channel for each one to prevent interference.



with each one having the same name, security type, and password. Only the channel was changed to avoid interference.




Chapter 2
VPN
VPN +GRE

VPN (Virtual Private Network)

What is VPN ?

A **virtual private network** (**VPN**) is a mechanism for creating a secure connection between a computing device and a computer network, or between two networks, using an insecure communication medium such as the public Internet.

VPN function

1. Confidentiality
2. Authentication
3. Integrity
4. anti replay

What is asymmetric encryption?

Asymmetric encryption uses the notion of a key pair: a different key is used for the encryption and decryption process. One of the keys is typically known as the private key and the other is known as the public key.

The private key is kept secret by the owner and the public key is either shared amongst authorised recipients or made available to the public at large. Data encrypted with the recipient's public key can only be decrypted with the corresponding private key. Data can therefore be transferred without the risk of unauthorised or unlawful access to the data.

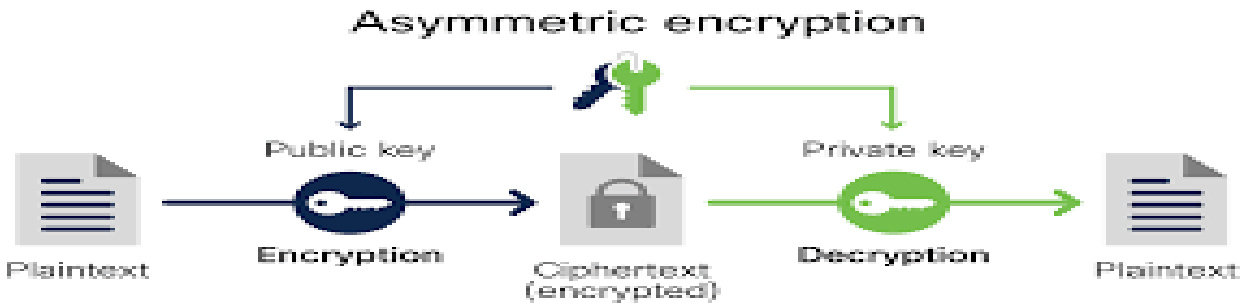


Figure 1-symmetric encryption

There are several encryption algorithms used in Virtual Private Networks (VPNs) to ensure the confidentiality and security of data. Here are some common types of encryption used in VPNs:

1. **AES (Advanced Encryption Standard):**
2. **DES (Data Encryption Standard):**
3. **3DES (Triple DES):**
4. **RSA (Rivest–Shamir–Adleman):**
5. **IPsec (Internet Protocol Security)**

GRE(Generic Routing Encapsulation)

GRE tunnels

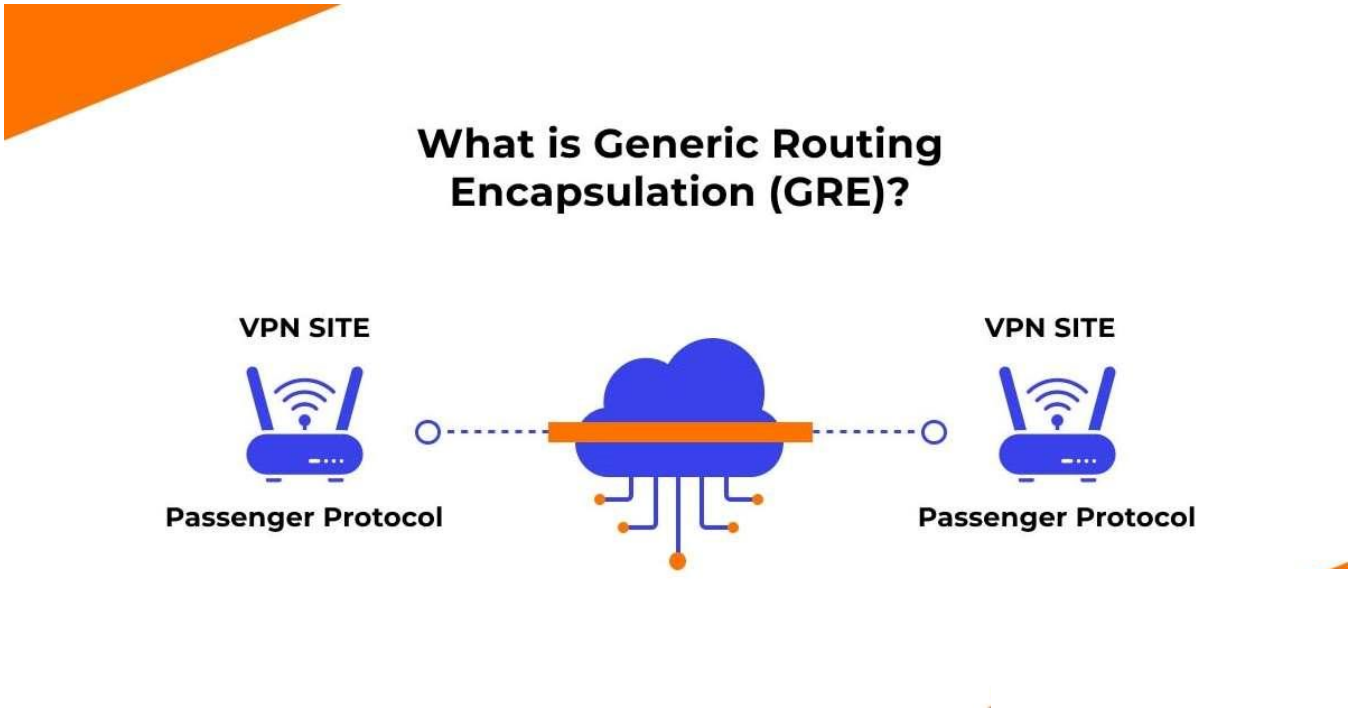


Figure 2-tunnels

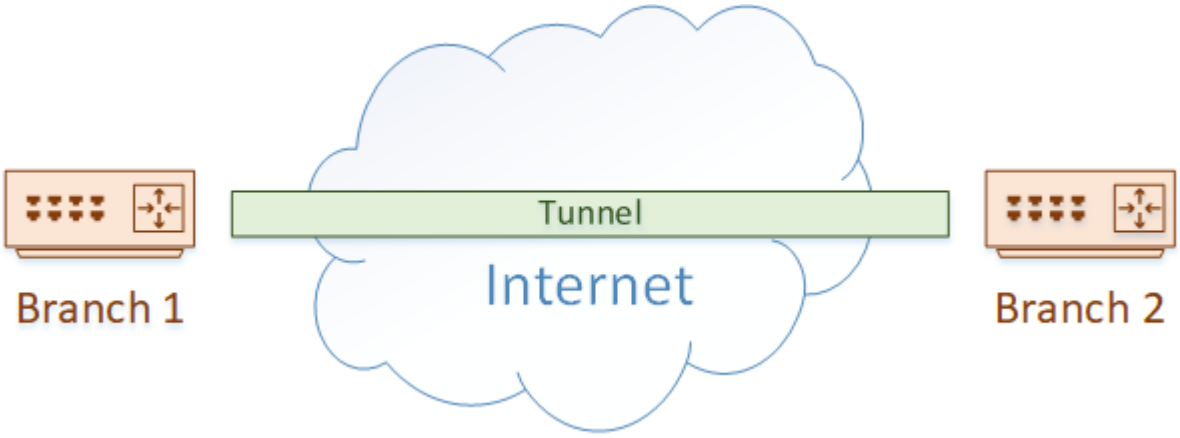
Introduction:

Generic Routing Encapsulation (GRE) is a tunneling protocol developed by Cisco Systems that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links or point-to-multipoint links over an Internet Protocol network.

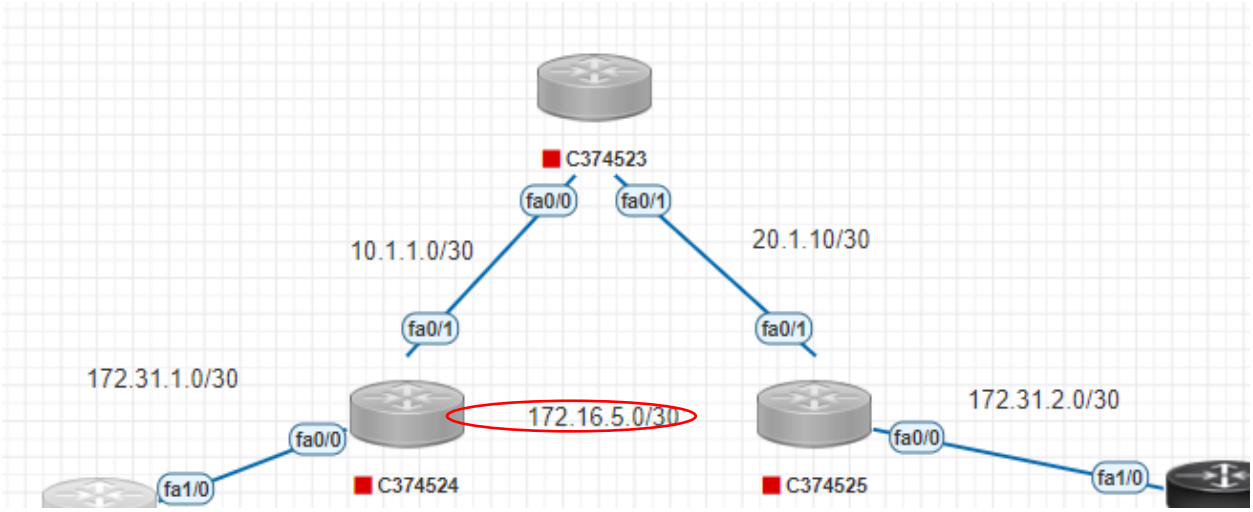
When you want to join two networks together, one option you may investigate is a tunnel. GRE, or Generic Routing Encapsulation, is one of the technologies that we use to build these tunnels.

A great example of this is when you have two branch offices, which are separated by the internet. They may decide to build a GRE tunnel across the internet to provide connectivity

RE is not the only method of tunnelling, but it does have some advantages over some other technologies. For one, it is defined in RFC2784, so any vendor can support it. Also, it supports multicast packets, which means it can be used with dynamic routing protocols (unlike IPSec tunnels for example).



GRE Configuration



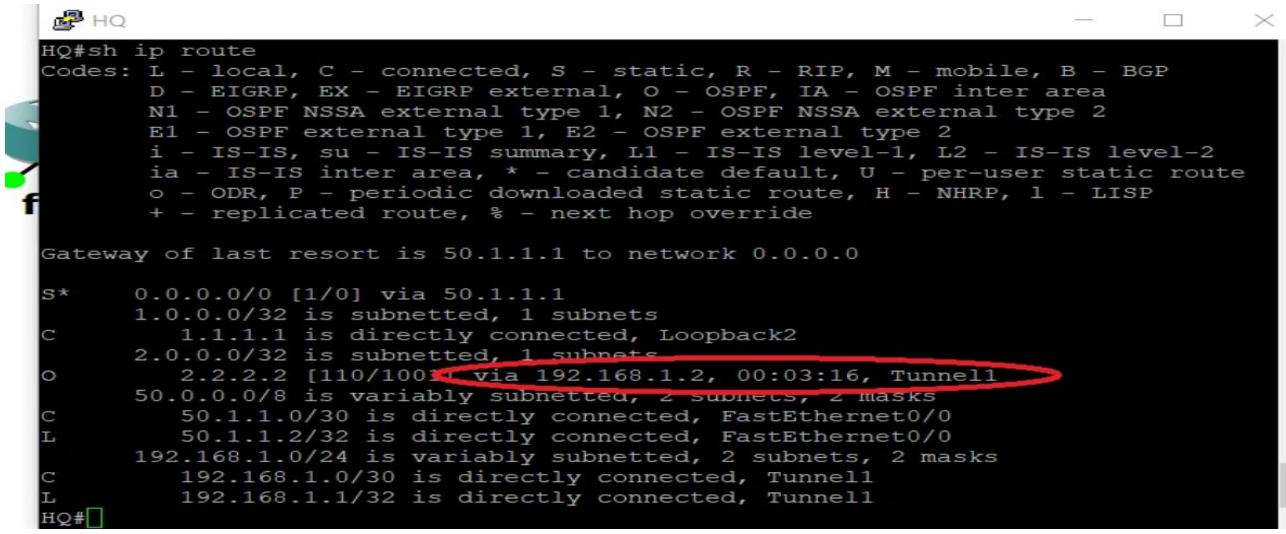
Branch router

```
R1(config-if)#no sh
R1(config-if)#ip add 172.16.5.2 255.255.255.252
R1(config-if)#tunnel source 20.1.1.2
R1(config-if)#io ospf 1 ar 0
               ^
% Invalid input detected at '^' marker.

R1(config-if)#tunnel destination 10.1.1.2
R1(config-if)#
R1(config-if)#
R1(config-if)#int tunnel 1
R1(config-if)#no sh
R1(config-if)#ip add 172.16.5.2 255.255.255.252
R1(config-if)#tunnel source 20.1.1.2
R1(config-if)#ip ospf 1 ar 0
R1(config-if)#tunnel destination 10.1.1.2
R1(config-if)#
```

HQ router

```
R1#
R1#
R1#
R1#
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int tunnel 1
R1(config-if)#no sh
R1(config-if)#ip add 172.16.5.1 255.255.255.252
R1(config-if)#tunnel source 10.1.1.2
R1(config-if)#tunnel destination 20.1.1.2
R1(config-if)#
*Mar  1 00:01:25.807: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, c
hanged state to down
R1(config-if)#
```

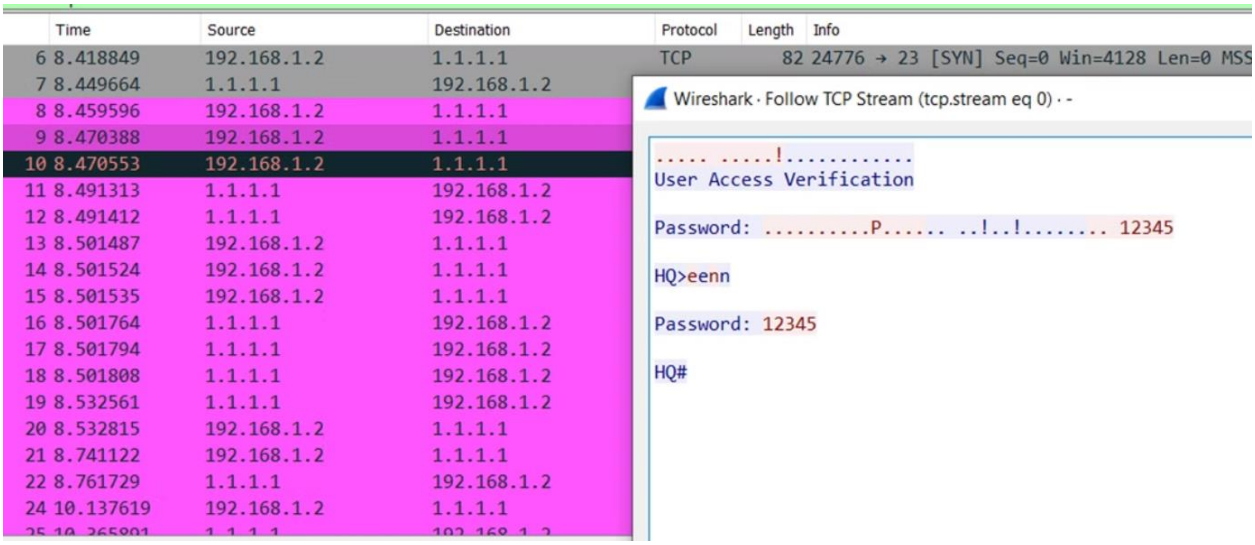
Show routing table (HQ)



Disadvantage of GRE:

Lack of Security Features:

GRE does not inherently provide encryption or security features. If secure communication is required, additional protocols such as IPsec need to be implemented in conjunction with GRE



IPSec configuration

To configure IPSec, it is done in two stages

Phase 1: isakmp

This stage is responsible for securing the tunnel.

Phase 2: IPSec

This stage is responsible for encrypting and securing the data.

Phase 1: isakmp (HQ)

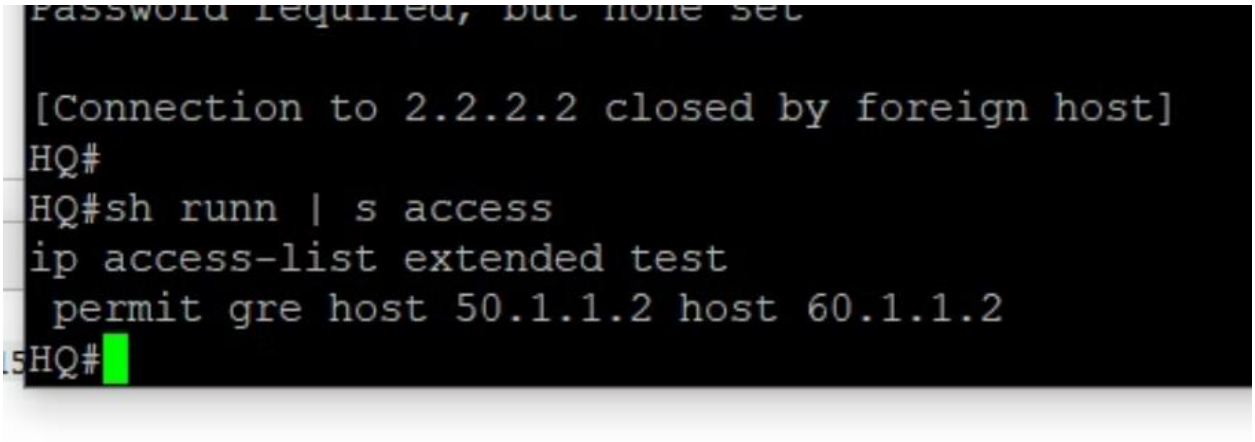
```
R9(config-isakmp)# encr aes 256
R9(config-isakmp)# authentication pre-share
R9(config-isakmp)# group 5
R9(config-isakmp)#
R9(config-isakmp)#crypto isakmp key 12345 address 20.1.1.2
R9(config)#
R9(config)#ip access-list extended abdo-nasser
R9(config-ext-nacl)#permit gre host 10.1.1.2 host 20.1.1.2
R9(config-ext-nacl)#
R9(config-ext-nacl)#$c transform-set abdo esp-sha-hmac esp-aes ah-sha-hmac
R9(cfg-crypto-trans)#crypto map abdo-nasser 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R9(config-crypto-map)# set peer 20.1.1.2
R9(config-crypto-map)# set transform-set abdo
R9(config-crypto-map)# match address abdo-nasser
R9(config-crypto-map)#int f0/0
R9(config-if)#cry map abdo-nasser
R9(config-if)#
*Mar  1 00:01:15.747: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R9(config-if)#
*Mar  1 00:01:22.979: %CRYPTO-4-RECVD_PKT_NOT_IPSEC: Rec'd packet not an IPSEC p
acket. (ip) vrf/dest_addr= /10.1.1.2, src_addr= 20.1.1.2, prot= 47
R9(config-if)#
```

Phase 1: isakmp (Branch) must match

Branch-Router

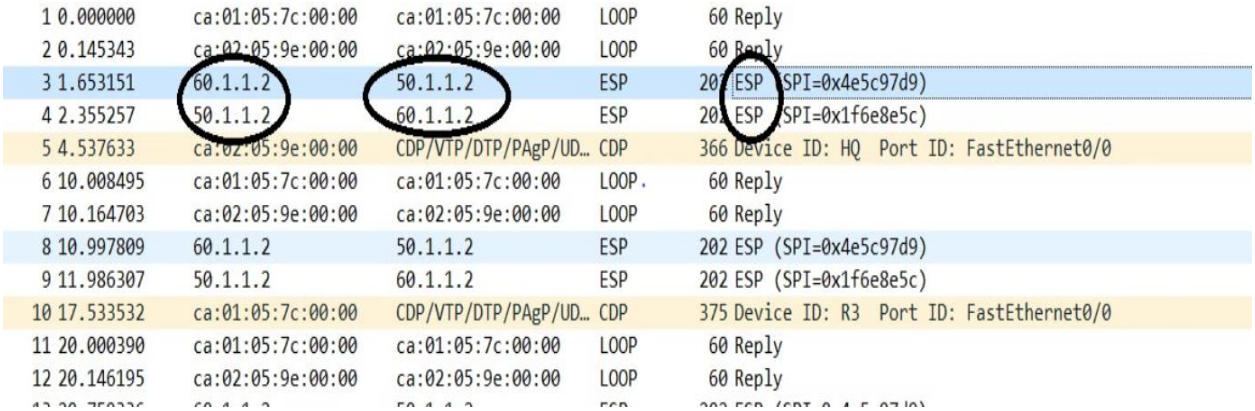
```
R8(config-isakmp)# encr aes 256
R8(config-isakmp)# authentication pre-share
R8(config-isakmp)# group 5
R8(config-isakmp)#
R8(config-isakmp)#crypto isakmp key 12345 address 10.1.1.2
R8(config)#
R8(config)#ip access-list extended abdo-nasser
R8(config-ext-nacl)#permit gre host 20.1.1.2 host 10.1.1.2
R8(config-ext-nacl)#
R8(config-ext-nacl)#$c transform-set abdo esp-sha-hmac esp-aes ah-sha-hmac
R8(cfg-crypto-trans)#crypto map abdo-nasser 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R8(config-crypto-map)# set peer 10.1.1.2
R8(config-crypto-map)# set transform-set abdo
R8(config-crypto-map)# match address abdo-nasser
R8(config-crypto-map)#int f0/0
R8(config-if)#cry map abdo-nasser
R8(config-if)#
*Mar  1 00:02:21.351: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R8(config-if)#
*Mar  1 00:02:33.263: %OSPF-5-ADJCHG: Process 1, Nbr 172.31.1.1 on Tunnel1 from
LOADING to FULL, Loading Done
R8(config-if)#
```

Interesting traffic(HQ)



Activation (HQ-Brach)

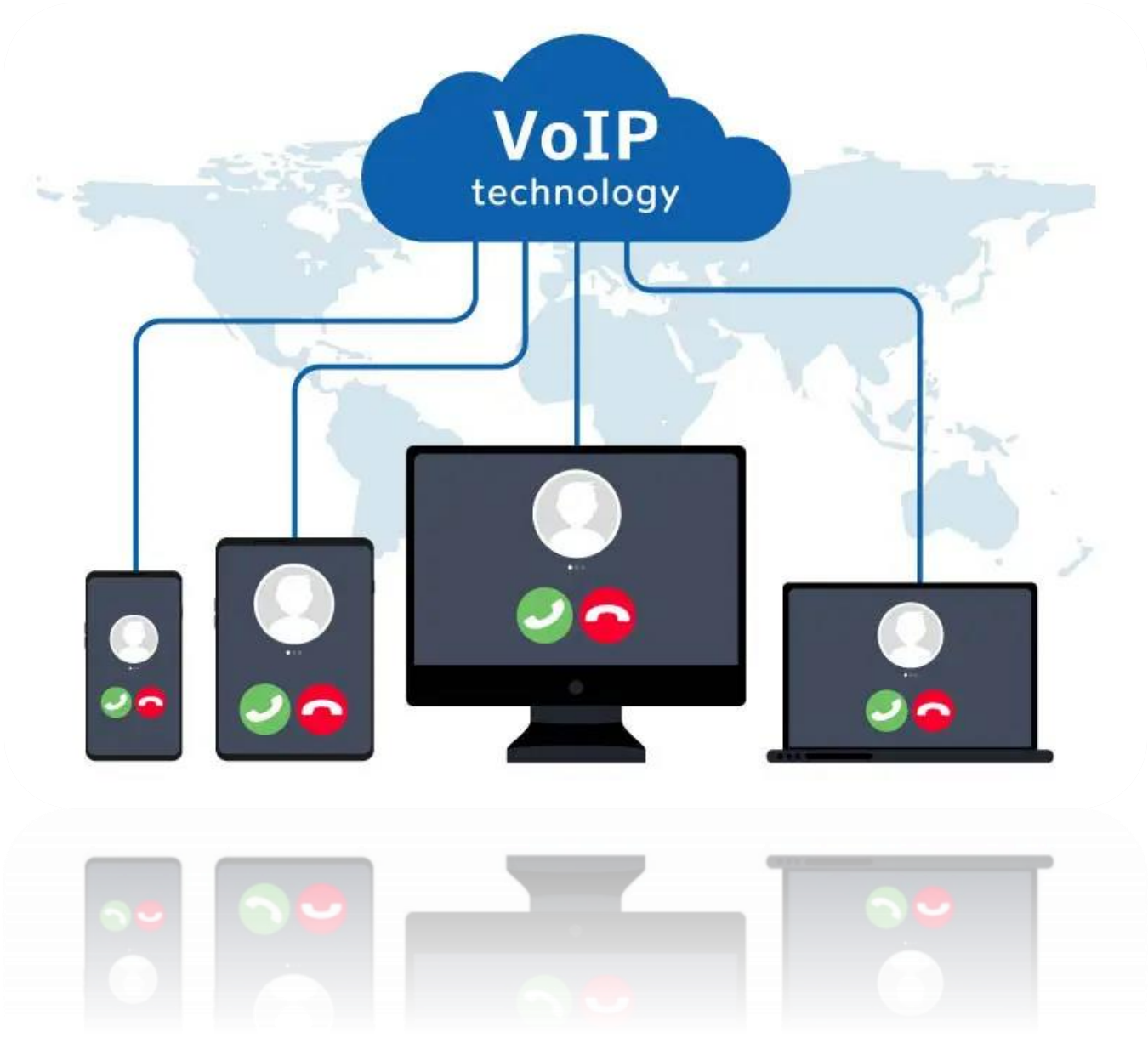
After ipsec



Chapter 3

VOIP

Voice Over Internet protocol



VOIP

Voice-over-Internet protocol (VoIP) is communications technology that allows users to interact by audio through an Internet connection, rather than through an analog connection. Voice-over-Internet Protocol converts the voice signal used in traditional phone technology into a digital signal that travels through the Internet instead of through analog telephone lines.

KEY TAKEAWAYS

- Voice-over-Internet protocol (VoIP) is a technology that lets users make calls using a broadband Internet connection instead of a standard phone line.
- VoIP technology converts the voice signal used in traditional phone calls into a digital signal that travels via the Internet rather than analog phone lines.
- Because calls are being made over the Internet, they are essentially free when made wherever the Internet is available.
- The traditional telephone industry was hit hard by the VoIP boom, with many users abandoning it as some of its services have become nearly obsolete.
- During the COVID-19 pandemic, VoIP became essential to modern workplaces as telecommuting replaced the office.

Understanding Voice-Over-Internet Protocol (VoIP)

Voice-over-Internet-Protocol (VoIP) technology allows users to make "telephone calls" through Internet connections instead of through analog telephone lines, which renders these calls effectively free wherever the Internet is available. VoIP changed the telecommunications industry by making traditional phone lines and services nearly obsolete and reducing demand for them significantly.

As access to the Internet has become more widely available, VoIP has become ubiquitous both for personal use and for business use

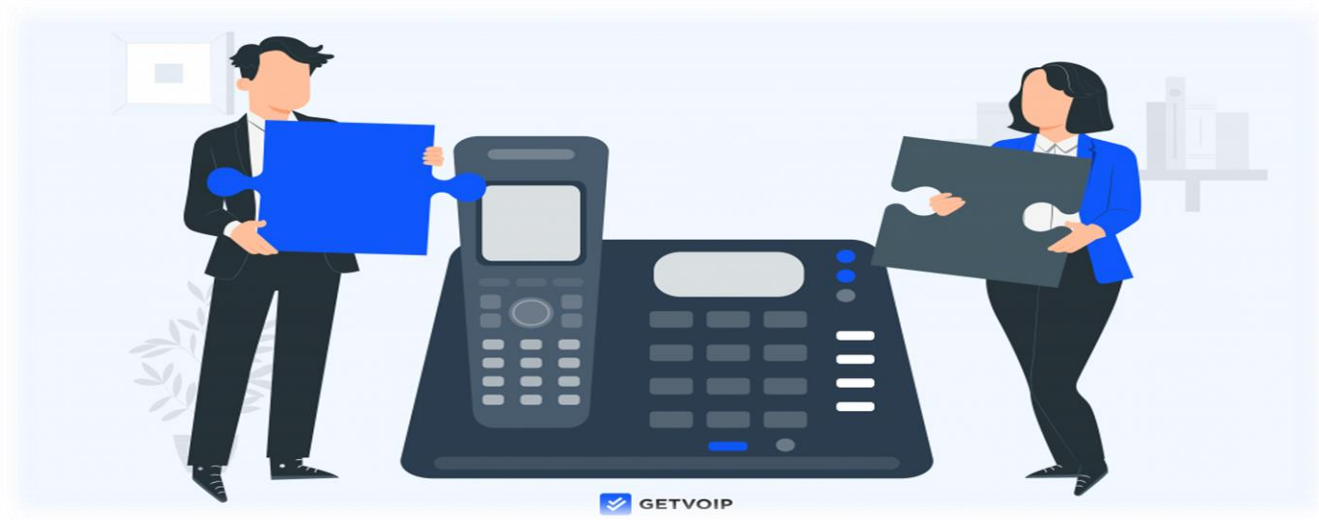


Figure 3-VOIP

What is a VoIP Number?

Also known as a virtual phone number, a VoIP number is a telephone number that is assigned to a specific user, rather than a specific phone line.

We have already observed that voice-over IP is largely a location-independent system. Area codes have no particular relevance to VoIP phone numbers. In fact, VoIP users can choose a phone number with any area code. This enables businesses to establish a local presence in different regions, which can be very lucrative for businesses.

Essential components for VoIP calling

While there are many ways in which a VoIP phone system can be implemented — on-prem, cloud, or hybrid — the basic components that drive the whole system remain the same. Here are the most essential components of a VoIP phone system:

VoIP Server:

This is the backbone of a VoIP phone system. The VoIP server routes all incoming, outgoing and internal calls made to or from an organisation. This can either be hosted on the cloud or it can be on-prem. With Exotel, you don't have to worry about purchasing a VoIP server.

VoIP Enabled Endpoints:

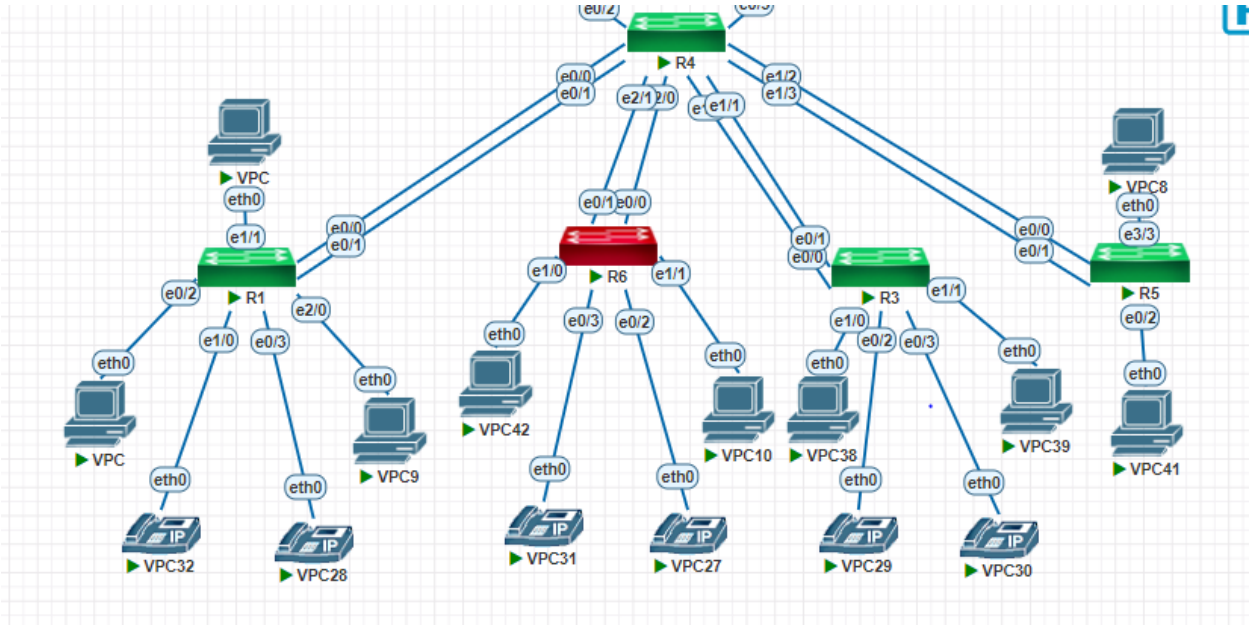
These are required to enable VoIP communication. There are different types of VoIP phones:

- **VoIP phone:** Specialized phones made for VoIP communication.
- **Softphone:** A softphone is a piece of software installed on a computer/smartphone that allows the device to make and receive VoIP calls. The software installed is called a SIP client and it can be installed on any computer/smartphone. Zoiper, Linphone, etc are some of the most commonly used softphones.
- **Analogue phone with a VoIP adapter:** VoIP adapters can be used to enable VoIP communication over analogue phones. This is used when a business already has PBX infrastructure.

A Stable Internet Connection:

Since all the calls are made over the internet, it goes without saying that a good internet connection with sufficient bandwidth is required for VoIP calls.

VOIP topology



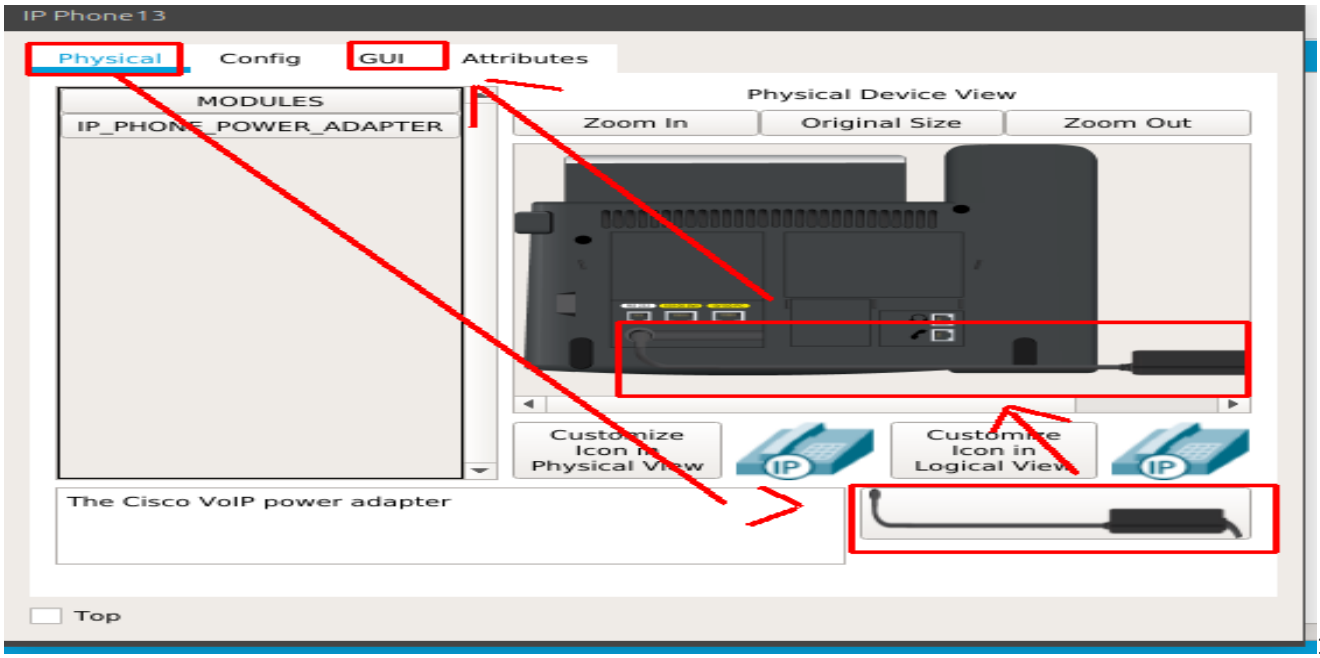
CM configuration

```
R1
R1#
R1#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#telephony-service
R1(config-telephony)#max-ephones 20
R1(config-telephony)#max-dn 20
R1(config-telephony)#ip source-address 172.16.1.1 port 2000
%Error deleting flash:SEPDEFAULT.cnf (No device available)
%Error deleting flash:XMLDefault.cnf.xml (No device available)
R1(config-telephony)#exit
R1(config)#ephone-dn 1
R1(config-ephone-dn)#number 101
R1(config-ephone-dn)#ephone-dn 2
R1(config-ephone-dn)#number 102
R1(config-ephone-dn)#ephone-dn 3
R1(config-ephone-dn)#number 103
R1(config-ephone-dn)#exit
R1(config)#ephone 1
R1(config-ephone)#type 7960
R1(config-ephone)#button 1:1
Need to configure ephone mac address or VM station-id
R1(config-ephone)#ephone 1
R1(config-ephone)#
```

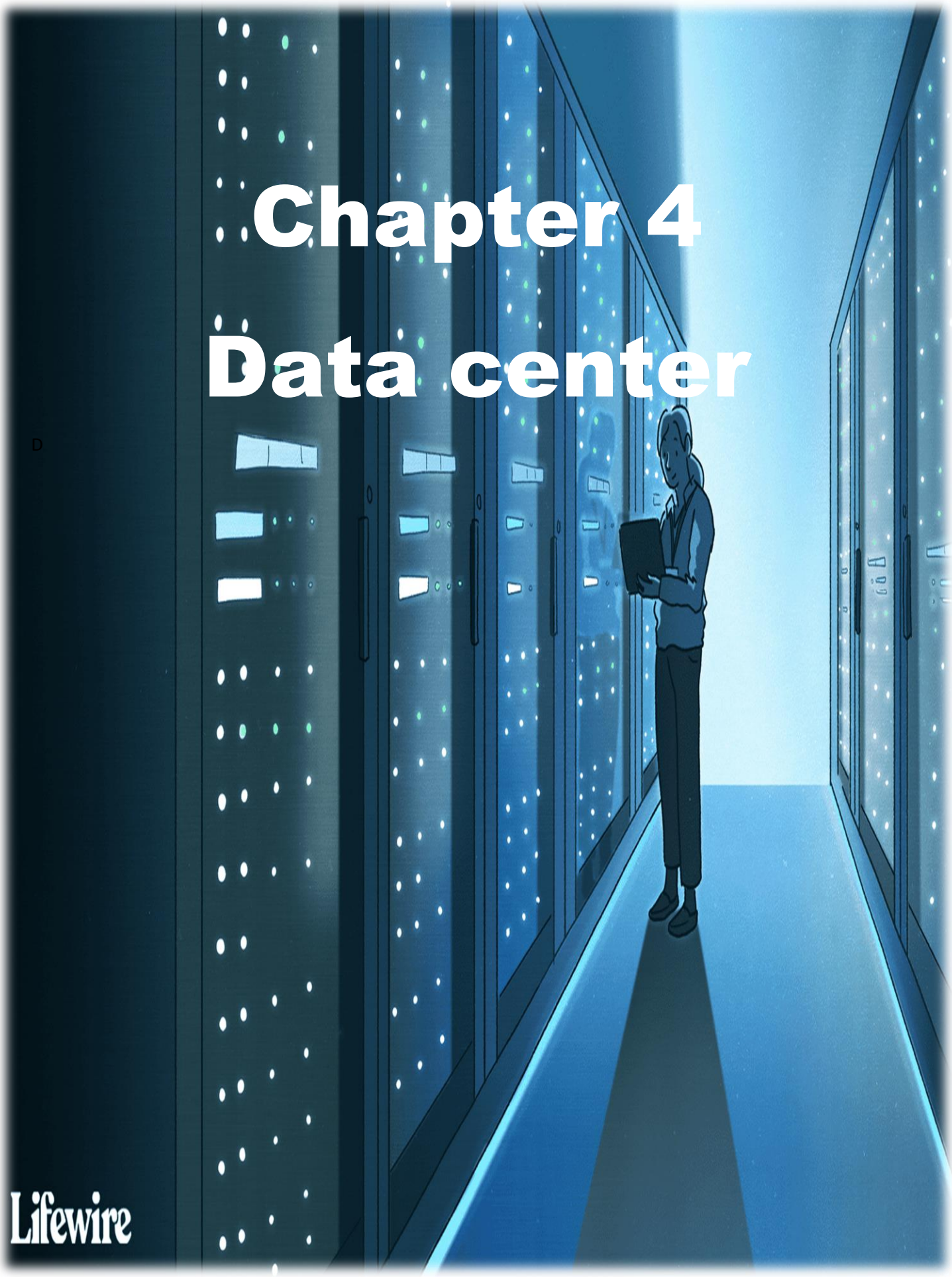
Call 102

101 calls

Ip phone



1


Chapter 4
Data center
Lifewire

Servers implemented on Linux OS: -

(1) File Transfer Protocol (FTP) Server:

FTP is a mature protocol that allows data files to be exchanged between computers over a TCP/IP network.

- Implementation:

	Command	Description
Server Machine	yum install vsftpd	to install the service.
	systemctl start vsftpd	to start the daemon for service.
	systemctl enable vsftpd	to make it start automatically on booting.
	firewall-cmd --list-all	to check the firewall allowed services and ports.
	firewall-cmd --permanent --add-port=21/tcp	allowing port 21 on firewall.
	firewall-cmd --permanent --add-service=ftp	allowing service on firewall.
	firewall-cmd --reload	to restart the firewall.
	From /etc/vsftpd/vsftpd.conf anonymous_enable=NO local_enable=YES write_enable=YES local_umask=022 connect_from_port_20=YES ftpd_banner=Welcome to FTP Server. data_connection_timeout=120 idle_session_timeout=600 chroot_local_user=YES	

	chroot_list_file=/etc/vsftpd/chroot_list allow_writeable_chroot=YES	
	From /etc/vsftpd/chroot_list	the file in which the local user will be on it to restrict them from travelling through the file system.
	From /etc/vsftpd/ftpusers	the file in which the users can't login to ftp server.
	setenforce 0	to disable the selinux.
	systemctl restart vsftpd	to restart the service so the changes be implemented.
Client Machine	yum install ftp	to install the service.
	ftp [server ip]	to connect on the server from client.
	ftp> get [file name]	to download files from the server.
	ftp> put [file name]	to upload files to the server.

(2) Network File System (NFS) Server: -

Network File System (NFS) is a distributed file system that allows various remote systems to access a file share.

- Implementation:

	Command	Description
Server Machine	yum install nfs-utils	to install the service.
	systemctl enable nfs	to make it start automatically on booting.
	systemctl start nfs	to start the service.
	systemctl status nfs.service	to check the status of the service.

	netstat -ntlp	to show the ports that nfs listen on and other services.
	mkdir nfs_share_dir	creating directory from which we will share files.
	From /etc/exports /root/nfs_share_dir * (rw)	that means share this directory with anyone with permission read and write.
	exportfs -r	to referesh the service without restarting it.
	firewall-cmd --add-service=nfs --permanent firewall-cmd --add-service=rpc-bind --permanent firewall-cmd --add-service=mountd –permanent	to make firewall allow the services.
	ls -ld /root/nfs_share_dir	to test the other part permission on the directory.
	chmod o+w /root/nfs_share_dir	to change the other part permission to allow write so the clients can touch files when accessing the server.
Client Machine	showmount -e 192.168.1.76	to connect to the server.
	mount -t nfs 192.168.1.76:/root/nfs_share_dir/ /srv/	to mount the files (nfs + server ip + the file or dir path + the location to be mounted in).
	df -h	to test if the mounted has done.
	cd /srv/ [root@client srv]# touch file1	the client can touch files on the location he mounted on it.
	From /etc/fstab 192.168.1.76:/root/nfs_share_dir/ /srv/ nfs defaults,_netdev 0 0	to make the mount permanent.

	umount /srv/	to unmount the share.

(3) Apache Web Server :-

Apache powers the behind-the-scenes aspects of serving your website's files to visitors.

- Implementation:

	Command	Description
Server Machine	yum install httpd yum install httpd-manual yum groupinstall "Basic Web Server"	to install the service
	systemctl start httpd	to start the service.
	systemctl enable httpd	to make it start automatically on booting.
	systemctl status httpd	to check the status of the service.
	From /var/www/html/ Touch index.html	The path from which it will serve the files.
	firewall-cmd --list-all	to check the firewall allowed services and ports.
	firewall-cmd --add-service=http --permanent	to make firewall allow the service.
	firewall-cmd --reload	to restart the firewall.
	/etc/httpd/conf/httpd.conf	The configuration file of the service.
	/var/log/httpd/access_log	the access log file of the web server.
	/var/log/httpd/error_log	the errors log file of the web server.
Client Machine	From browser search bar: server ip	To connect to the server and view the web pages.

(4) MariaDB Server: -

MariaDB Server is one of the most popular database servers in the world.

-Implementation:

	Command	Description
Server Machine	yum install mariadb-server	to install the service.
	systemctl enable mariadb.service	to make it start automatically on booting.
	systemctl start mariadb.service	to start the daemon for this service.
	systemctl status mariadb.service	to check status of the service.
	mysql_secure_installation	to secure the service with basics.
	mysql -V	to test the installation.
	rpm -ivh https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm yum repolist	to install packages for the service.
	From /etc/my.cnf [mysqld] skip-networking=0 skip-bind-address	To allow remote connection.
	firewall-cmd --permanent --add-port=3306/tcp	To allow remote access on the server.
	mysql -u root -p	to connect to the database from server itself.
	show databases;	to view the databases.
	create database employees;	to create new database.
	use employees;	to deal with one specific database.
	show tables;	to show the tables of used database.

	select * from user\G;	to show the whole content of this table in readable format.
	GRANT ALL PRIVILEGES ON *.* TO 'root'@'192.168.1.%' IDENTIFIED BY '12345' WITH GRANT OPTION;	to give the permissions to database user (root), the first * for database name (all databases) , the second * for table name (all tables) , after @ sign the domain name of the machine that the client will connect to the server from or the client Ip address , and the password for that client (12345).
	FLUSH PRIVILEGES;	to reload users and their privileges.
	mysqldump -u root testdb -p > dbbackup.sql	to back up the database into file.
Client Machine	mysql -h <server_ip> -u <username> -p<password>	to connect from remote machine.

Network Interface Card (NIC) Teaming: -

Network Interface Card (NIC) is a procedure that helps to configure the grouping of physical network adapters to improve our network system performance and redundancy. It is a process of combining multiple network cards together

- Implementation:

Command	Description
nmcli connection show	to view the interfaces on the machine.
nmcli connection add type team con-name team0 ifname team0 config '{"runner": {"name" : "activebackup" } }'	to configure nic teaming with mode active backup.
nmcli connection add type team-slave ifname ens36 con-name team0-slave1 master team0 nmcli connection add type team-slave ifname ens37 con-name team0-slave2 master team0	to assign the interfaces to the team.
nmcli connection modify team0 ipv4.address 192.168.1.82/24 ipv4.method manual	to assign static Ip address for the virtual interface for nic teaming.
nmcli connection delete [UUID or name]	to delete profile name.
nmcli connection down team0	to make the virtual interface down.
nmcli connection up team0 nmcli connection up team0-slave1 nmcli connection up team0-slave2	To make the virtual interface and the two assigned interfaces up.
teamdctl team0 state	to check the state of team0.
teamnl team0 -p ens36 setoption priority 100	to set priority in link so it will be the active one , when it is down it will switch to the other link.

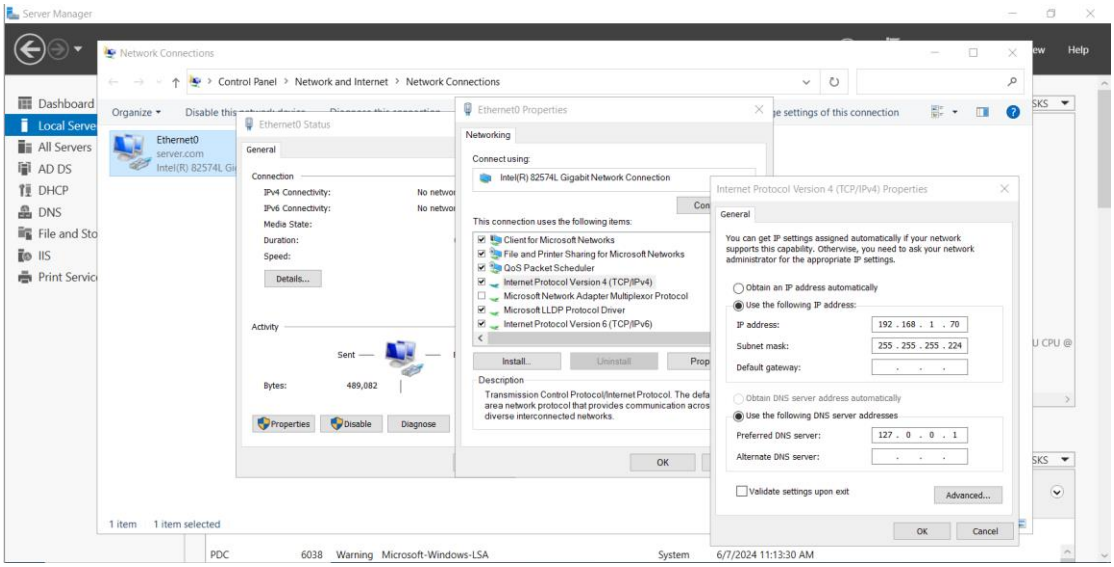
Windows server

In the simplest form, the server is a computer with high capabilities, the most prominent of which is the ability to connect to the Internet at high speed and a continuous source of electricity, in addition to the presence of high cooling systems because it works continuously 24 hours a day, and site data is stored on it. Stopping the server for one minute means that the websites hosted on it have stopped working.

In this context, the basis of our project is the server, and we made a model of the server and what happens inside it on the VMware Workstation by creating a server and clients.

There are many types of servers such as DHCP, DNS, DC, Printer.

We have created a domain server called SERVER.com with an ip of 192.168.1.70 and a computer name PDC.

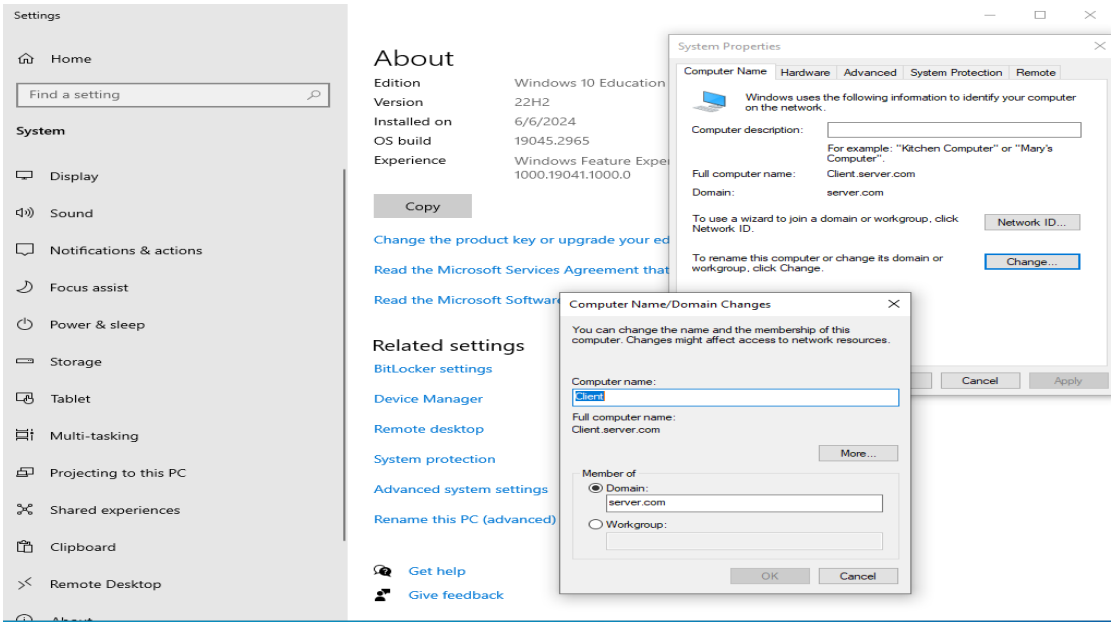


And we have created 4 departments (Doctors and Nurses, IT, Voice, Employees).

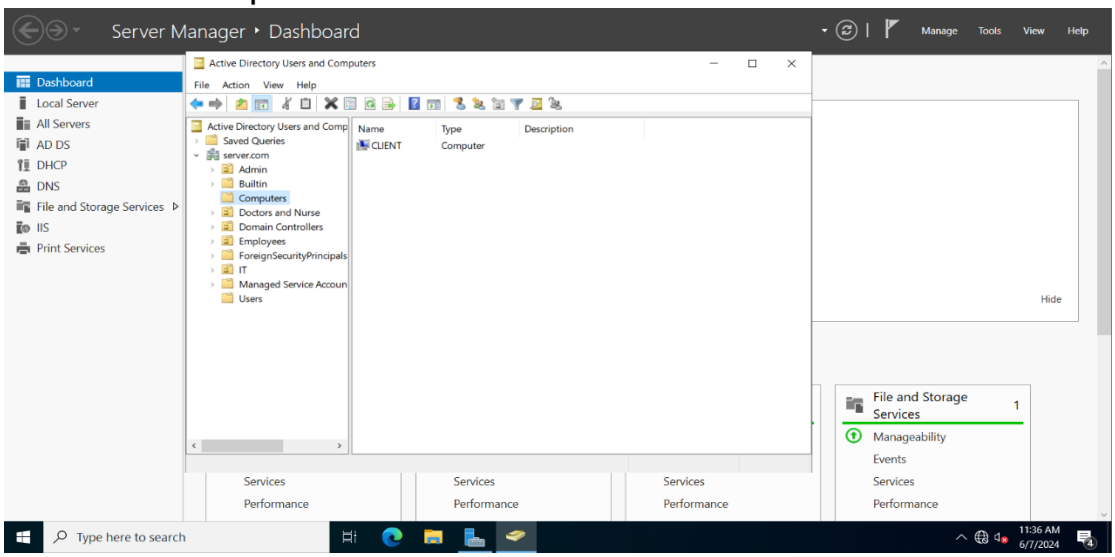
1- Computer name:

After adding the computer to the domain, a computer name will be Client and so onThe name of the computer can be done in two ways:

1-by writing the name of the computer directly in the laptop, and thus it will be automatically created on the server.



2- Login to the server and press on create computer name in active directory users and computer.

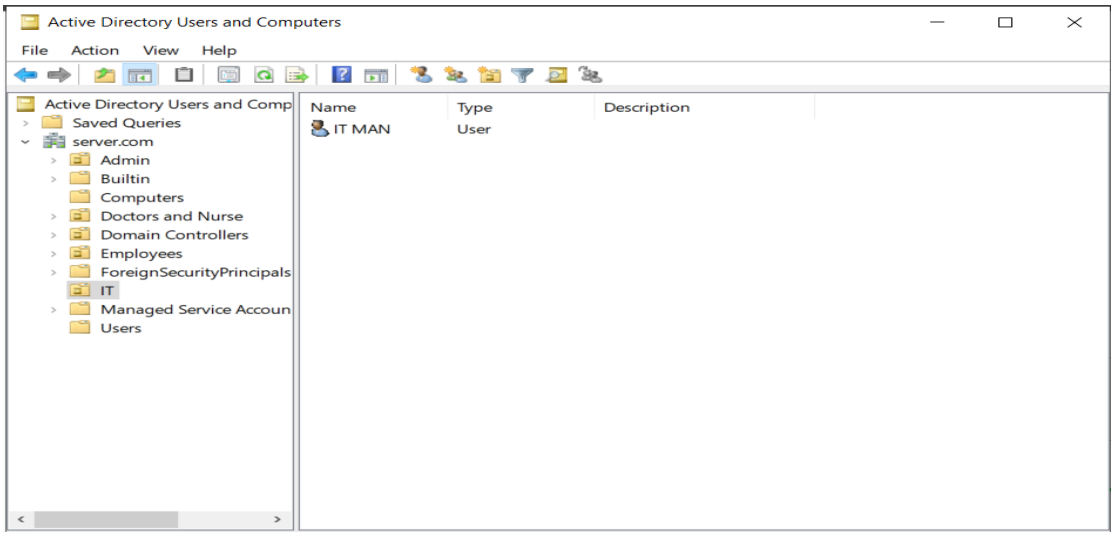


2- groups

To obtain an order in the sections and to facilitate the addition of anything in the server, we will use groups.

For example, when applying a specific policy to a group of people in a specific section, we can dispense with adding one person and adding another, so we can create a group for the department and add all the people in the department to it.

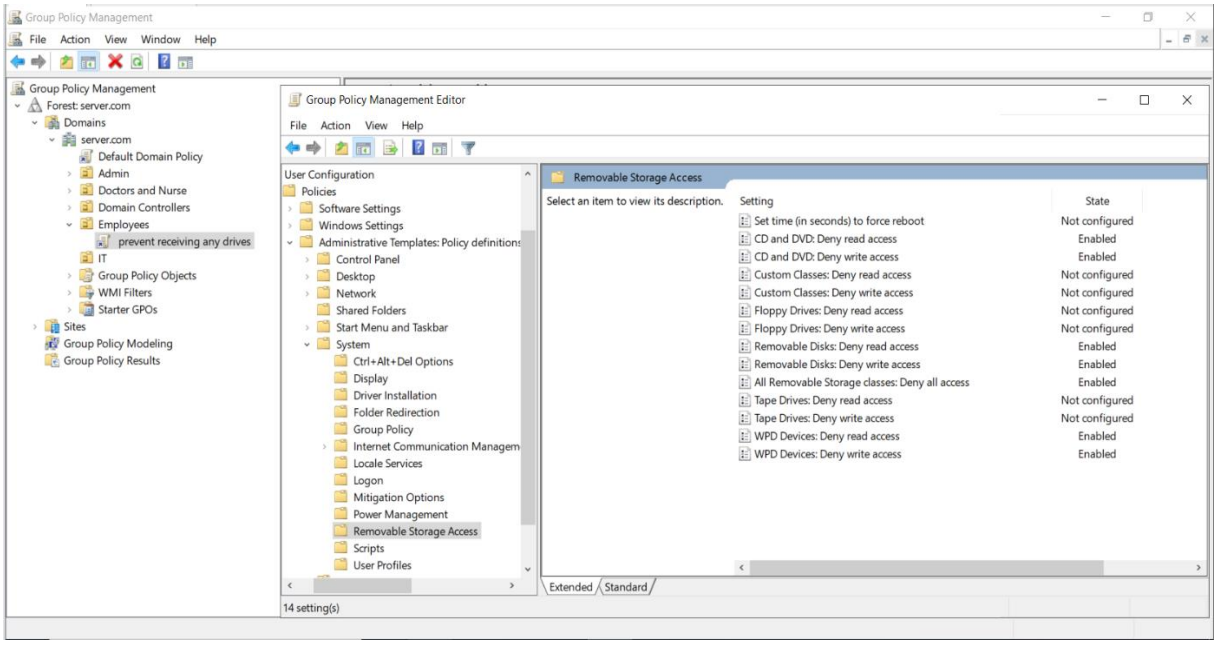
Active Directory users and computers -> click right in server.com -> new group OR we can create new group in any OU

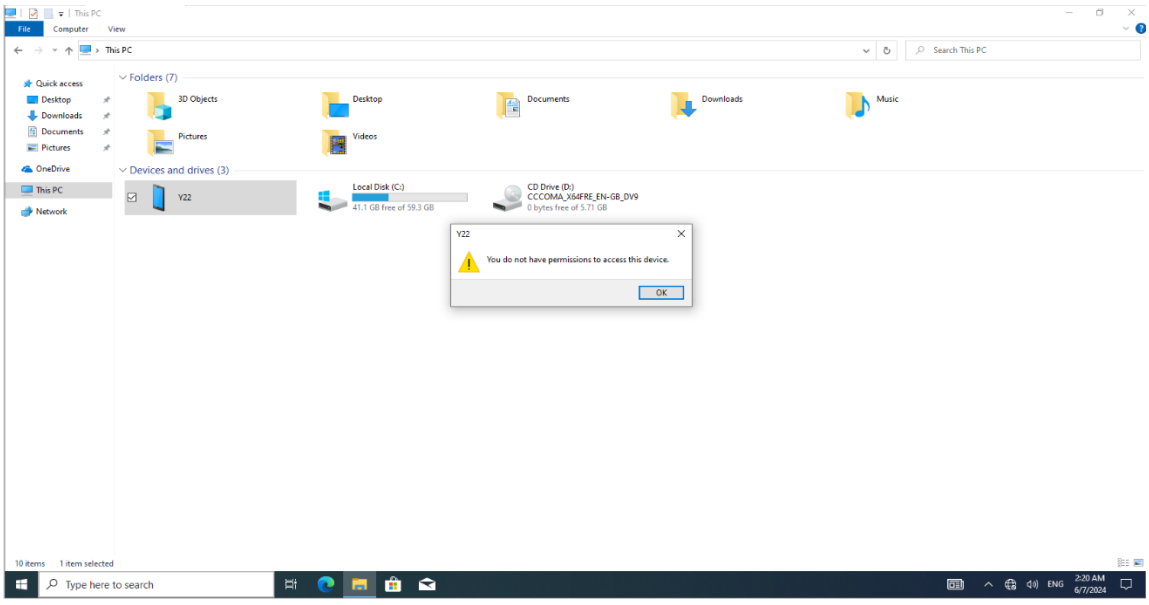


.3) group policy in any company, there must be permissions and rules that must be followed to obtain security, and these permissions and rules apply to users and computers. Here, all the policy that was added will be explained:

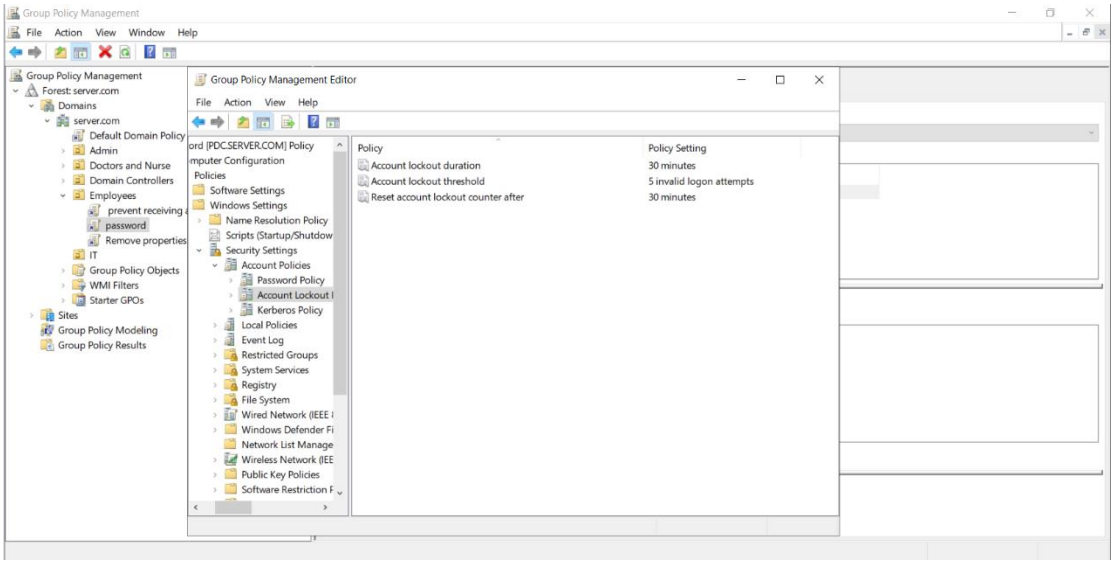
3- Group Policy:

1- Create a policy to prevent receiving any flash drives, CDs, or any inputs in general for finance department

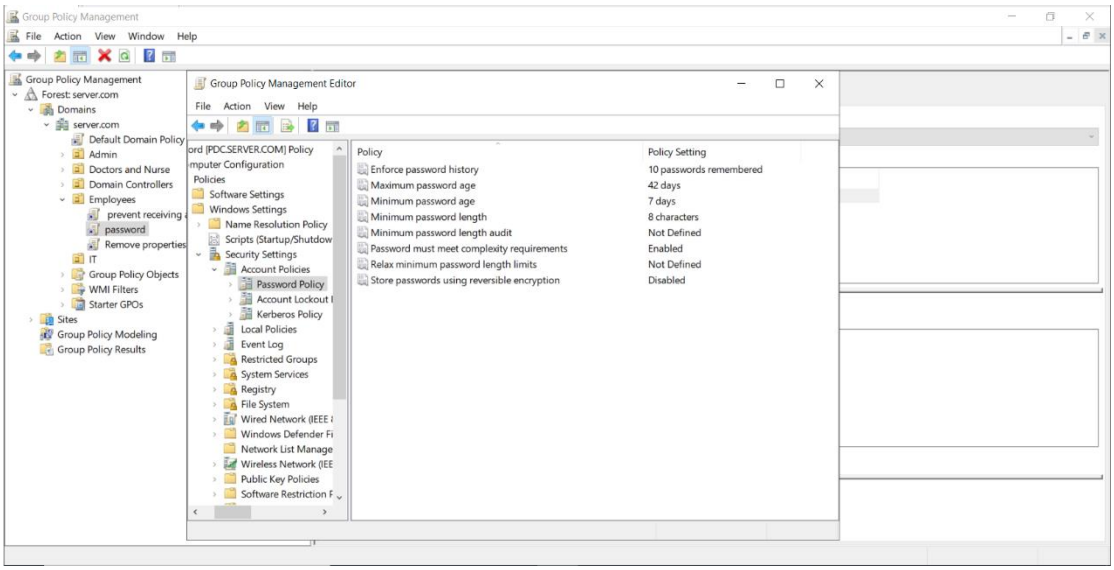




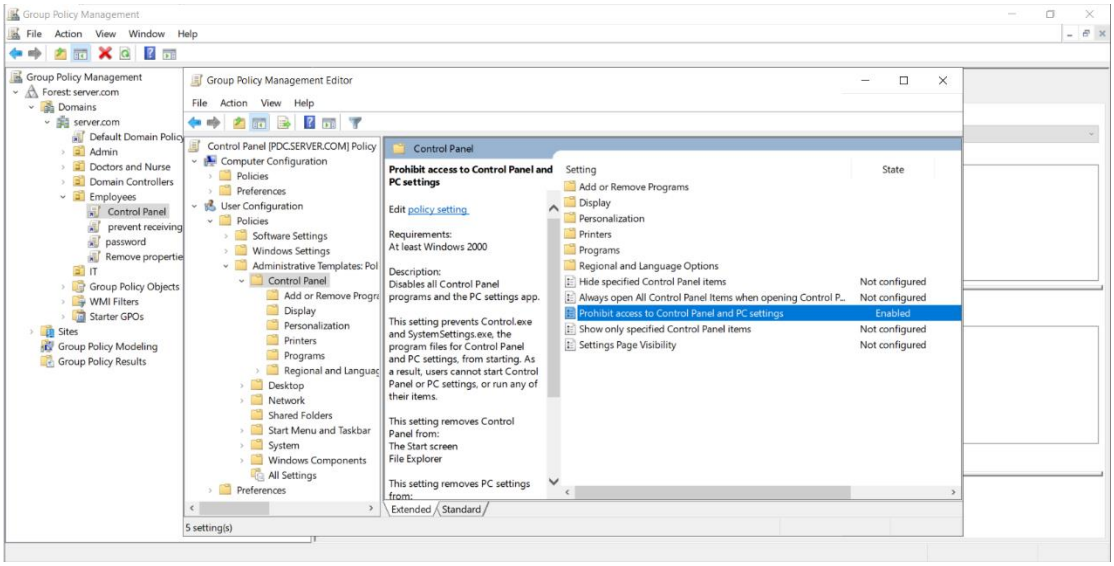
2- Activate the policy at the computer level, that the client cannot guess the password more than 5 times, he cannot write again except after 30 minutes, or if he is in a hurry, he will send an email to it admin and the IT will enter his account and find it closed and unlock.



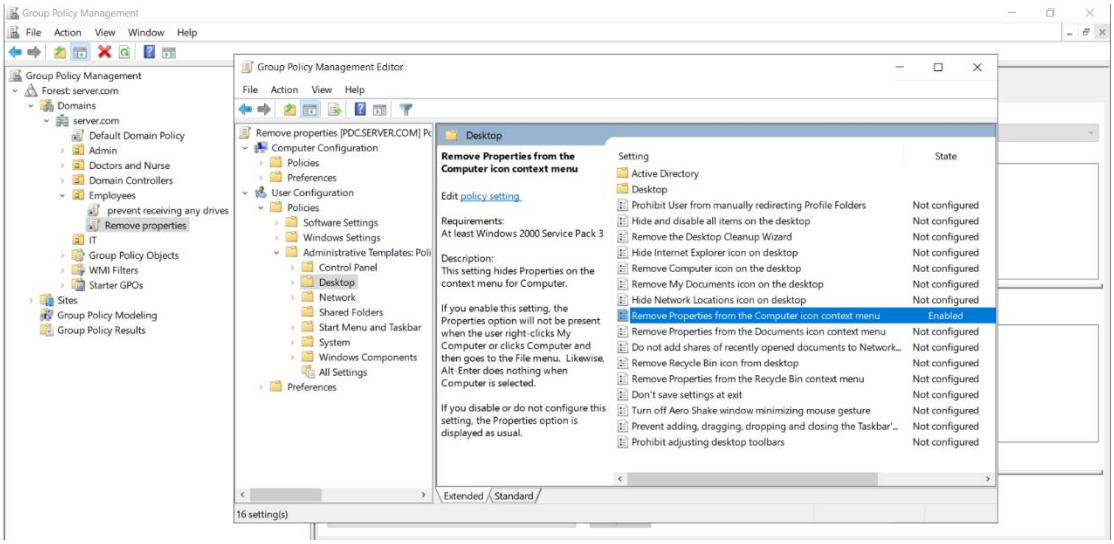
3- To implement security for users, we will make them change the password every 42 days, and this is through a policy that has been activated, and that they do not change the password except after a full day has passed.

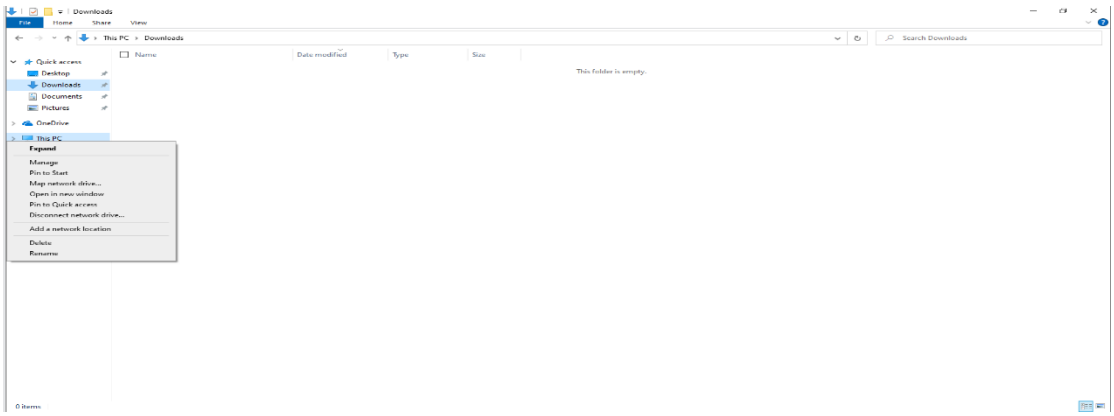


4- Activate the policy not to use Control Panel

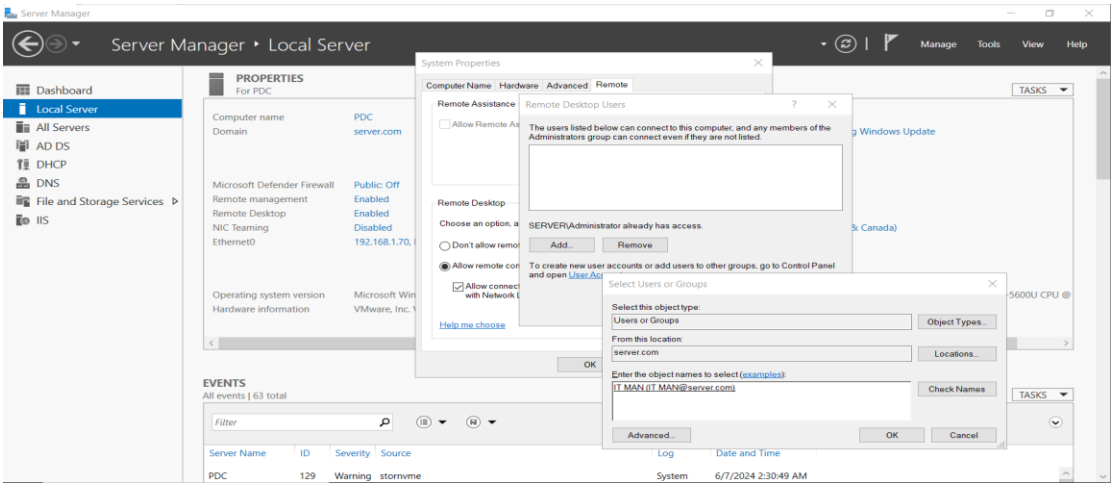


5- Activate the policy not to use Properties



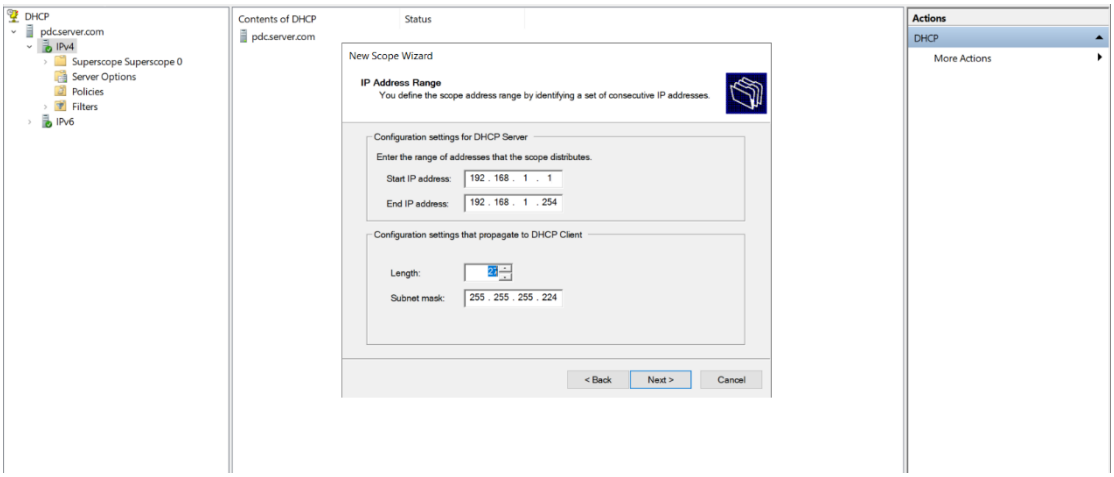


6- There is an addition that we will make to the IT department, which is that they can control the server remotely.

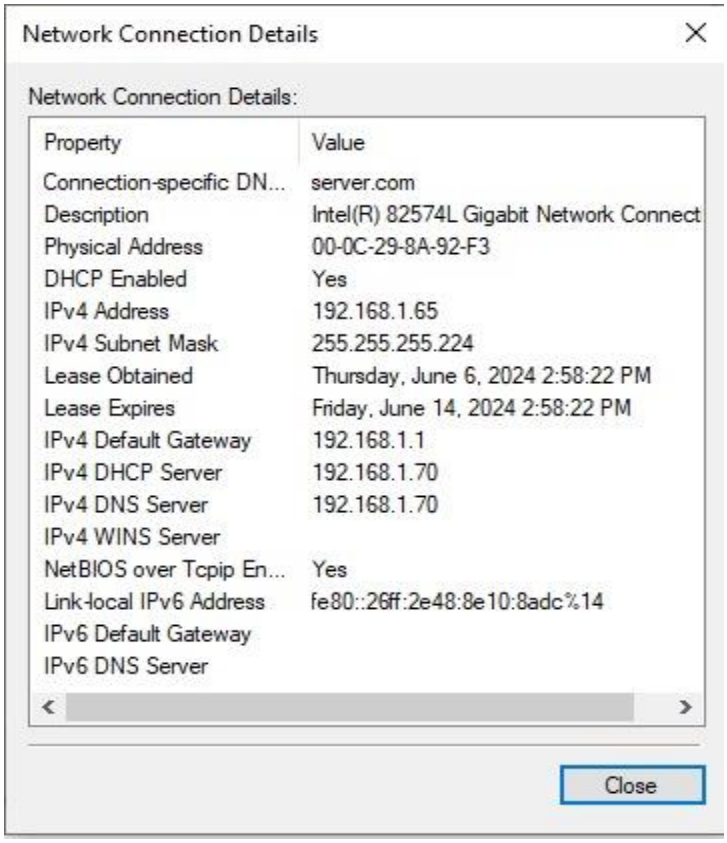


4- DHCP Server:

server A Dynamic Host Configuration Protocol is a network server that automatically provides and assigns IP addresses, default gateways. DHCP servers usually assign each client with a unique dynamic IP address, which changes when the client's lease for that IP address has expired. from tool -> DHCP ->click right in IPv4-> choose new scope -> and give the name of scope like LAN1

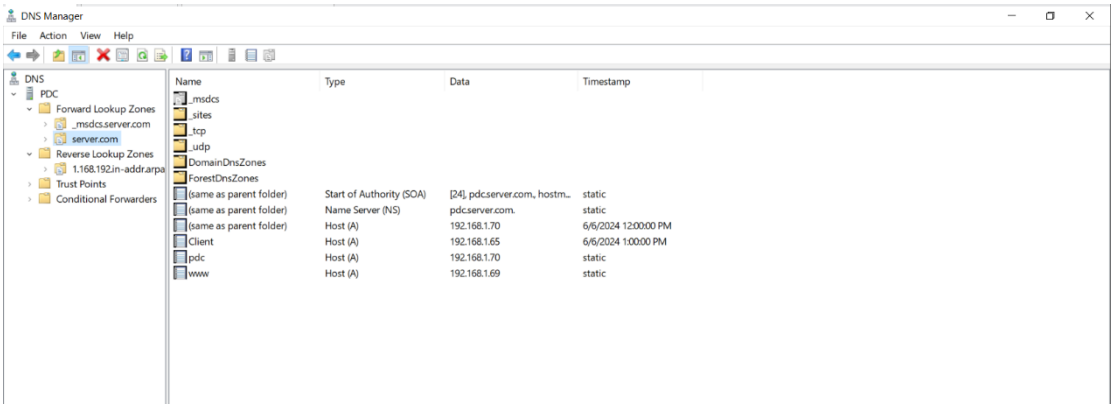


the second screen is belong to the client



In the DHCP Server, we can reserve an IP, whether it includes the IP Server or even the user's.

5- DNS Server:



We set the server ip as DNS ip -> 192.168.1.70

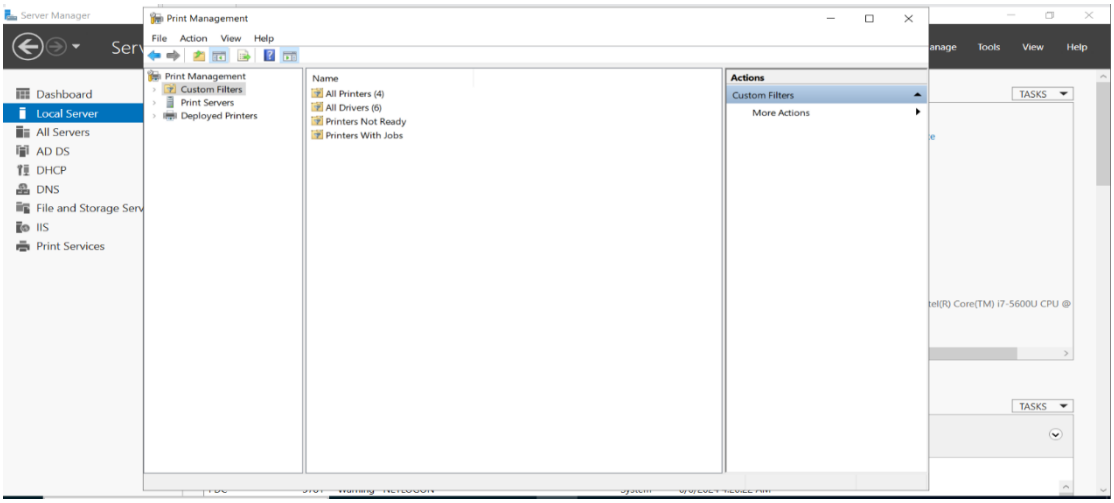
6- PRINT Server:

A print server connects to multiple printers to a network, allowing users to a send print jobs to the server, which then distributes them to the appropriate printer. This simplifies connectivity and reduces congestion.

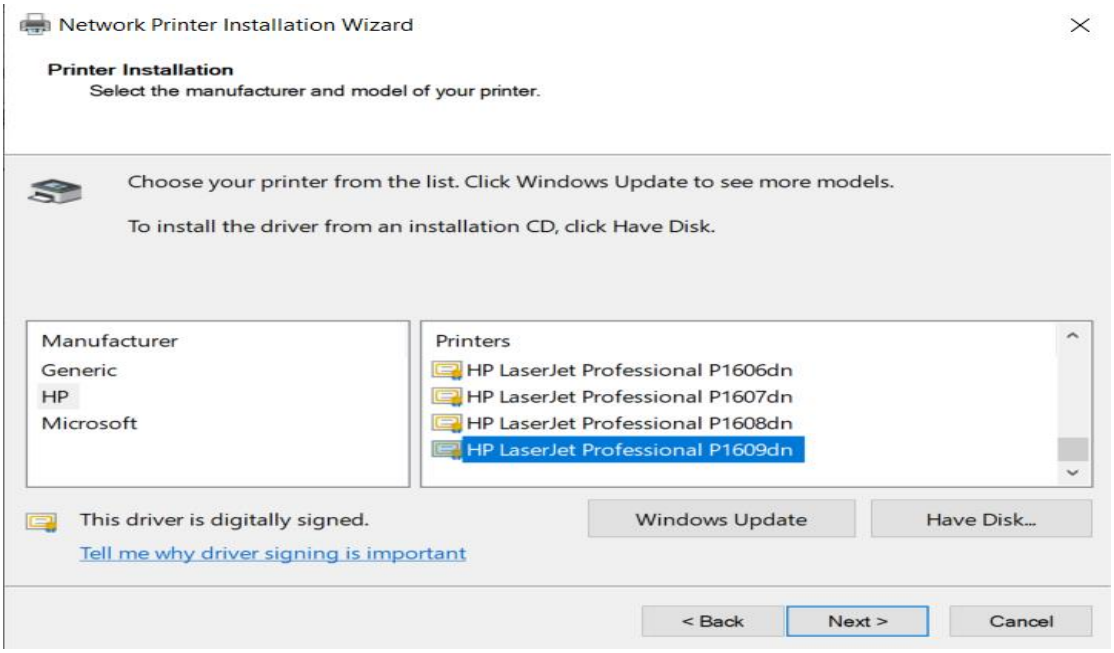
Print service installation:
From the server manager where you want to install the print service, click Add Roles and Features ->When launching the wizard, click Next ->Choose the option based on role one or feature and click Next ->Select server and click Next ->Check the box for printing and scanning documents ->Add Features ->The Print Services role is selected, click Next >Skip the list of features by clicking Next ->A Print Services Summary is displayed, click Next ->
Select the Print Server ->Click on the Install ->Wait while installing the print service …->
The installation completed, exit the wizard by clicking Close

[Windows Print Server: Installation and Configuration - RDR-IT]

Then Click Tools -> print management

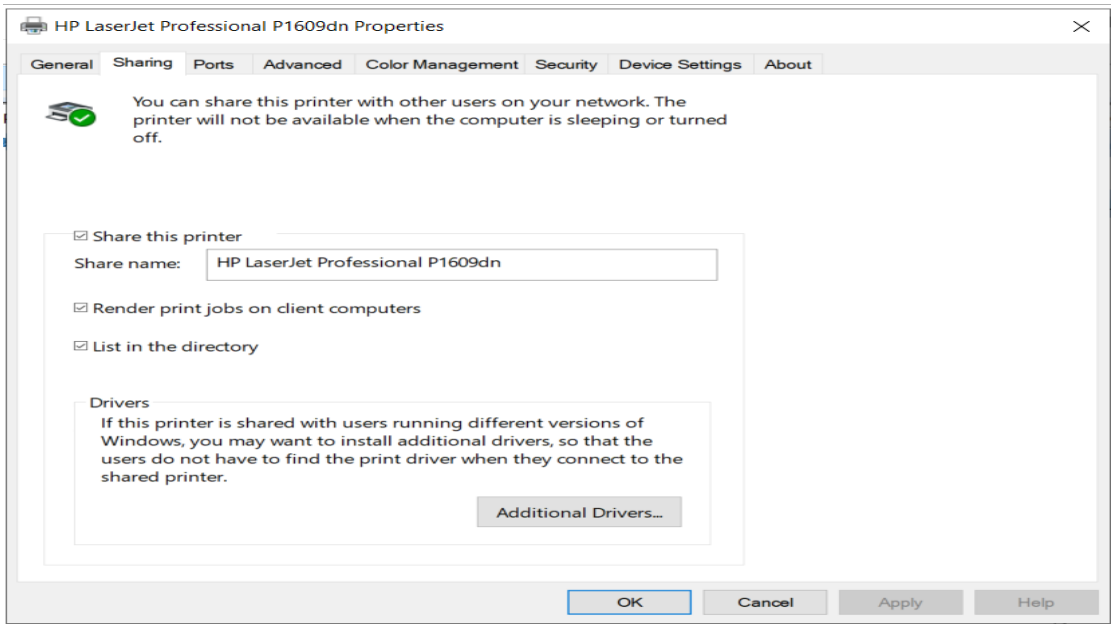


Then add printer : printer servers -> add printer and choose driver:

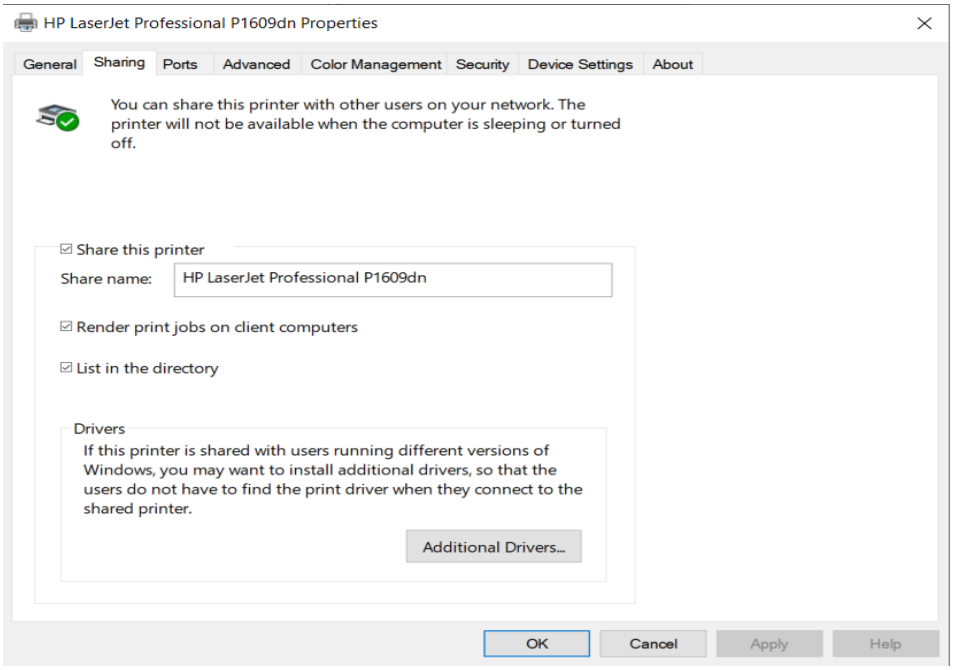


Choose the available printer and click Next ,after finish configuration -> right click on the printer to configure and click Properties:

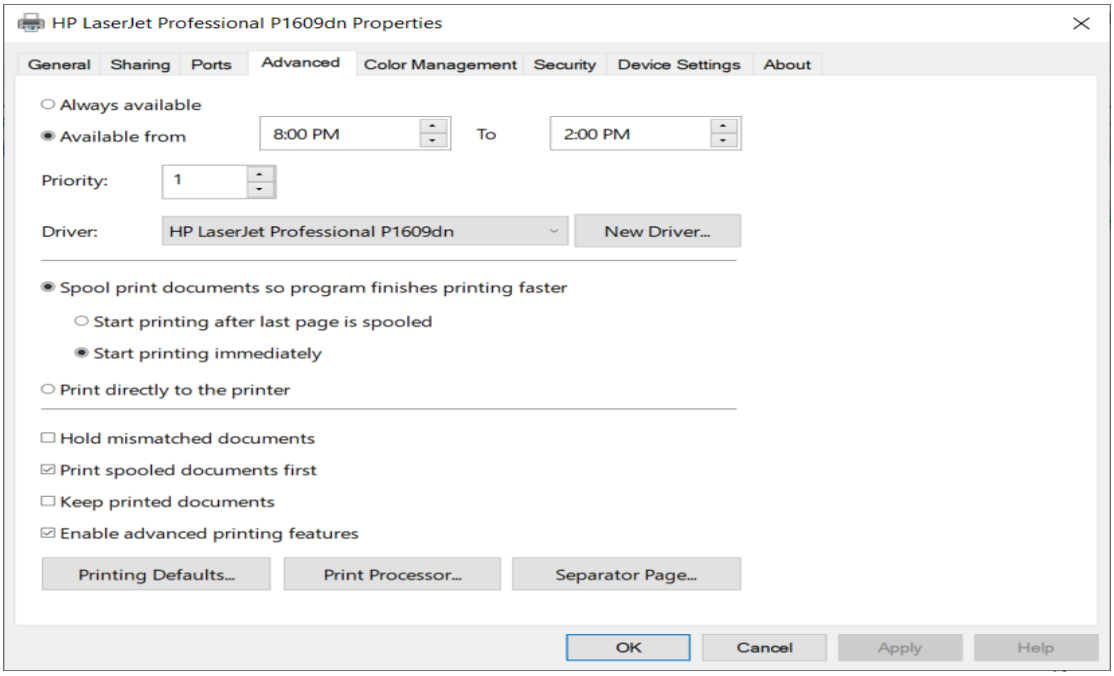
The General tab allows you to configure the name of the printer visible from the server, displays a summary of the features and starts printing a test page.



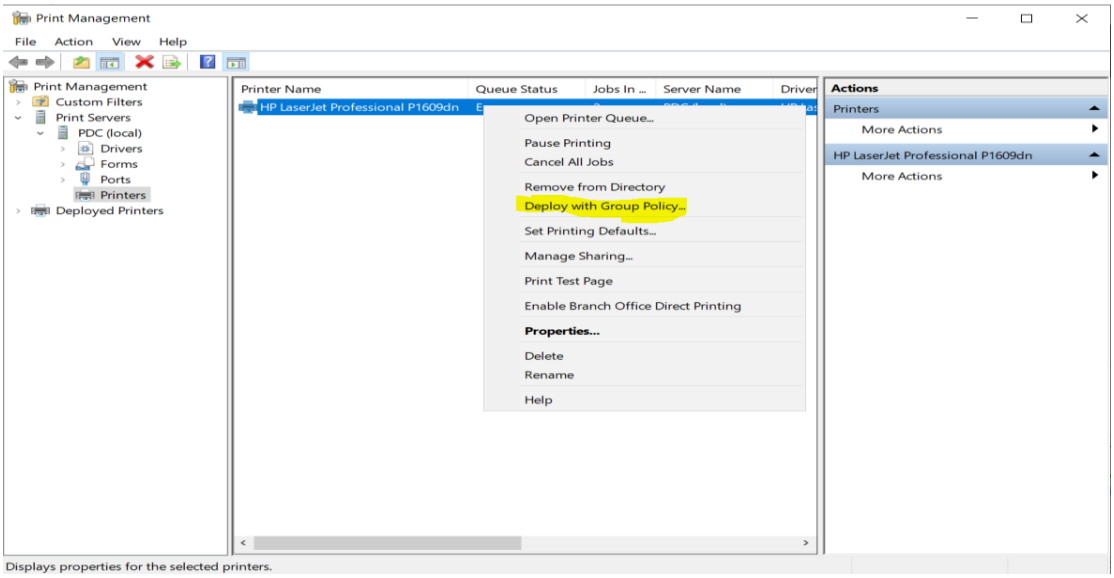
The Sharing tab is used to configure the SMB name

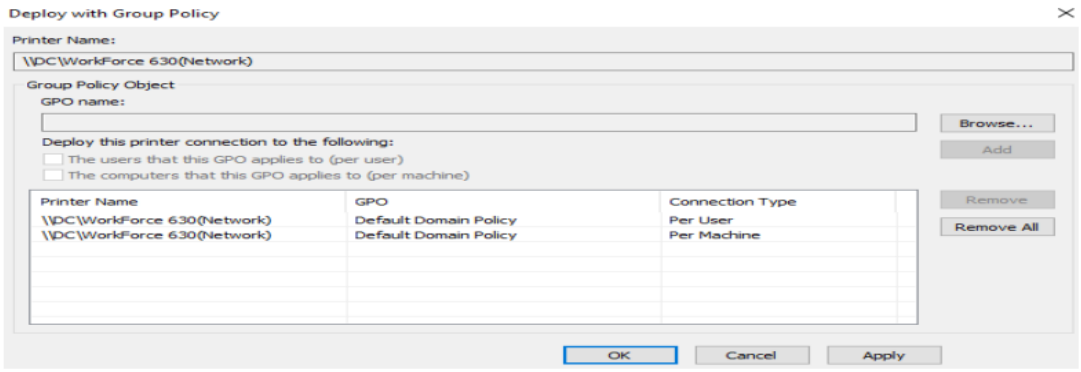


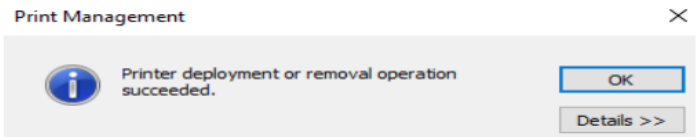
The Advanced tab allows you to configure the driver used as well as the default print settings (black and white, double-sided ….).



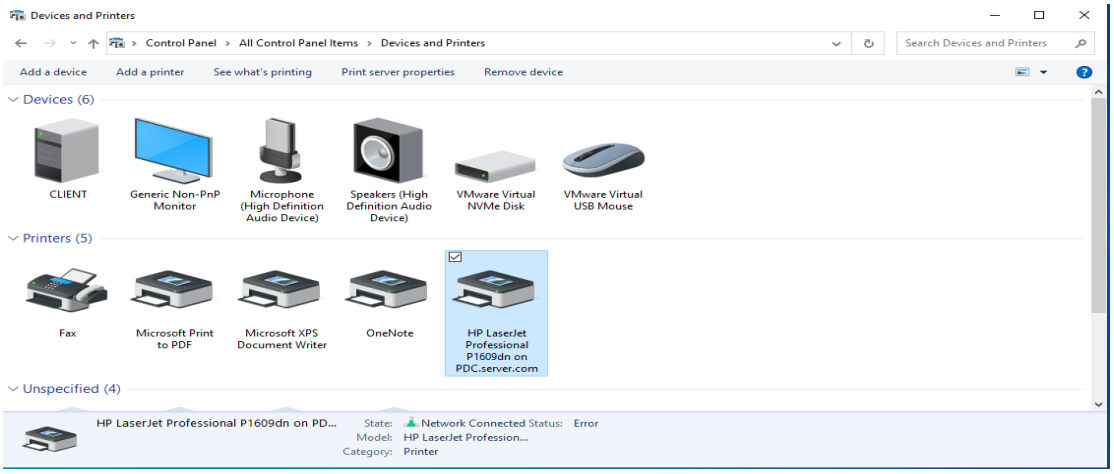
Now we can deploy this printer through GPO



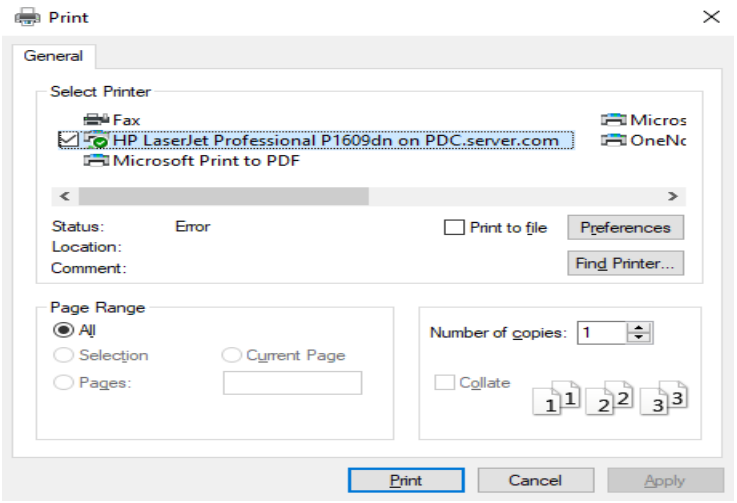


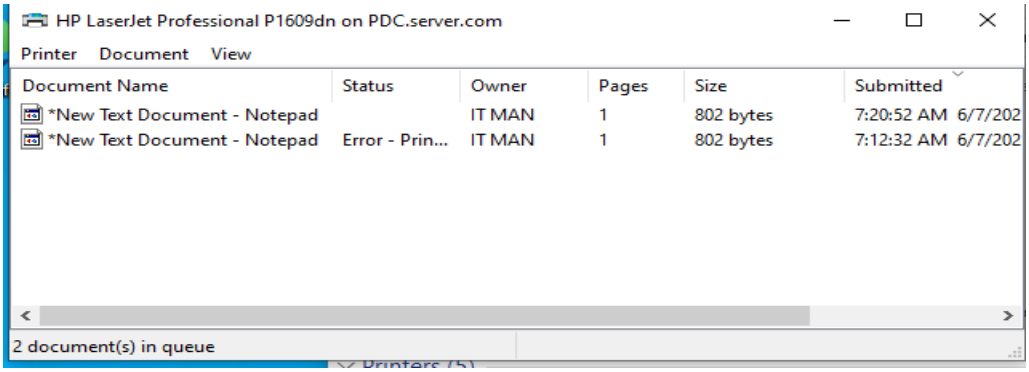


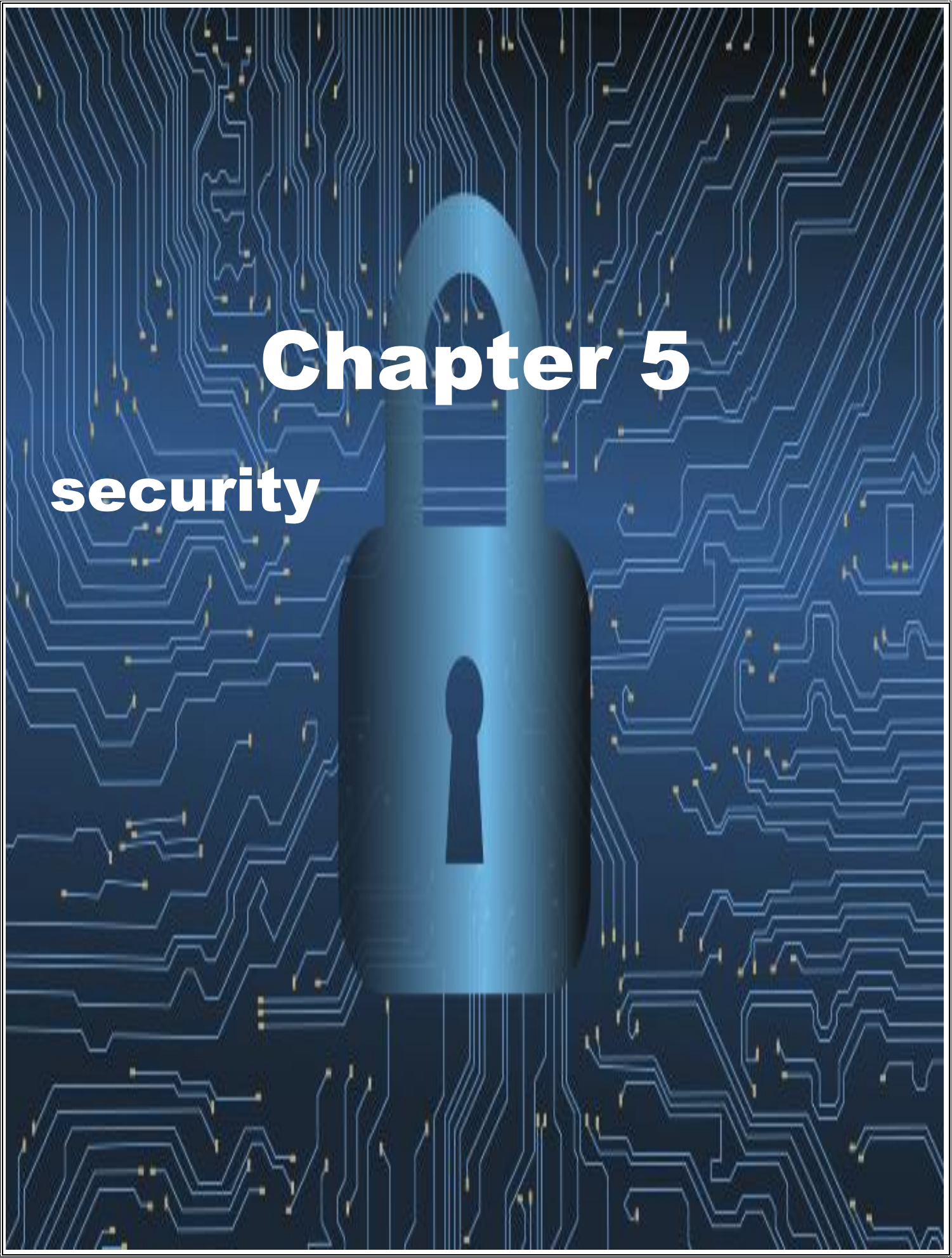
I logged into a client machine. Here is the network printer.



Then make text file and Click (ctrl+P) to print :






Chapter 5
security

Introduction

Information security is the practice of protecting information by mitigating information risks. It involves the protection of information systems and the information processed, stored, and transmitted by this system from unauthorized access, use, disclosure, disruption, modification, or destruction. These include the protection of personal information, financial information, and sensitive or confidential information stored in both digital and physical forms. Effective information security requires a comprehensive and multi-disciplinary approach, involving people, processes, and technology.

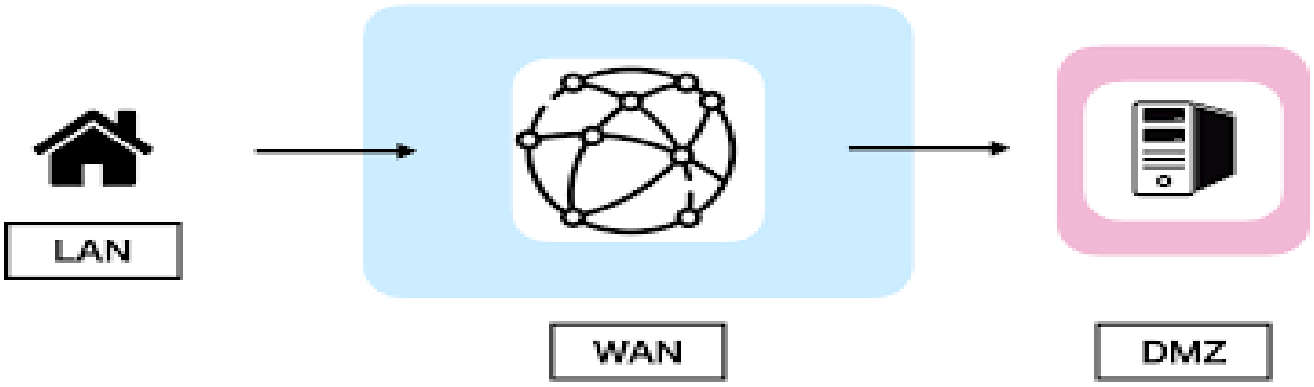
Information security is keen to investigate:

1. **Confidentiality**
2. **Integrity**
3. **Availability**

Design network security

The first step that we take when designing an insurance solution for the network is dividing the single network into several areas. The most important 3 areas we know when dividing the network are

- Internal network zone –private (IN), Lan
- DMZ zone
- External network zone –public (out), wan



External network zone

It is the part dedicated to the public Internet, this part I have no control over and as a result I do not fully trust this part and consider it a source of all risks.

Security level zero

Internal network zone

This part represents the devices that we trust and that we can control from the network that I am responsible for protecting. This part is where I put the server that contains the important data and programs of the organization that I want to protect from any external threat coming from the public network It is especially important to separate the internal network of my organization from the public network

Security level 100

DMZ (Demilitarized zone)

The end goal of a DMZ network is to allow an organization to access untrusted networks, such as the internet, while ensuring its private network or LAN remains secure.

Security level from 1 to 99

Attacks

- **DOS attack**
- **DDOS attack**

What is Denial-of-services (DOS)?

A denial-of-service (DoS) attack is a type of cyber-attack in which a malicious actor aims to render a computer or other device unavailable to its intended users by interrupting the device's normal functioning. DoS attacks typically function by overwhelming or flooding a targeted machine with requests until normal traffic is unable to be processed, resulting in denial-of-service to additional users.

A DoS attack is characterized by using a single computer to launch the attack.

A distributed denial-of-service (DDoS) attack is a type of DoS attack that comes from many distributed sources, such as a botnet DDoS attack.

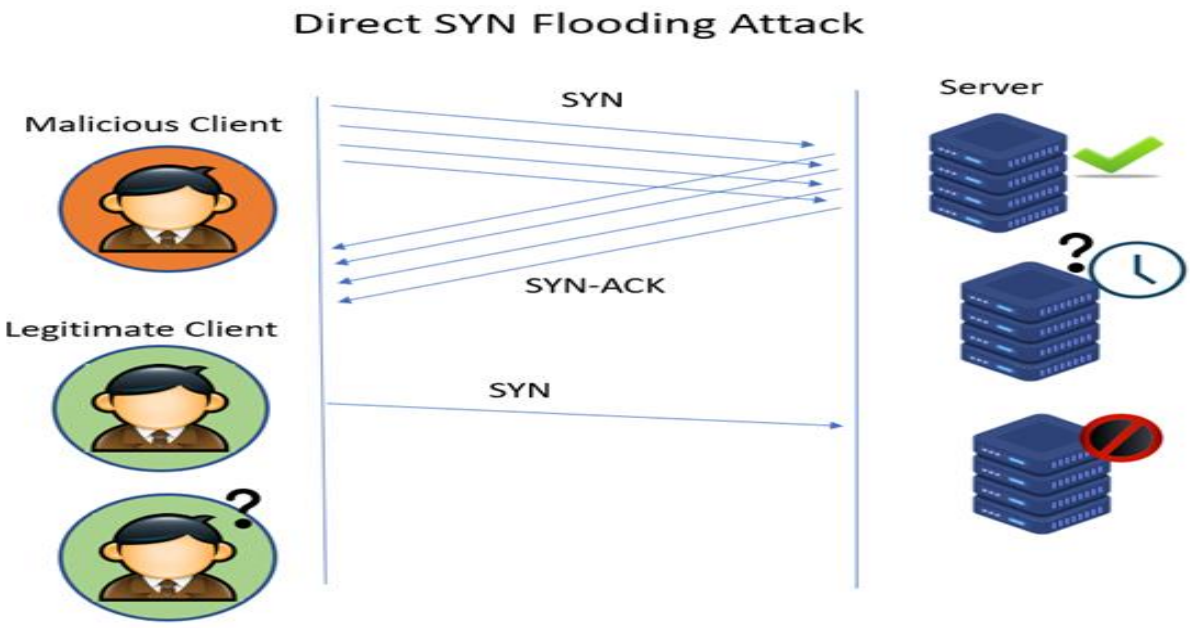
There are two general methods of DoS attacks: flooding services or crashing services. Flood attacks occur when the system receives too much traffic for the server to buffer, causing them to slow down and eventually stop. Popular flood attacks include:

- **Ping of Death`**

  The ping command is usually used to test the availability of a network resource. It works by sending small data packets to the network resource. The ping of death takes advantage of this and sends data packets above the maximum limit (65,536 bytes) that TCP/IP allows. TCP/IP fragmentation breaks the packets into small chunks that are sent to the server. Since the sent data packages are larger than what the server can handle, the server can freeze, reboot, or crash.

- **SYN attack**

  SYN is a short form for Synchronize. This type of attack takes advantage of the three-way handshake to establish communication using TCP. SYN attack works by flooding the victim with incomplete SYN messages. This causes the victim machine to allocate memory resources that are never used and deny access to legitimate users.



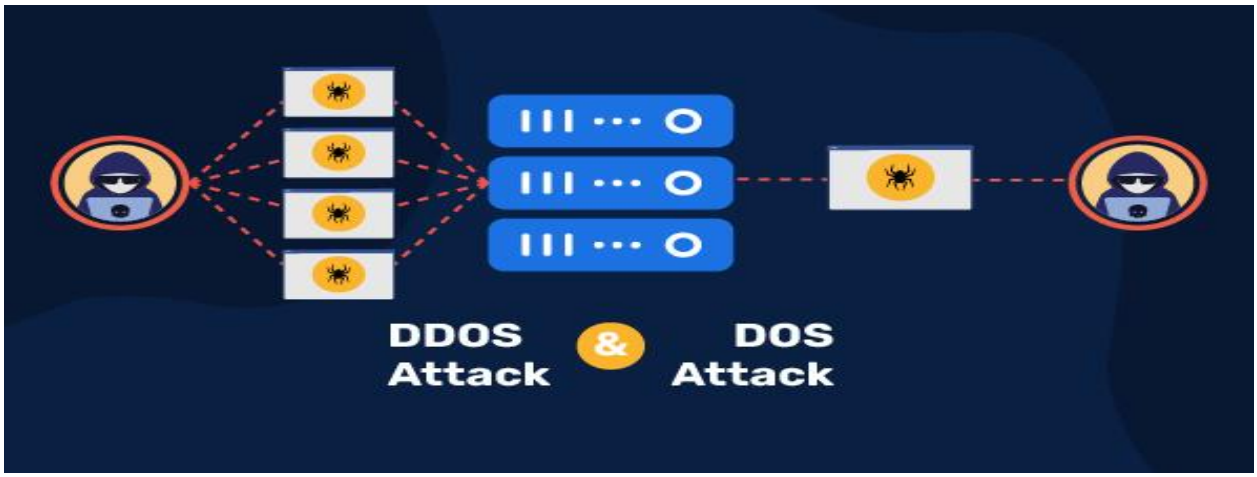
How can you tell if a computer is experiencing a DoS attack?

While it can be difficult to separate an attack from other network connectivity errors or heavy bandwidth consumption, some characteristics may indicate an attack is underway. Indicators of a DoS attack include:

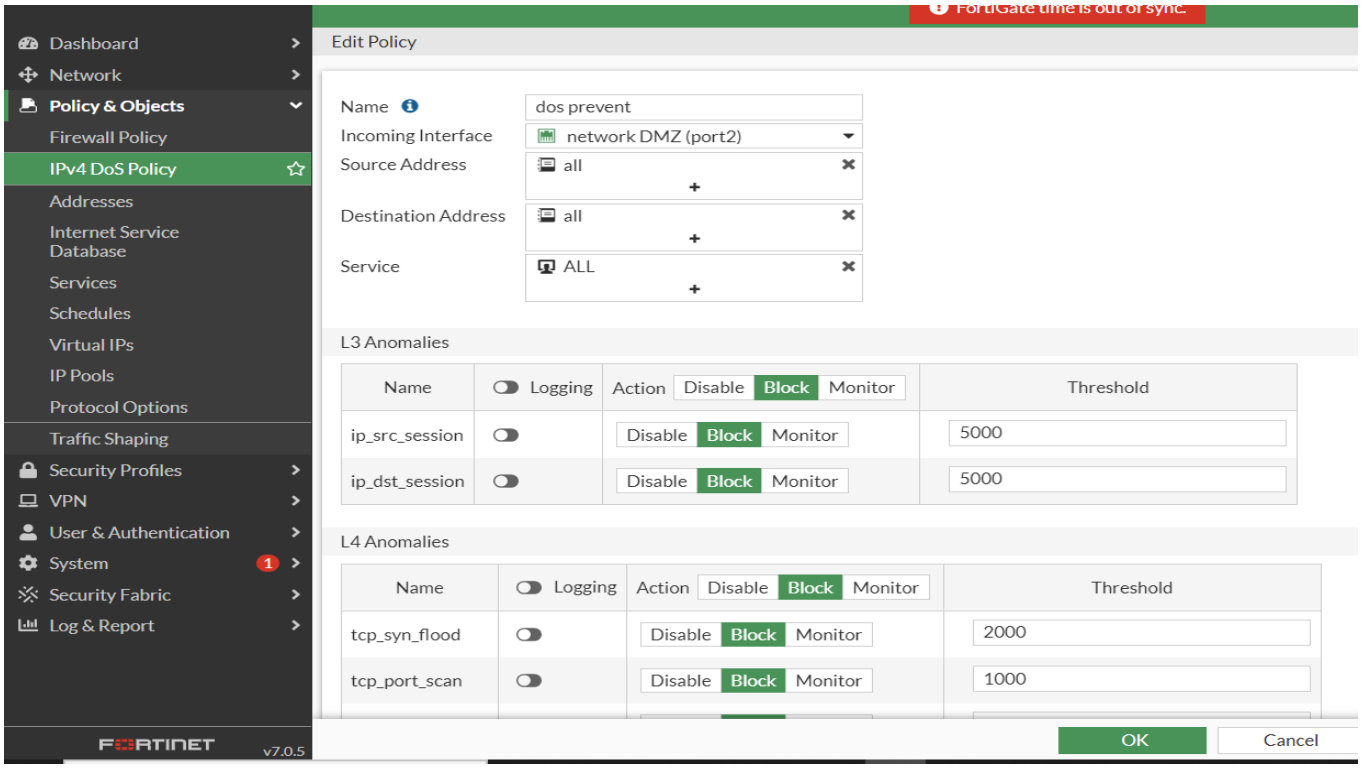
- Atypically slow network performance such as long load times for files or websites
- The inability to load a particular website such as your web property
- A sudden loss of connectivity across devices on the same network

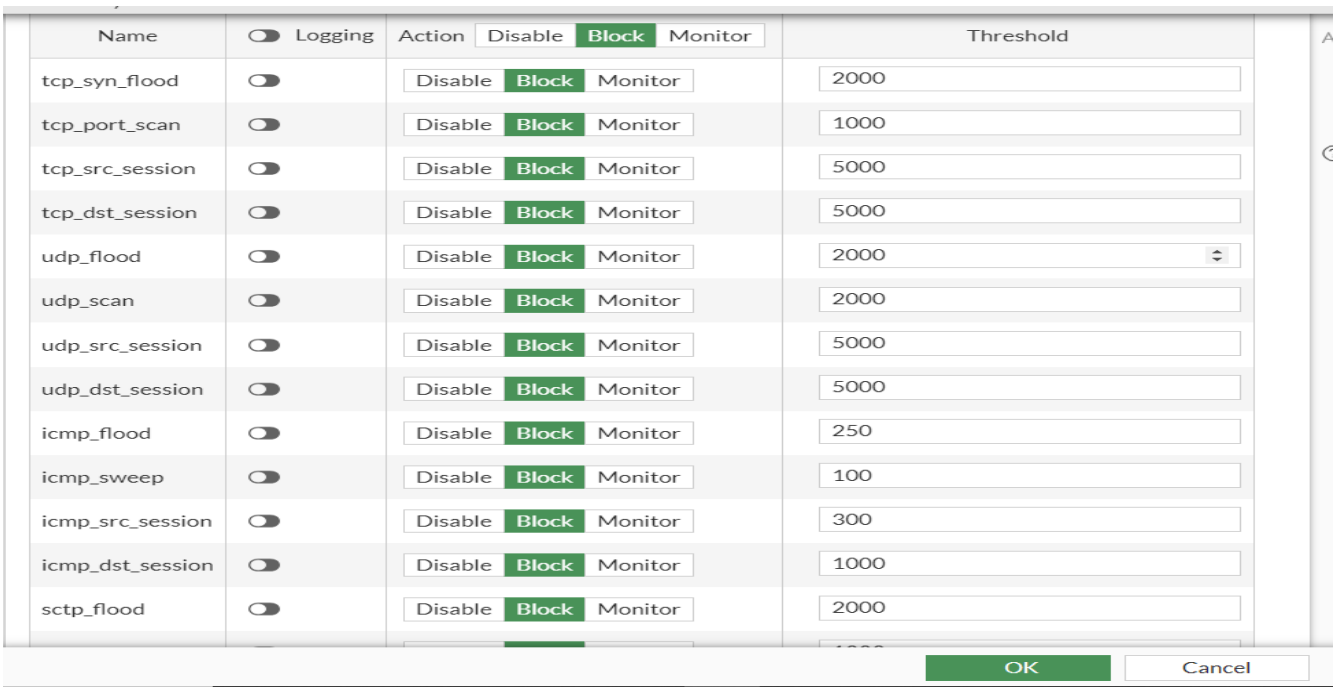
What is the difference between a DDoS attack and a DOS attack?

The distinguishing difference between DDoS and DoS is the number of connections utilized in the attack. DoS utilizes a single connection, Some DoS attacks, such as “low and slow” attacks like Slow loris, derive their power in the simplicity and minimal requirements needed for them to be effective. While a DDoS attack utilizes many sources of attack traffic, often in the form of a botnet. Many of the attacks are fundamentally similar and can be attempted using one or more many sources of malicious traffic.



Protection from DOS attack





Standard defensive-oriented technologies

- Firewall
- Intrusion Detection System
- Intrusion Prevention System
- Access Control
- VPN
- VLAN
- Port Security

Intrusion Detection System (IDS):

IDS is a system that observes network traffic for malicious transactions and sends immediate alerts when it is observed. It is software that checks a network or system for malicious activities or policy violations. Each illegal activity or violation is often recorded either centrally using a SIEM system or notified to an administration. IDS monitors a network or system for malicious activity and protects a computer network from unauthorized access from users, including insiders. The intrusion detector learning task is to build a predictive model capable of distinguishing between bad connections (intrusion/attacks) and good (normal) connections.

Intrusion Prevention System (IPS):

IPS is a cybersecurity tool that examines network traffic to identify potential threats and automatically acts against them. An IPS might, for example, recognize and block malicious software or vulnerability exploits before they can move further into the network and cause damage. IPS tools continually monitor and log network activity in real time. An intrusion prevention system expands on the capabilities of intrusion detection systems (IDS), which are similar but less advanced tools. Unlike an IPS, an IDS can detect but not respond to malicious activity. Today, security vendors often package IPS and IDS capabilities within broader product suites or platforms.

Firewall

What is a firewall?

A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It acts as a barrier between a trusted internal network and an untrusted external network, such as the Internet. Firewalls are essential in protecting networks from cyber attacks and unauthorized access. They can prevent malware, viruses, and other malicious software from entering a network, as well as stop hackers from gaining access to sensitive data.

Types of firewalls

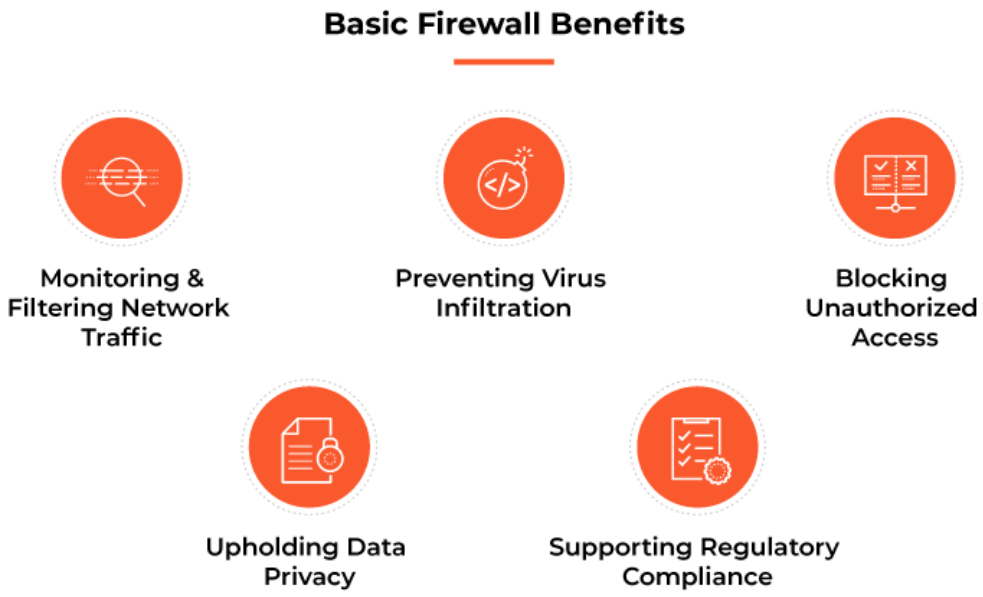
- **Packet filtering firewalls**
- **Stateful inspection firewalls**
- **Circuit-level Gateway**
- **A web application firewall**
- **A proxy firewall**
- **A next-generation firewall (NGFW)**,

How Firewalls Work

by examining incoming and outgoing network traffic and comparing it against a set of predetermined security rules. There are several methods that firewalls use to do this, including packet filtering, stateful inspection, and application-level gateway. Packet filtering is the most basic method, where the firewall examines each packet of data and decides whether to allow or block it based on its source, destination, and other criteria. Stateful inspection is a more advanced method that examines the context of each packet and uses this information to make more informed decisions. Application-level gateway firewalls are the most sophisticated and can examine the content of each packet to determine whether it is safe or not.

Advantages of a Firewal

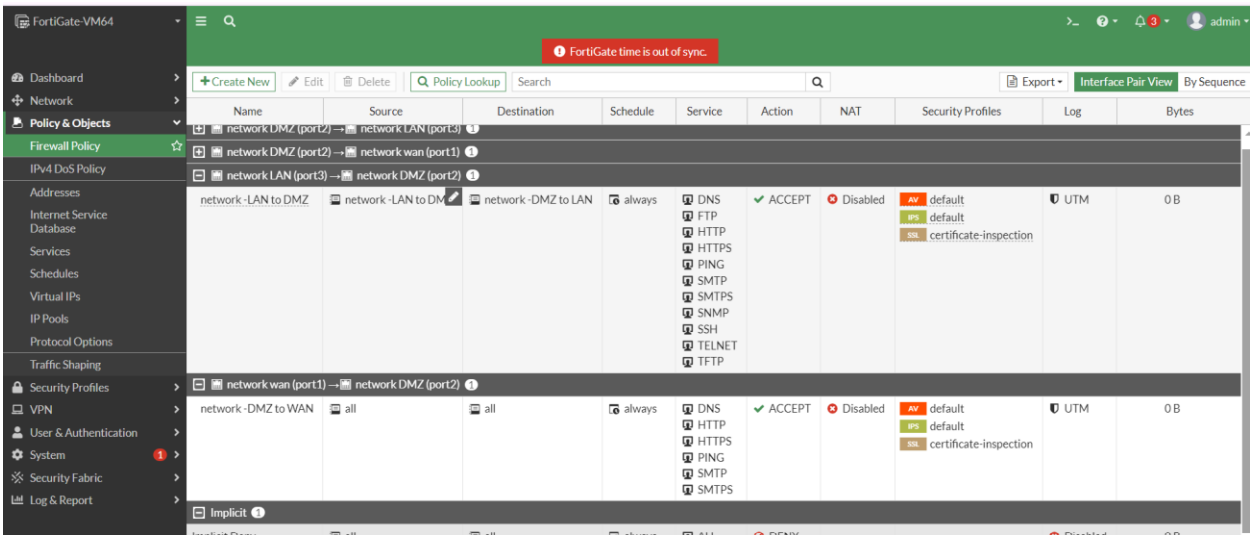
- **Monitoring and Filtering Network Traffic**.
- **Preventing Virus Infiltration**
- **Blocking Unauthorized Access**
- **Upholding Data Privacy**
- **Supporting Regulatory Compliance.**

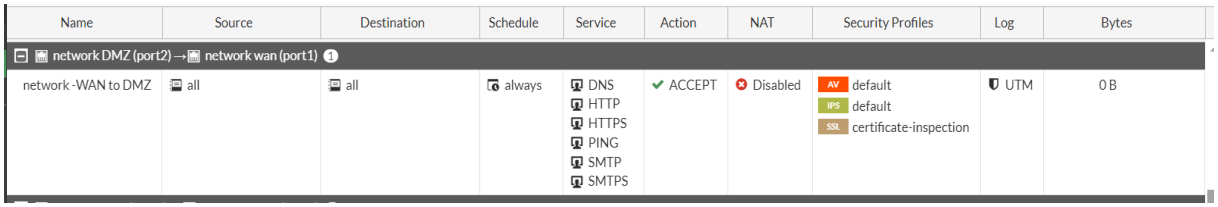


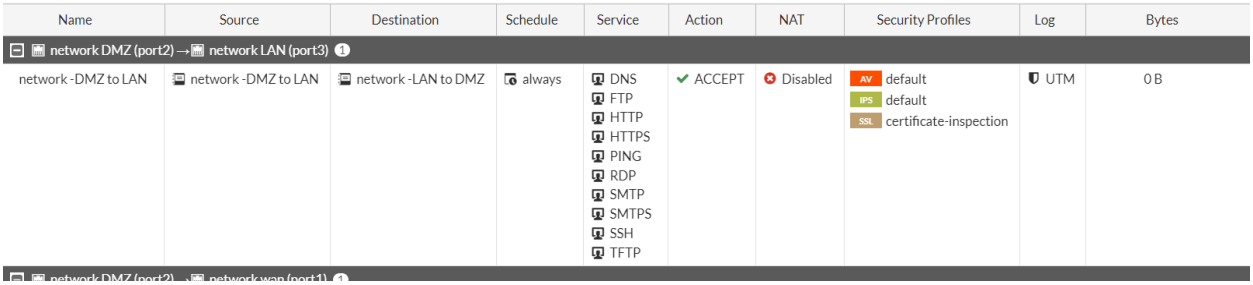
Disadvantages of using Firewall

- **Complexity**
- **Limited Visibility**
- **False sense of security**
- **Limited adaptability**
- **Performance impact**
- **Limited VPN support**
- **Cost**

Policy applied to firewall

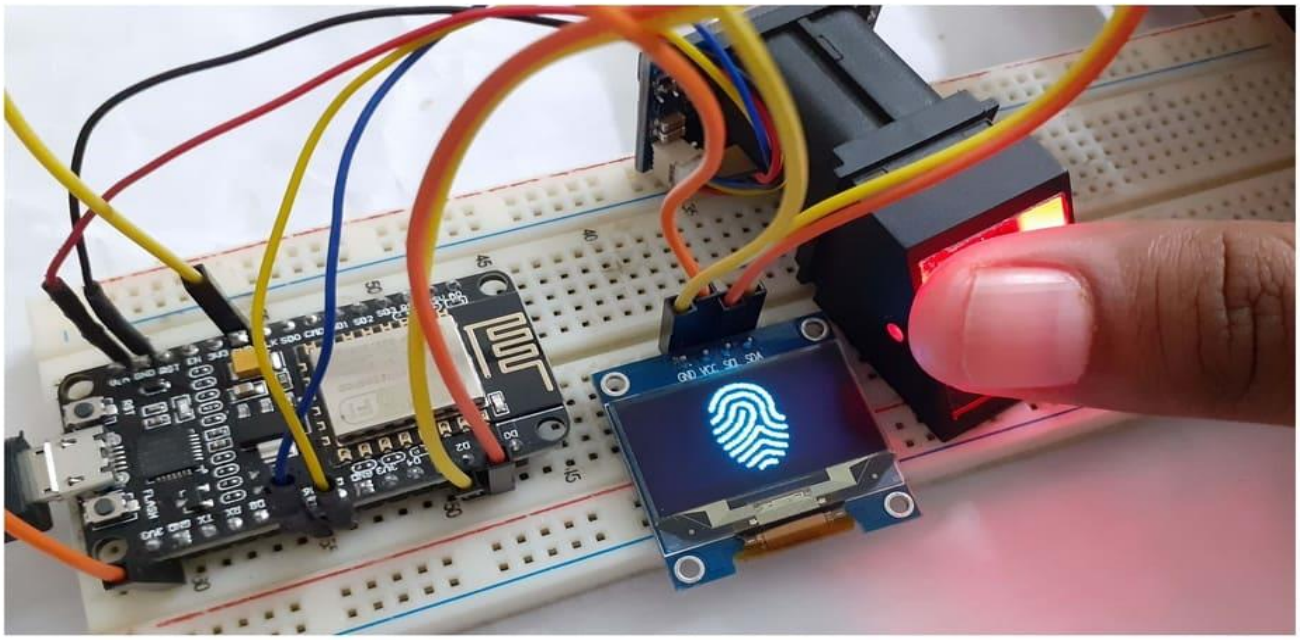






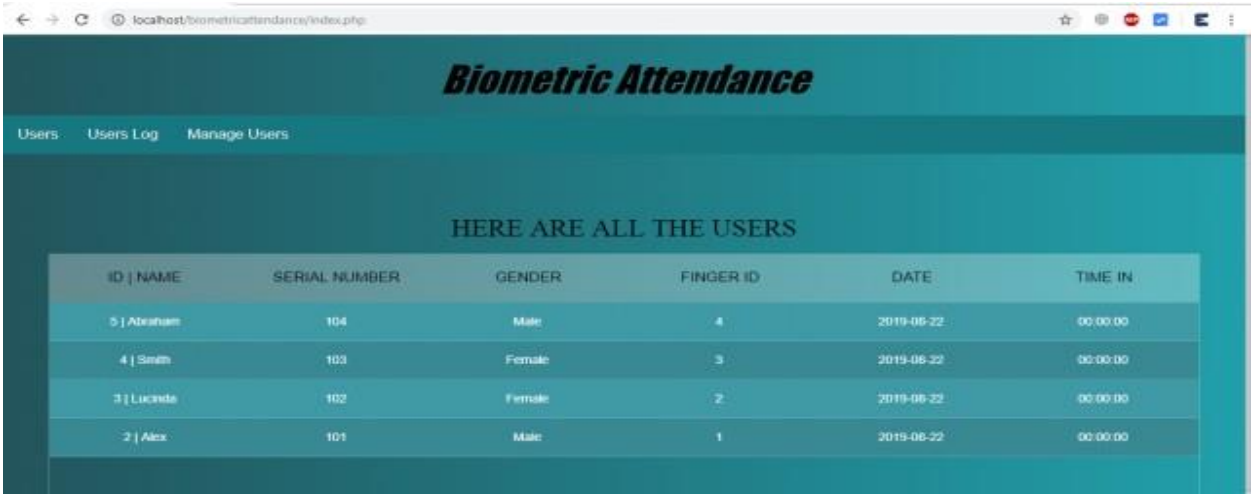
Chapter 6

IoT Biometric Fingerprint Attendance System using ESP8266



In this project **IoT Biometric Project**, we will learn how to build I**oT based Biometric Fingerprint Attendance System** using **NodeMCU ESP8266 ESP8266 12E**, 0.96" **OLED Display** & **R305 Fingerprint Sensor**. The **ESP8266 Wi-Fi Module** will collect the **fingerprint data** from multiple users and sends it over the internet to a **website**. The Enrolment of fingerprints is done on the Server using **R305** or **R307** or any other compatible Fingerprint Sensor and verification is done on the client with the transmission of fingerprint templates over the network.

The **website** that is coded in **PHP** has a **database** and **records of attendance**. By logging into the website, you can collect all the attendance records of each user including personal details as well as incoming & outgoing timing. The data can also be downloaded and exported to an **excel sheet**.



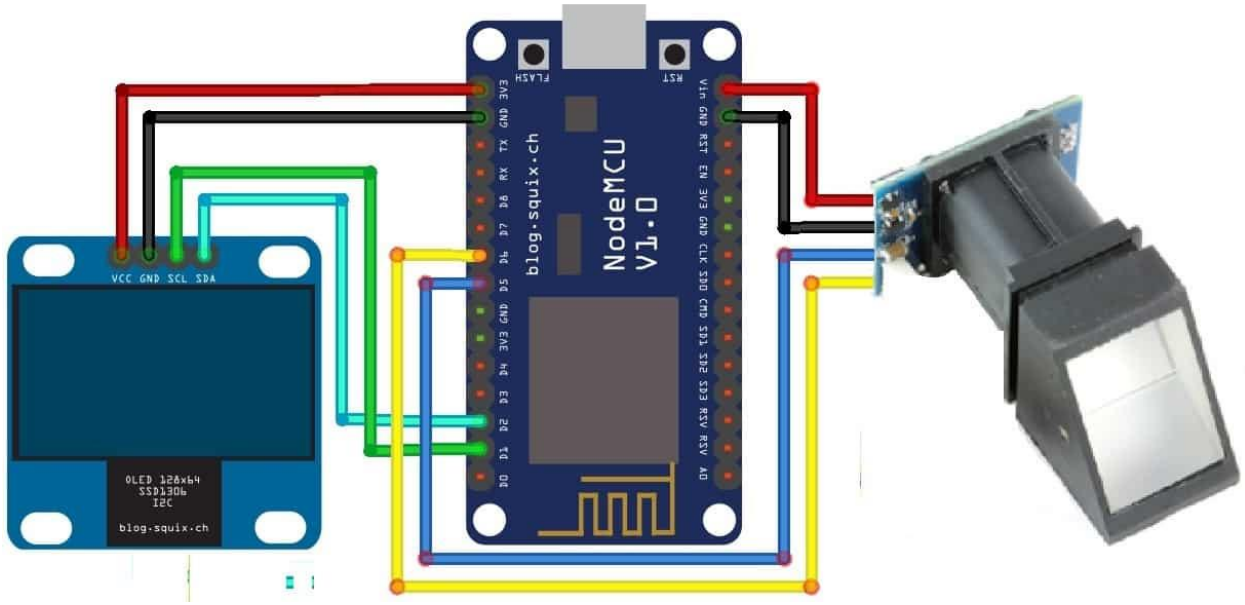
Conventional authentication technologies like RFID tags and authentication cards have a lot of weaknesses, the biometric method of authentication is a prompt replacement for this. **Biometrics** such as **fingerprints**, voices and ECG signals are unique human characters that cannot be tampered or replicated. This facilitates real-time system implementations. **Biometric Attendance systems** are commonly used systems to mark the presence in offices and schools as well as in **Biometric Security Lock**. This project has a wide application in schools, colleges, business organizations, offices where marking of attendance is required accurately with time. Thus, by using the **fingerprint sensor**, the system will become more secure for the users.

Bill of Materials

The following are the components required to make **IoT Based Biometric Fingerprint Attendance System**. All the components can be purchased from Amazon. The purchase links are given below.

S.N.	Components	Quantity
1	**Node MCU ESP8266 Board**	1
2	**R305/R307 Fingerprint Sensor**	1
3	**0.96" I2C OLED Display**	1
4	**Connecting Wires**	20
5	**Breadboard**	1

Circuit Diagram: IOT Based Biometric Fingerprint Attendance System



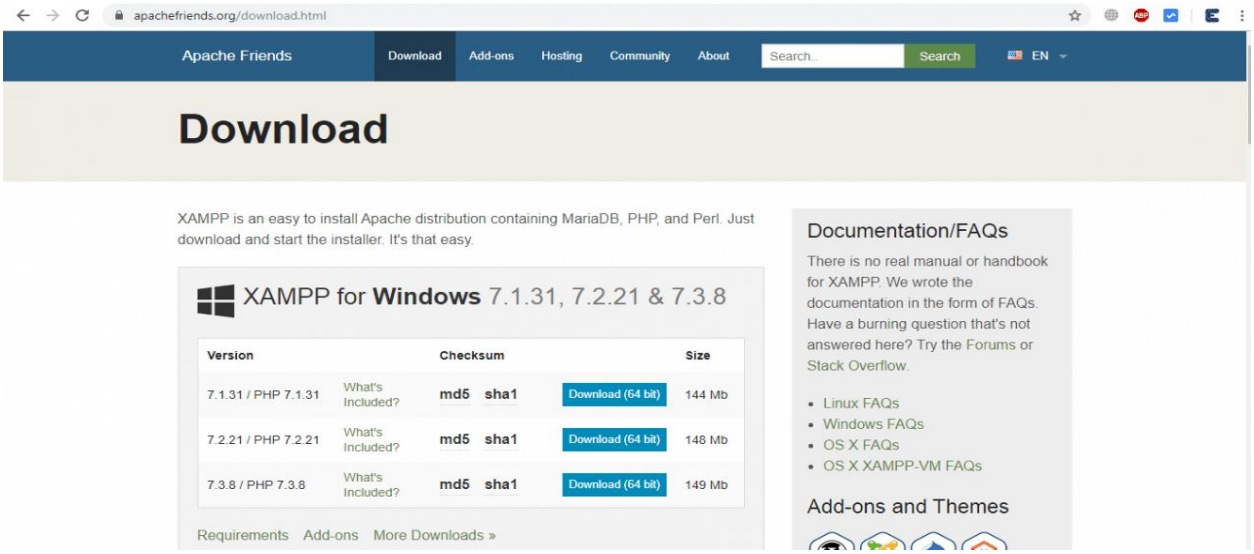
The above circuit diagram shows how an OLED Display & Fingerprint Sensor is interfaced with **NodeMCU ESP8266 ESP8266** 12E Board. The I2C pins of OLED Display, i.e SDA & SCL are connected to NodeMCU D2 & D1 pins respectively. Similarly, the fingerprint sensor is connected to UART pins D5 & D6. The fingerprint sensor Tx and Rx wire's color may vary. In my case, the color is yellow and blue where yellow is Tx and Blue is Rx. So connect it by finding appropriate color wires else the module won't be detected by NodeMCU.

The R305 fingerprint sensor is supplied with 5V through Vin pins of NodeMCU. In my case, the sensor didn't work at 3.3V. Similarly, connect OLED Vcc pin to 3.3V of NodeMCU.

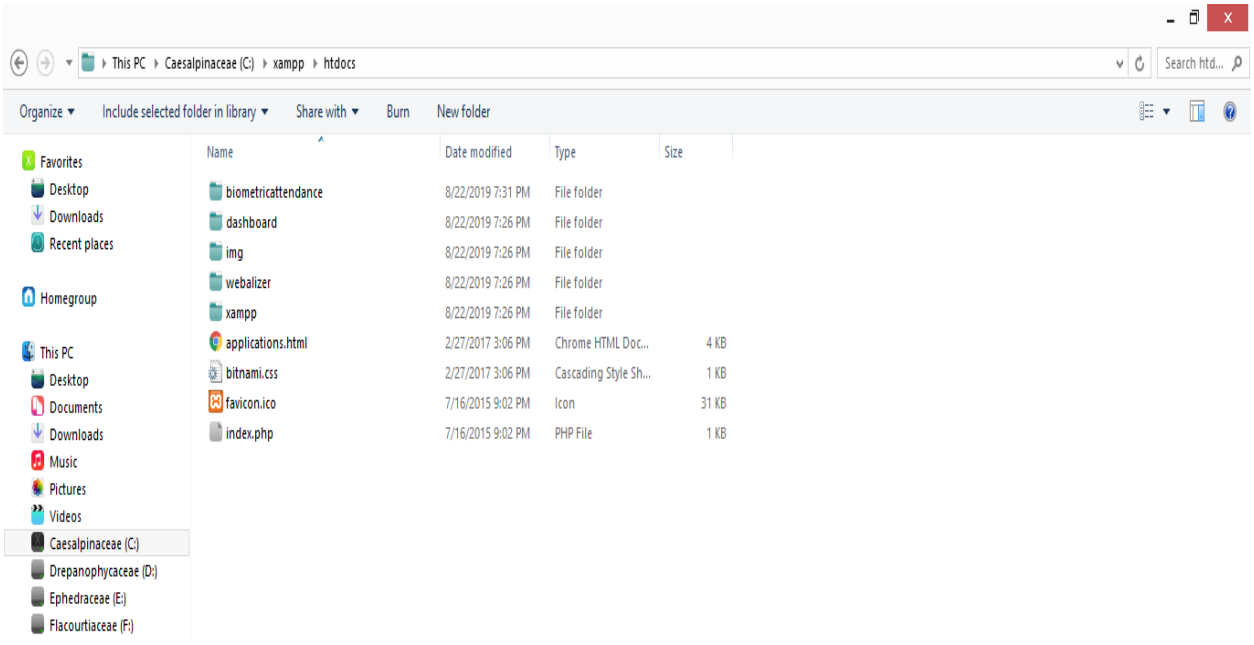
Setting Up the Website

Here we can set up a website if you have a website and a server. In case you don't wanna spend money on website management, then you can use your computer IP as a server to store the data locally in localhost.

First Download and install Xampp from the link here: Download XAMPP



Once the download and installation is completed copy the following folder: Biometricattendance Folder to **C:\xampp\htdocs**. This is the location of the website in your C drive.



Source Code/Program

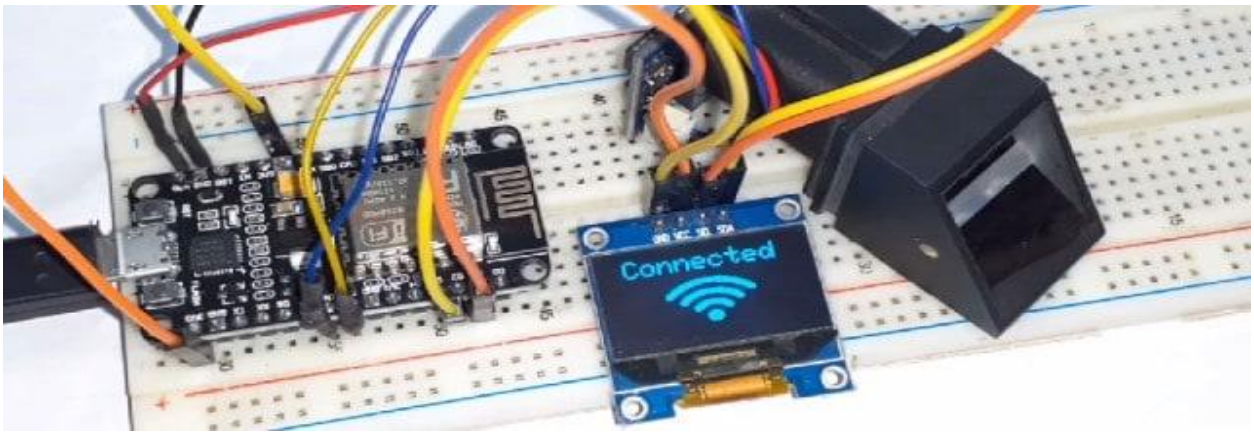
Add the following libraries via library manager or simply by adding the following zip files:

1. OLED GFX Library: Download
2. SSD1306 Library: Download
3. Adafruit Fingerprint Sensor Library: Download

```
#include <ESP8266WiFi.h>
#include <SoftwareSerial.h>
#include <ESP8266WebServer.h>
#include <ESP8266HTTPClient.h>
#include <Adafruit_GFX.h>           //https://github.com/adafruit/Adafruit-GFX-Lib
#include <Adafruit_SSD1306.h>       //https://github.com/adafruit/Adafruit_SSD1306
#include <Adafruit_Fingerprint.h>  //https://github.com/adafruit/Adafruit-Fingerp
//*************************************************************************
//Fingerprint scanner Pins
#define Finger_Rx 14 //D5
#define Finger_Tx 12 //D6
// Declaration for SSD1306 display connected using software I2C
#define SCREEN_WIDTH 128 // OLED display width, in pixels
#define SCREEN_HEIGHT 64 // OLED display height, in pixels
#define OLED_RESET     0 // Reset pin # (or -1 if sharing Arduino reset pin)
Adafruit_SSD1306 display(SCREEN_WIDTH, SCREEN_HEIGHT, &Wire, OLED_RESET);
//*************************************************************************
SoftwareSerial mySerial(Finger_Rx, Finger_Tx);
Adafruit_Fingerprint finger = Adafruit_Fingerprint(&mySerial);
//*************************************************************************
/* Set these to your desired credentials. */
const char *ssid = "SSID";  //ENTER YOUR WIFI SETTINGS
const char *password = "password";
//*************************************************************************
String postData ; // post array that will be send to the website
String link = "http://YourComputerIP/biometricattendance/getdata.php"; //computer
int FingerID = 0;      // The Fingerprint ID from the scanner
uint8_t id;
//************************Biometric Icons*********************************
```

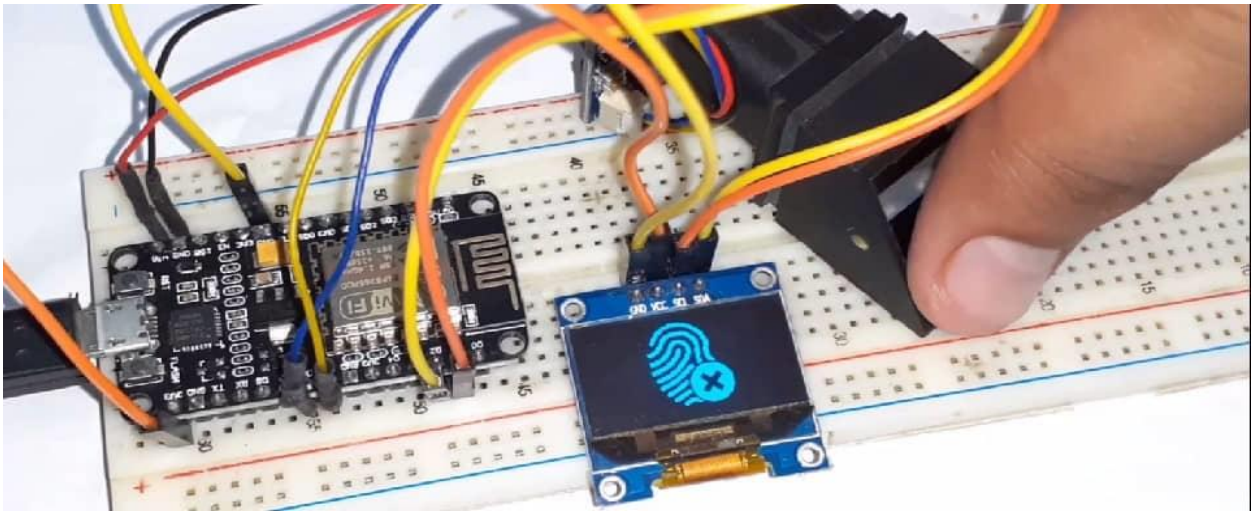
Results

Once the Code is uploaded the NodeMCU will boot up with the Adafruit logo. And then it will try the connection to the wifi. Once it gets Connected it will display Connected. This log can be viewed on Serial Monitor as well as in OLED Display.

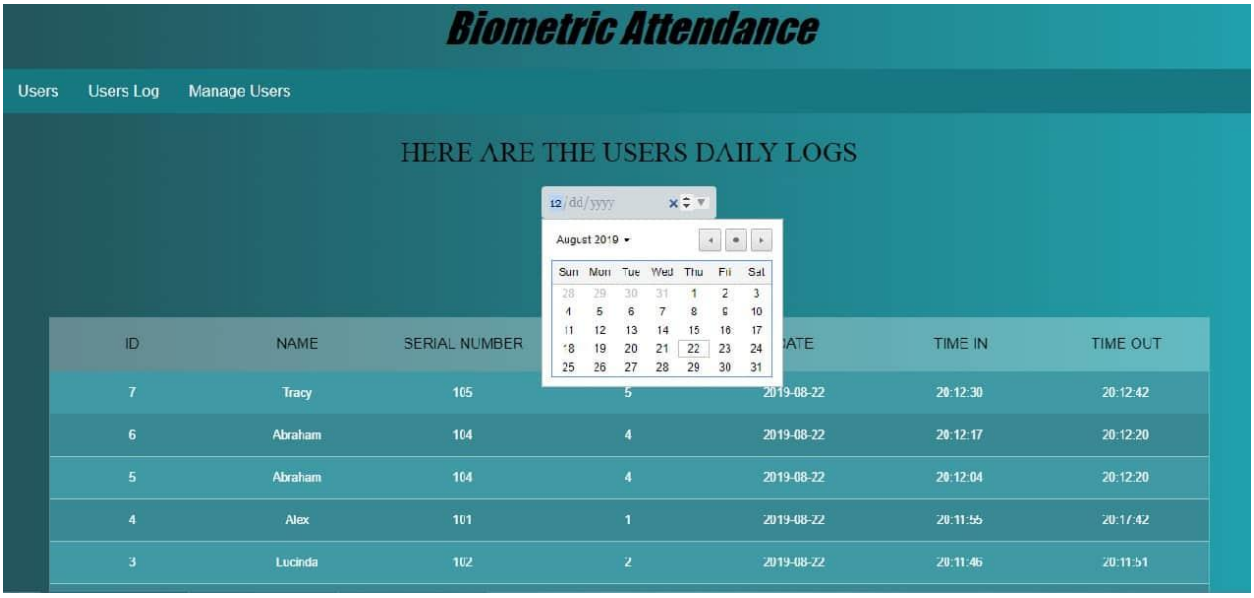


So now you can start registering the user using the website. The whole process of registration is explained in the video below. You can follow the video for the registration process. The user fingerprint is taken twice and stored in the EEPROM of the Fingerprint Sensor. It is to be noted that only 127 fingerprints can be stored in this R305/R307 module.

So once the fingerprint of multiple users is stored, you can start scanning and registering the attendance. In case the fingerprint is not matched it will display an error message as shown in the figure below.



Finally you can see the entire data of the users on the website as shown below:



Sources:

1. https://helpcenter.trendmicro.com/en-us/article/tmka-11447
2. https://honestproscons.com/advantages-and-disadvantages-of-vpn/
3. https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html
4. https://www.fortinet.com/resources/cyberglossary/how-does-vpn-work
5. https://en.wikipedia.org/wiki/Generic_Routing_Encapsulation
6. https://www.wallarm.com/what/generic-routing-encapsulation-gre
7. https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/13772-12.html
8. https://www.nextiva.com/blog/what-is-voip.html
9. https://www.net2phone.com/guide/what-is-voip
10. https://exotel.medium.com/what-is-voip-how-does-it-work-advantages-disadvantages-cost-6dcaae1525d2
11. https://www.investopedia.com/terms/v/voiceoverinternet-protocol-voip.asp
12. https://www.3cx.com/pbx/voice-over-ip/
13. https://study-ccna.com/port-security/
14. https://drive.google.com/drive/mobile/folders/1UZzSCKLMDynGVF_F0wZEQq2HIooi4PS4
15. https://www.techtarget.com/searchsecurity/definition/intrusion-prevention
16. https://www.geeksforgeeks.org/intrusion-detection-system-ids/
17. https://www.fortinet.com/resources/cyberglossary/what-is-dmz
18. https://www.geeksforgeeks.org/ip-security-ipsec/
19. https://www.techtarget.com/searchsecurity/definition/IPsec-Internet-Protocol-Security
20. https://www.arabes1.com/2013/11/DMZ.html
21. http://www.networkset.net/2010/10/22/ids-vs-ips/
22. https://www.techtarget.com/searchsecurity/definition/firewall
23. https://www.geeksforgeeks.org/introduction-of-firewall-in-computer-network/
24. https://techprosoh.com/fortinets-fortigate/
25. https://www.axians.co.uk/news/complete-guide-to-fortigate-firewalls/
26. https://www.geeksforgeeks.org/what-is-arp-spoofing-attack/
27. https://community.fs.com/article/what-is-dhcp-snooping-and-how-it-works.html
28. https://www.computernetworkingnotes.com/ccna-study-guide/how-dhcp-snooping-works-explained.html
29. https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/