كلية الحاسبات والذكاء الإصطناعي

جامعة سوهاج

SIMULATION OF A SMART NETWORK COMPANY

Level 4 [2023]

FEBRUARY 13, 2023

Project Team

number	name
1	Mahmoud Hassan Hegazy
2	Abdelmalik Ahmed Abdelaziz
3	Abdelrahman Ali Hamdan Ali
4	Abdallah Ragab Fawzy Mahmoud
5	Abdelgaber Elsayed Abdelgaber Hamed
6	Ahmed Hamouda Ahmed Ahmed

Supervisors

1	Dr. Hamdy Hasan
2	Dr.Shreen Khalaf
3	Dr.Mohamed Khalil

Examination Committee

1	Prof.Dr. Ahmed Abdelhakem
2	Prof.Dr. Hamdy Hasan
3	Prof.Dr. Hanan Hamed

Acknowledgement

At the beginning, we would be remiss if we fail to express our profound gratitude to Allah who always we ask for his help and we owing to him with any success and progress we made in our life. We are obliged to everyone who assisted us during that time to get out with this knowledge and results presented in this book. In particular, we want to express our gratitude to our supervisor Dr.Hamdy Hasan for all the valuable advice, encouragement, and discussions. The opportunity to work with him was a precious experience, he exerts all the effort and time to help us to learn, search, and do our best in this project. Thanks to Dr.Shreen Khalaf for her advice and encouragement. Really no matter what we mentioned, we will not list part of her mighty effort that she did with us. she was as our sister. Most of all, we thank our beloved families for their immeasurable support, encouragement, and patience while working on this project. Without their love and understanding, this book and our project would not have come to fruition.

Contents:

Chapter (1)

Introduction

Chapter (2)

Routing & switching

Chapter (3)

Voice Over Internet Protocol (VOIP)

Chapter (4)

SERVER

Chapter (1)

Introduction

1.1 Abstract

Simulation methodology is becoming increasingly popular among computer network researchers worldwide in recent years.

This popularity results from the availability of various sophisticated and powerful simulation software packages, and also because of the flexibility in model construction and validation offered by simulation. For selecting an appropriate network simulator for a particular application, it is important to have knowledge of the simulator tools available, along with their strengths and weaknesses.

It is also important to ensure that the results generated by the simulators are valid and credible.

In this paper we describe, classify, and compare network simulators to aid researchers and developers in selecting the most appropriate simulation tool.

A recommendation for best practice in network simulation is also included.

1.2 Introduction

The goal of using any simulator is to accurately model and predict the behavior of a real world system.

Computer network simulation is often used to verify analytical models, generalize the measurement results, evaluate the performance of new protocols that are being developed, as well as to compare the existing protocols.

However, there is always a potential problem when using simulation in testing protocols because the results generated by a simulator are not necessarily accurate or representative.

To overcome this, it is important for network researchers and developers to choose a good simulator which is easy to use; more flexible in model development,

modification and validation; and incorporates appropriate analysis of simulation output data, pseudo-random number generators, and statistical accuracy of the simulation results (i.e., desired relative precision of errors and confidence interval).

To select a good simulator for a particular application, it is also important to have good knowledge of the available simulation tools.

Networking is referred as connecting computers electronically for the purpose of sharing information.

Resources such as files, applications, printers and software are common information shared in a networking. The advantage of networking can be seen clearly in terms of security, efficiency, manageability and cost effectiveness as it allows collaboration between users in a wide range.

Basically, network consists of hardware component such as computer, hubs, switches, routers and other devices which form the network infrastructure.

These are the devices that play an important role in data transfer from one place to another using different technology such as radio waves and wires.

There are many types of network available in the networking industries and the most common network are Local Area Network (LAN) and Wide Area Network (WAN).

LAN network is made up of two or more computers connected together in a short distance usually at home, office buildings or school.

WAN is a network that covers wider area than LAN and usually covers cities, countries and the whole world.

Several major LAN can be connect together to form a WAN.

As several devices are connected to network, it is important to ensure data collision does not happened when this devices attempt to use data channel simultaneously.

A set of rules called Carrier Sense Multiple Access / Collision detection are used to detect and prevent collision in networks.

1.3 General idea of project topology

The project aims to create a WAN network for a company that has two branches located in two different areas, where it is difficult to connect them with cables, so we have to use wireless, and to facilitate communication between company members within the company and between the two branches, and to facilitate the management of the company from file management and transfer, and to establish a security system against intrusions.

1.4 Problem And Definition

It is easy to implement a network for a company, but it is difficult to implement an integrated network in terms of security, speed, and ease of use.
Therefore, in this project, we will implement a network that contains a system. This system follows certain rules, and no one has the right to change these rules other than an admin.

Network Definitions :-

A group of devices connected together to share Information, Resources & Connection

Importance of Network :-

Easy sharing of :

1- information (files & folders)

- Through the network, I can put the employees' data (files and folders) in a central place, such as a server, and we share it so that all the employees included in the network can make a connection to the server and deal with the data at the same time.

2- Resources

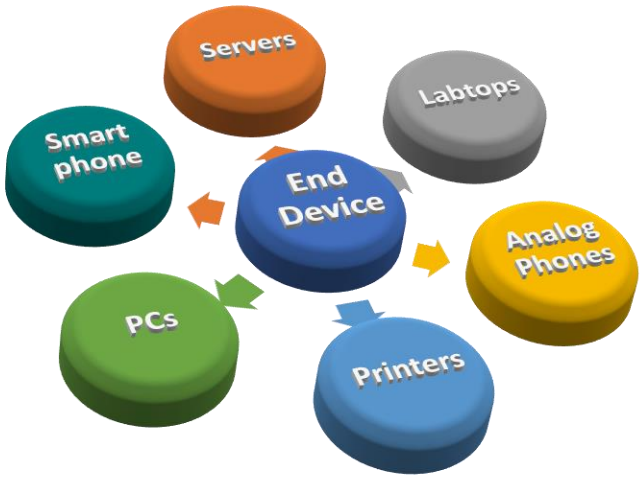
- I cannot buy a printer for each employee. I will only have one printer in each department, and we share the printer and make all users in this department connect to the printer and they can print on it at the same time.
- It is also possible that Resource is expensive software or an expensive program. I cannot bring this software to every device I have.
- The solution is to bring one program and put it on the server and share it. Through the network, users can make a connection to the server and work on this program.

3- Connections

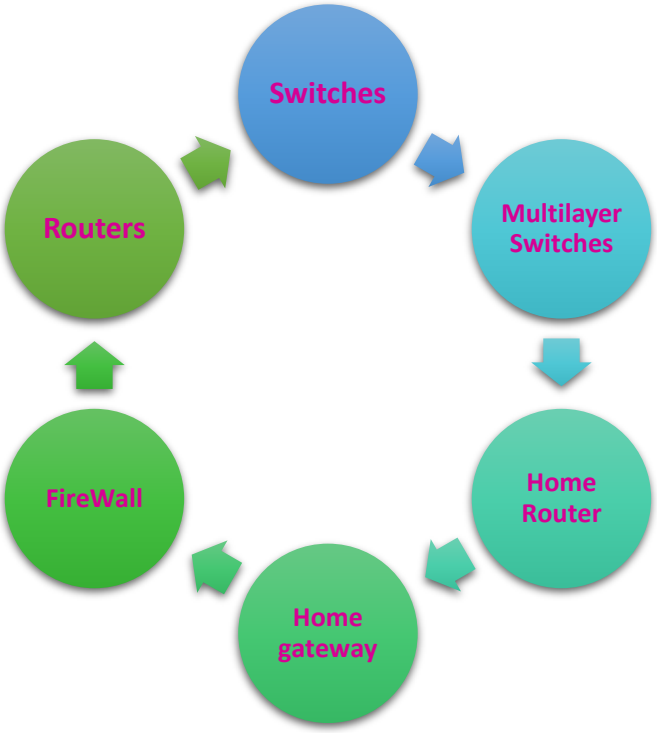
- I cannot bring an internet line for each device. I bring one internet line with a high speed that can cover all the employees I have, and through the network all the employees can go out on the Internet through one net line

Project Components :-

1- End Device



2- Network Devices



3- Connectivity

1.5 Smart Company Architecture (Topology)

1- Branch (USA)

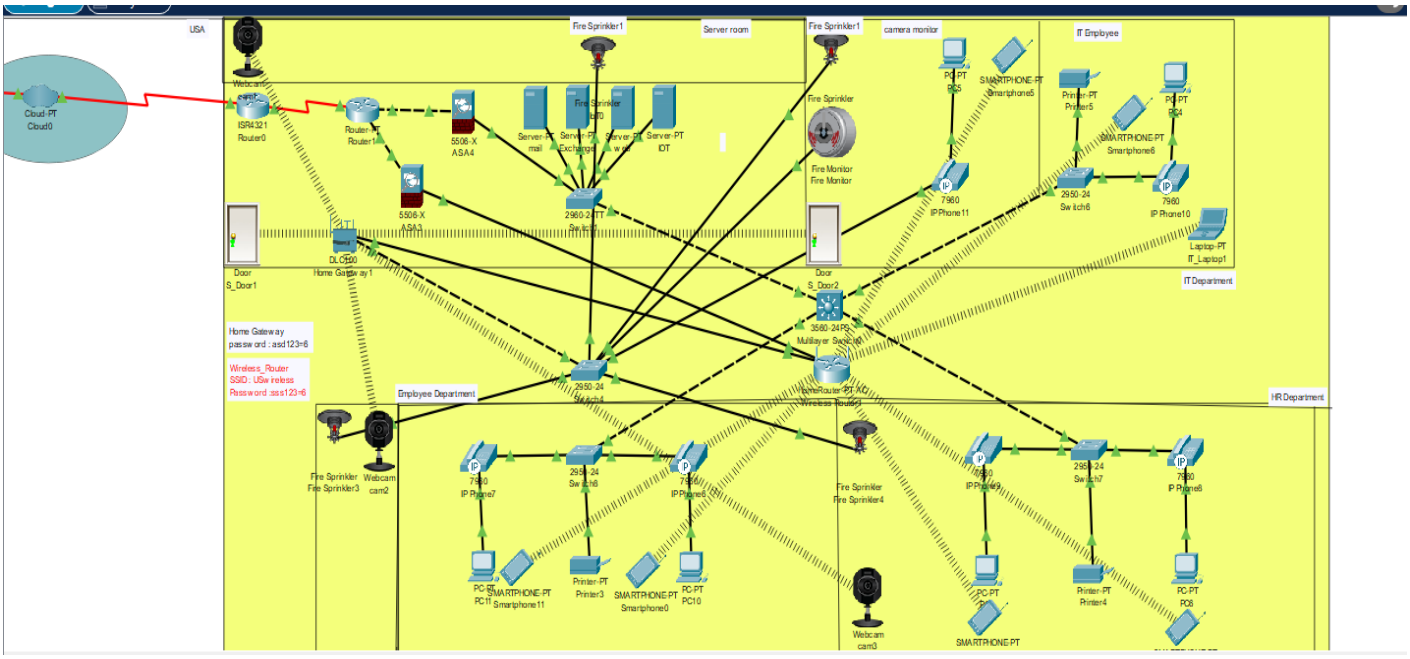


Fig (1): shows the total schematic architecture of the design model for branch 1

2- Branch 2 (EGY)

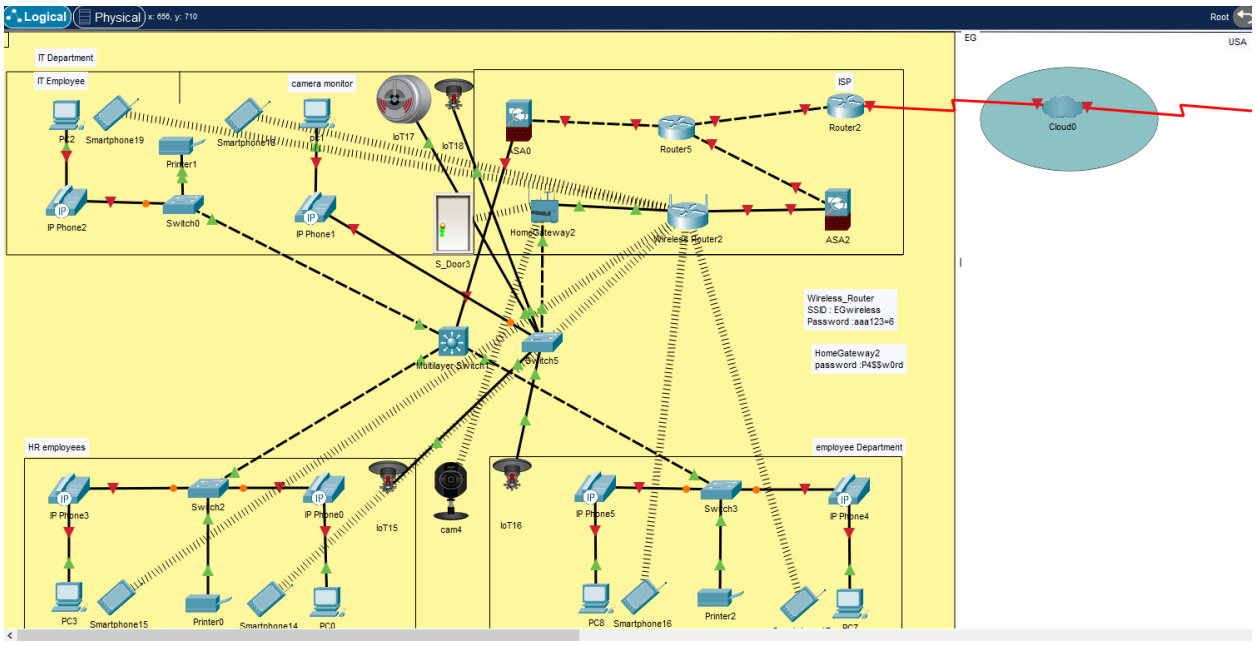


Fig (2): shows the total schematic architecture of the design model for branch 2

CHAPTER (2)

Routing & Switching

2.1 Introduction :-

In this chapter we are going to talk about

- **Routing**
- **Switching**
- **Subnetting**

2.2 what is the router ?

A router is a device that connects two or more packet-switched networks or sub networks . It serves two primary functions: managing traffic between these networks by forwarding data packets to their intended IP addresses, and allowing multiple devices to use the same Internet connection.

There are several types of routers, but most routers pass data between LANs (local area networks) and WANs (wide area networks). A LAN is a group of connected devices restricted to a specific geographic area. A LAN usually requires a single router.

A WAN, by contrast, is a large network spread out over a vast geographic area. Large organizations and companies that operate in multiple locations across the country, for instance, will need separate LANs for each location, which then connect to the other LANs to form a WAN. Because a WAN is distributed over a large area, it often necessitates multiple routers and switches ,and we can use static routing or dynamic routing .

fig 2.1

2.3 Routing

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

2.3.1 Static Routing

Static routes are user-defined route that specify the path that packets moving between source to destination that uses a route that a network administrator enters into the router manually.

The administrator must manually update his static route entry whenever an internetwork topology changes require an update**.**

Advantages of static routing

- Static routing causes very little load on the CPU of the router, and produces no traffic to other routers.
- Static routing leaves the network administrator with full control over the routing behavior of the network.
- Static Routing is very easy to configure on small networks.

Disadvantages of static routing

- Network changes require manual reconfiguration
- Does not scale well in large topologies

2.3.2 Default Routing

Default Routing is something called gateway of last resort, when a specific route to a particular network does not exist, a router will drop all the packets destined to that specific network. Router forward packets using a default route when there is no specific routes that match a packet's destination IP address in the routing table. The default route can be identified by all zeros in both the network and sub net

mask (0.0.0.0 0.0.0.0). It is the least specific route possible. Default route are also use to connect ISP site or head site.

```
     172.16.0.0/24 is subnetted, 5 subnets
C       172.16.10.0 is directly connected, FastEthernet0/0
C       172.16.20.0 is directly connected, Serial2/0
S       172.16.30.0 [1/0] via 172.16.20.2
S       172.16.40.0 [1/0] via 172.16.20.2
S       172.16.50.0 [1/0] via 172.16.20.2

Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#no ip route 172.16.30.0 255.255.255.0 172.16.20.2
Router(config)#no ip route 172.16.40.0 255.255.255.0 172.16.20.2
Router(config)#no ip route 172.16.50.0 255.255.255.0 172.16.20.2
Router(config)#ip route 0.0.0.0 0.0.0.0 172.16.20.2
Router(config)#do sh ip route
```

fig 2.3

2.3.3 Dynamic Routing

Dynamic routing is a networking technique that provides optimal data routing. Unlike static routing, dynamic routing enables routers to select paths according to real-time logical network layout changes. In dynamic routing, the routing protocol operating on the router is responsible for the creation, maintenance and updating of the dynamic routing table. In static routing, all these jobs are manually done by the system administrator.

2.4 Routing Protocols Class

Distance vector The distance-vector protocols in use today find the best path to a remote network by judging distance (EX: RIP)

Link state In link-state protocols, also called shortest-path-first (SPF) protocols,.

OSPF is an IP routing protocol that’s completely link-state.

Advanced distance vector Advanced distance-vector protocols use aspects of both distance vector and link-state protocols, and **EIGRP** is a great example

Table (1)

Characteristic	OSPF	RIPv2	RIPv1
Type of protocol	Link state	Distance vector	Distance vector
Classless support	Yes	Yes	No
Path metric	Bandwidth	Hops	Hops
Hop count limit	None	15	15
Convergence	Fast	Slow	Slow
Hierarchical network requirement	Yes (using areas)	No (flat only)	No (flat only)

And based on the previous table, it turns out that OSPF is the most appropriate protocol that we can use in the project before you

So we are going to talk in more detail about the OSPF routing protocol

2.5 Open Shortest Path First (OSPF)

- Standard Protocol

- Classless Protocol
- Offers an unlimited hop count (Hierarchical)
- Loop Free
- Administrative distance=110

OSPF Terminology

- **Link** A *link* is a network or router interface assigned to any given network
- **Router ID** The *router ID (RID)* is an IP address used to identify the router.
- **Neighbor** *Neighbors* are two or more routers that have an interface on a common network
- **Adjacency** An *adjacency* is a relationship between two OSPF routers that permits the direct exchange of route updates.
- **Designated router** A *designated router (DR)* is elected whenever OSPF routers are connected to the same broadcast network .
- **Hello protocol** provides dynamic neighbor discovery and maintains neighbor relationships.
- **Hello packets** and Link State Advertisements (LSAs) build and maintain the topological database.
- **Hello packets** are addressed to multicast address 224.0.0.5.
- **Neighbor ship database** is a list of all OSPF routers for which Hello packets have been seen.
- Including the router ID and state, are maintained on each router in the neighbor ship database.
- **Topological database** contains information from all of the Link State Advertisement packets that have been received for an area.
- The router uses the information from the topology database as input into the Dijkstra algorithm that computes the shortest path to every network

- **Link State Advertisement (LSA)** is an OSPF data packet containing link-state and routing information that's shared among OSPF routers.
- **OSPF areas** An OSPF area is a grouping of contiguous networks and routers. All routers in the same area share a common area ID.
- All of the routers within the same area have the same topology table.
- An area 0 and that this is typically considered the backbone area.
- Areas also play a role in establishing a hierarchical network organization.

OSPF Operation

- Each Router Will send Hello packet to all its interface to discover its direct connected neighbors
- Each router will sent LSA to all its neighbors, telling them about its LSA's
- Every Router receive LSA packet will take copy of it and send it as it is to its neighbors
- Each Router Will Form LSDB(Link Stat DB) for all LSA's
- Each Router Will draw a link state tree and put itself as the root of the tree
- Each router will apply OSPF algorithm to get the routing table

OSPF operation is basically divided into these three categories

1. Neighbor and adjacency initialization
2. LSA flooding
3. SPF tree calculation

Configuring OSPF

Enabling OSPF Router(config)#**router OSPF ?**<1-65535> Process ID

Process ID: is value in the range from 1 to 65,535 identifies the OSPF.

Configuring OSPF Areas

Newtork directConnectedNetIP wildCardMaskarea 0

Wild Card Mask : inverted of subnet mask

Wild card Mask=255-subnet mask

2.6 SWITCHING

2.6.1 what is the switch ?

A network switch is a physical device that operates at the Data Link layer of the Open Systems Interconnection (OSI) model -- Layer 2.

It takes in packets sent by devices that are connected to its physical ports, and forwards them to the devices the packets are intended to reach.

Switches can also operate at the Network Layer (Layer 3) where routing occurs.

Switches are a common component of networks based on Ethernet, Fibre Channel, Asynchronous Transfer Mode (ATM), and InfiniBand, among others. However, most switches today use Ethernet.

fig 2.7

According to that

We need to know more about switches that operate at layer 3

So we will talk about **multilayer switch**

2.6.2 Multilayer Switch

A multilayer switch is a network device that has the ability to operate at higher layers of the OSI reference model, unlike the Data Link Layer (DLL) traditionally used by switches. A multilayer switch can perform the functions of a switch as well as that of a router at incredibly fast speeds. A switch traditionally inspects frames, while a multilayer switch inspects deeper into the protocol description unit (at packet or even at segment level). Multilayer switches use ASIC hardware circuits to perform routing functions. This differs from typical routers, which reside on a microprocessor and use applications running on it to perform their routing operations.

fig 2.8

2.7 VLAN

A virtual LAN (VLAN) is a logical overlay network that groups together a subset of devices that share a physical LAN, isolating the traffic for each group. A LAN is a group of computers or other devices in the same place -- e.g., the same building or campus -- that share the same physical network.

2.7.1 Benefit of using VLAN

- Reduce Overhead
- Group Users by department or function

- the layout of the network equipment does not match the organization's structure
- more Security as we can keep sensitive device on VLAN

2.7.2 Set up a VLAN-based network

- the network administrator decides how many VLANs there will be,
- which computers will be on which VLAN,
- what the VLANs will be called

2.7.3 Configuring VLANs

Create two vlans10,20 on switch

Switch>enable

Switch#config t

Switch(config)#vlan10

Switch(config-vlan)#vlan20

Verify that the two vlans are created by run

show vlan commands

```
Switch#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
10   VLAN0010                         active
20   VLAN0020                         active
```

Fig 2.9

Configure switch ports

- Switch(config)#interface range f0/1-2
- Switch(config-if-range)#switchportaccess vlan10
- Switch(config-if-range)#interface range f0/3-4
- Switch(config-if-range)#switchportaccess vlan20
- Switch(config-if-range)#intrange fa0/1-4
- Switch(config-if-range)#switchportmode access

2.8 Subnetting

What is a subnet?

A subnet, or subnetwork, is a network inside a network. Subnets make networks more efficient. Through subnetting, network traffic can travel a shorter distance without passing through unnecessary routers to reach its destination.

What is a subnet mask?

A subnet mask is like an IP address, but for only internal usage within a network. Routers use subnet masks to route data packets to the right place. Subnet masks are not indicated within data packets traversing the Internet — those packets only indicate the destination IP address, which a router will match with a subnet.

Why is subnetting necessary?

As the previous example illustrates, the way IP addresses are constructed makes it relatively simple for Internet routers to find the right network to route data into. However, in a Class A network (for instance), there could be millions of connected devices, and it could take some time for the data to find the right device. This is why subnetting comes in handy: subnetting narrows down the IP address to usage within a range of devices.

Because an IP address is limited to indicating the network and the device address, IP addresses cannot be used to indicate which subnet an IP packet should go to. Routers within a network use something called a subnet mask to sort data into subnetworks.

CHAPTER (3)

Voice Over Internet Protocol (VOIP)

3.1 Introduction

Voice Over Internet Protocol (VoIP) is a category of hardware and software that enables voice calls to be made and received over the internet.

VoIP allows users to send and receive voice calls over the internet, without the need for traditional telephones or circuit transmission. Instead, VoIP sends voice data as data packets that are delivered over a packet-switched network with media delivery protocols that allow callers to speak and listen as if they were talking over a PSTN connection.

VoIP is particularly popular in contact centers for its cheaper price point and tight integration capabilities with CRM systems. Although special VoIP-enabled desktop "hard" phones have been used in contact centers for many years, most contact centers now simply use a headset equipped with a microphone to connect the agent and caller. This is known as a "soft" phone.

VoIP also has functionality advantages over conventional telephony. Incoming calls can be easily routed to a VoIP phone, no matter where in the network it is physically plugged in, allowing "phones" to be anywhere with a stable internet connection. Calls can be routed in concert with any number of digital protocols, and contact center agents can work remotely from anywhere using a VoIP phone. This makes call center scalability a much more practical reality than with conventional telephony alone.

3.2 VoIP (Voice Over Internet Protocol) phone – Definition

As mentioned, VoIP stands for Voice Over Internet Protocol (you might hear it referred to as IP telephony, too), and it's a technology that enables you to make and receive voice calls over the internet.

Traditionally, callers communicated over the Public Switched Telephone Network, or PSTN, or what we think of as landlines. VoIP, on the other hand, sends voice communications using data packets over a packet-switched network, which we know as the internet or local area networks (LANs).

All you need to make these calls is a device, an internet connection, a microphone, and VoIP. No traditional phones, analog lines, or circuit transmission is necessary. Simple, right?

VoIP can utilize cell phones, desk phones ("hard phones"), mobile devices, and even computers equipped with headset microphones ("softphones") to connect callers—allowing you to communicate with new or existing hardware.

Whether scaling a call center or expanding your business to include life-changing communications, VoIP can connect you to team members and clients with lower costs and greater functionality.

3.3 IP-Enabled Services

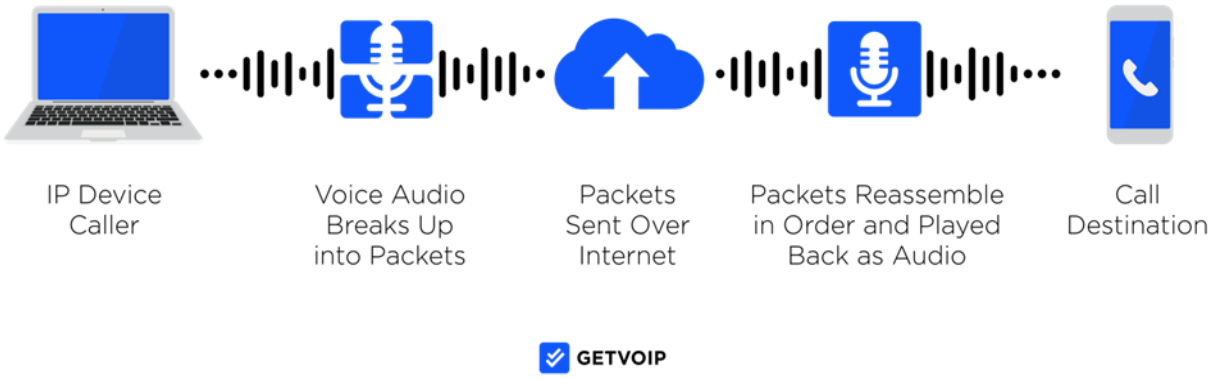
Voice over Internet Protocol (VoIP), is a technology that allows you to make voice calls using a broadband Internet connection instead of a regular (or analog) phone line. Some VoIP services may only allow you to call other people using the same service, but others may allow you to call anyone who has a telephone number - including local, long distance, mobile, and international numbers. Also, while some VoIP services only work over your computer or a special VoIP phone, other services allow you to use a traditional phone connected to a VoIP adapter.

3.4 The role of the VoIP in the project

VoIP can connect you to team members and clients with lower costs and greater functionality, The purpose of using VoIP in this project is to reduce the cost of making calls and facilitate communication between the company's employees in all departments of the company and to make calls at anytime and anywhere using a device connected to the Internet via the VoIP

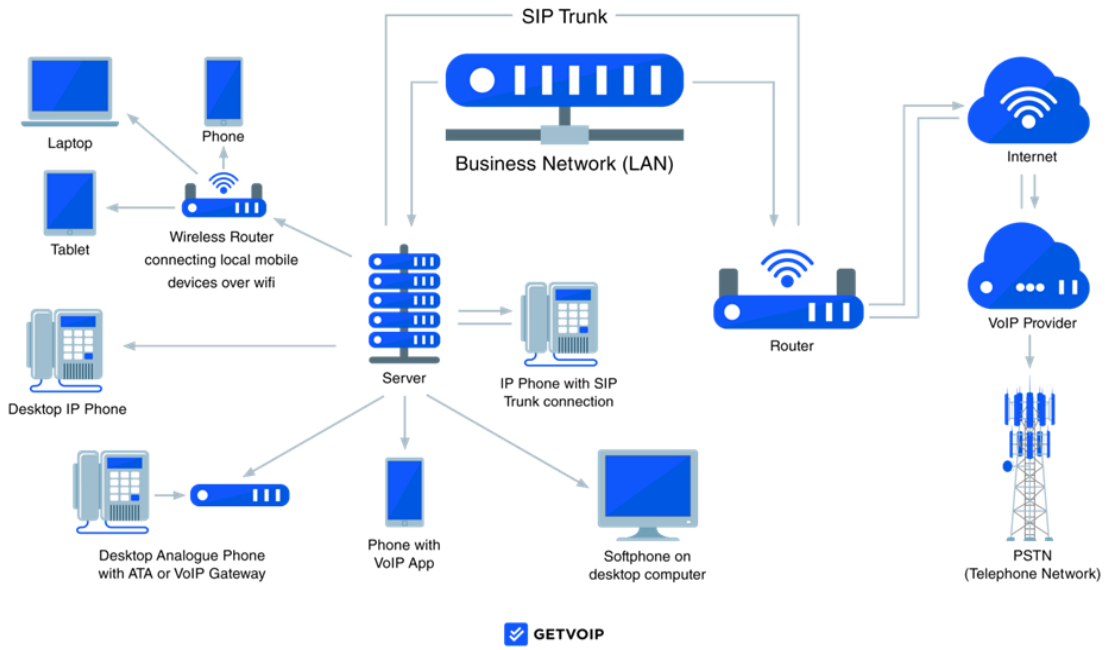
3.5 How Does VoIP Work?

VoIP technology breaks up the voice audio from a phone conversation into digital data packets, then sends **these data packets to the recipient over the Internet.**



Codecs compress/disassemble these voice data packets to travel over the IP network (a local area network or a wide area network.) Once these voice data packets reach their destination, they're decompressed/reassembled and sent to the recipient, transformed back into words and phrases instead of just digital signals in transit.

VoIP users can make calls via VoIP softphones, VoIP phones, and/or by connecting traditional analog phones to a VoIP system via an analog telephone adapter.



3.6 The Pros of VoIP

- Cheaper and more scalable than landline phone service
- More advanced features than standard business phones
- Increased portability and flexibility
- Better overall voice and call quality

VoIP's biggest advantage is how much money it saves on telecommunication costs.

Users can expect to save up to 50% on telecom charges if they switch to VoIP phones. Plus, because you don't have to purchase new equipment (as VoIP works with multiple devices like smartphones and desktop computers), you'll save even more.

Not only that but VoIP is proven to increase employee productivity. Its advanced features can save agents over 30 minutes of call time per day and add an extra 3.5 days of productivity per year per employee. As a whole, VoIP raises team productivity rates by roughly 20%.

The truth is that especially now, it's tough to find a bad thing to say about VoIP aside from its dependence on an excellent Internet connection.

3.7 Conclusion

If you're running a business that gets a lot of calls each day, upgrading your legacy phone system to VoIP can make your life much easier. With the right VoIP platform, you'll be able to manage calls from your computer, collect customer information, and give your employees better tools to work with.

CHAPTER (4)

SERVER

4.1 Introduction

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.

There are many types of servers such as DHCP, DNS, WEB, FTP, Mail Server**.**

4.2 DHCP Server

This protocol is responsible for automatically assigning an IP address to each device connected to the network without any intervention from you.
A DHCP server automatically sends the required network parameters for clients to properly communicate on the network.

Without it, the network administrator has to manually set up every client that joins the network, which can be cumbersome, especially in large networks.

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.

The router/switch DHCP server cannot create an entry into DNS on behalf of the client based on the IPv4 address that was leased to the client.

DHCP is based on a client-server model and based on discovery, offer, request, and ACK. DHCP port number for server is 67 and for the client is 68.

DHCP messages are

1- DHCP Discover

A DHCP client broadcasts this message to locate a DHCP server when the client attempts to connect to a network for the first time.

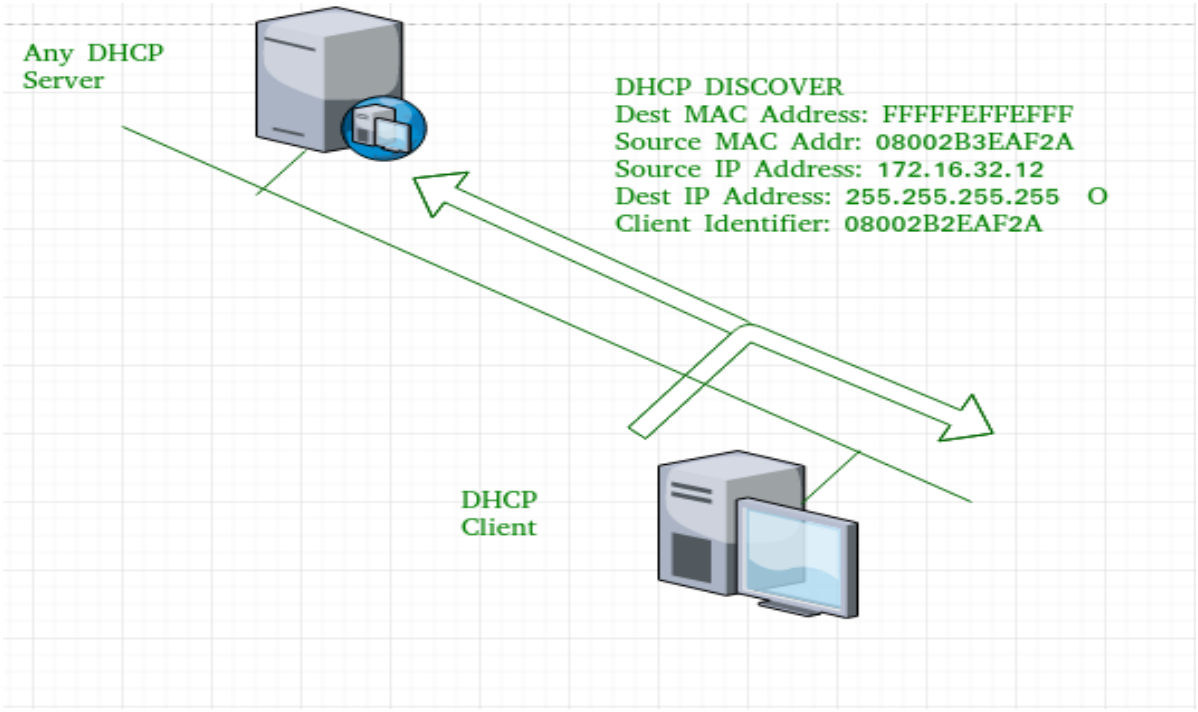


Fig.4.1 DHCP Discover

As shown in the figure, source MAC address (client PC) is 08002B2EAF2A, destination MAC address(server) is FFFFFFFFFFFF, source IP address is 0.0.0.0

(because PC has no IP address till now) and destination IP address is 255.255.255.255 (IP address used for broadcasting).

As the discover message is broadcast to find out the DHCP server or servers in the network therefore broadcast IP address and MAC address is used.

2- DHCP Offer

A DHCP server sends this message in response to a DHCP Discover message. A DHCP Offer message carries configuration information.

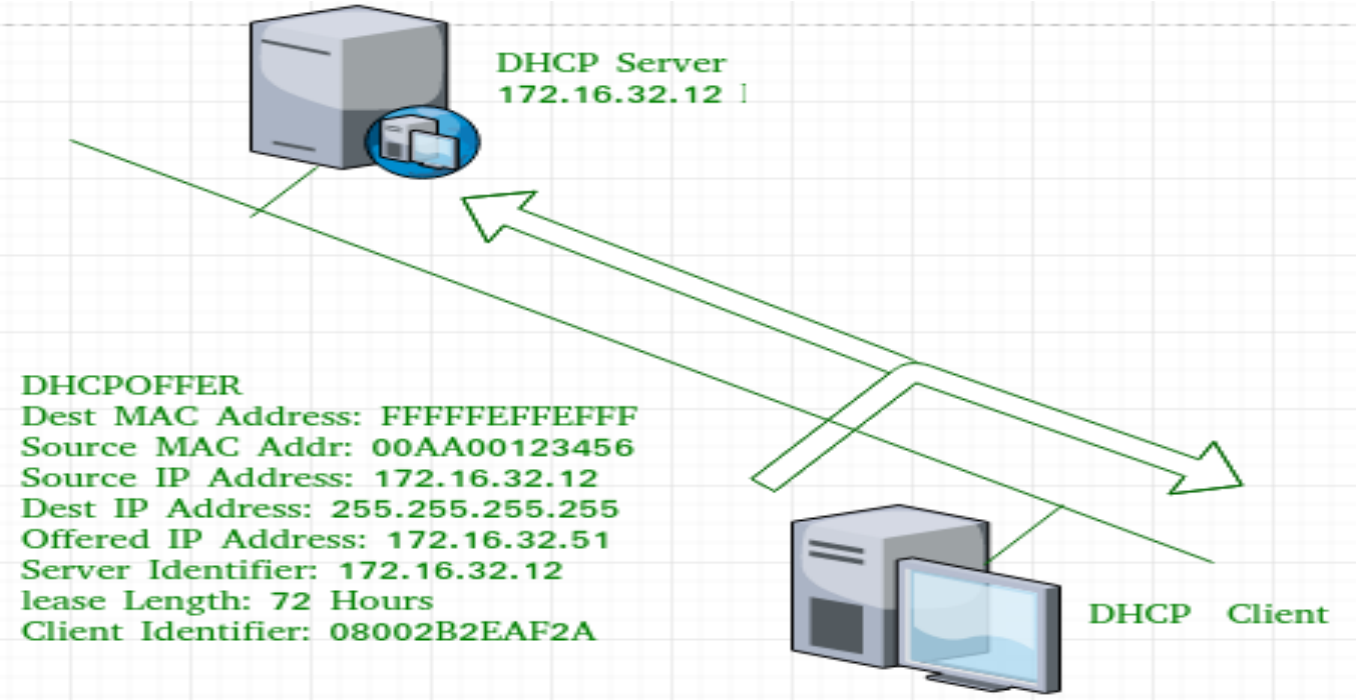


Fig.4.2 DHCP offer

Now, for the offer message, source IP address is 172.16.32.12 (server's IP address in the example), destination IP address is 255.255.255.255 (broadcast IP address) ,source MAC address is 00AA00123456, destination MAC address is FFFFFFFFFFFF.

3- DHCP Request

A DHCP client sends this message in the following scenarios:

- After the client starts, it broadcasts a DHCP Request message to respond to a DHCP Offer message sent by a DHCP server.

- After the client restarts, it broadcasts a DHCP Request message to confirm the configuration (including the allocated IP address).
- After the client obtains an IP address, it unicasts or broadcasts a DHCP Request message to renew the IP address lease.

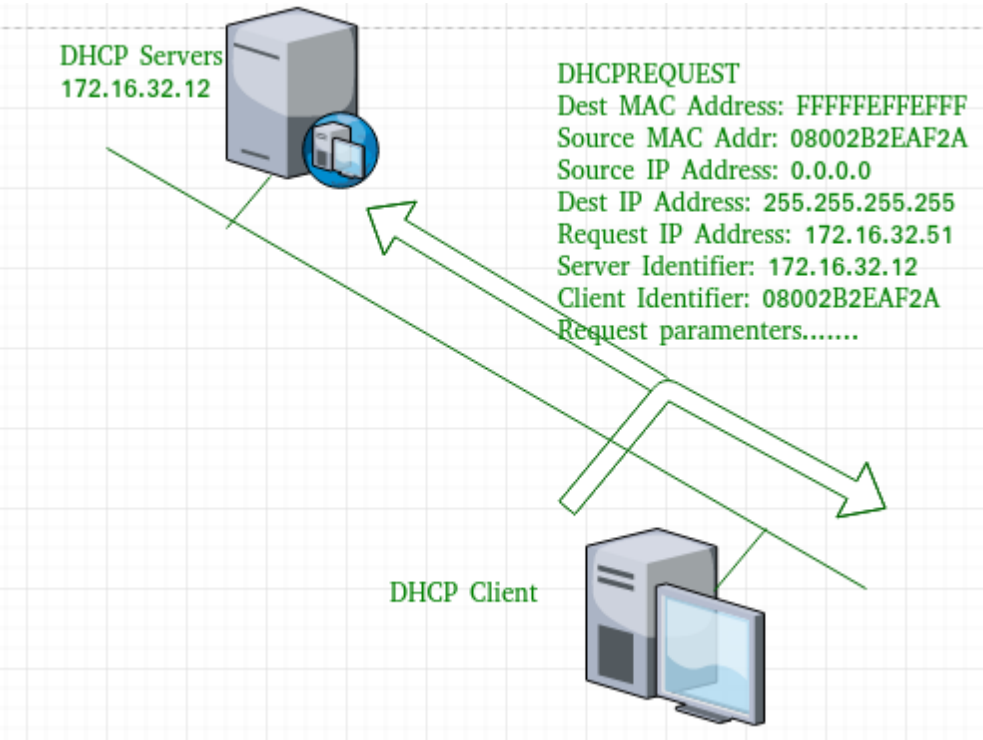
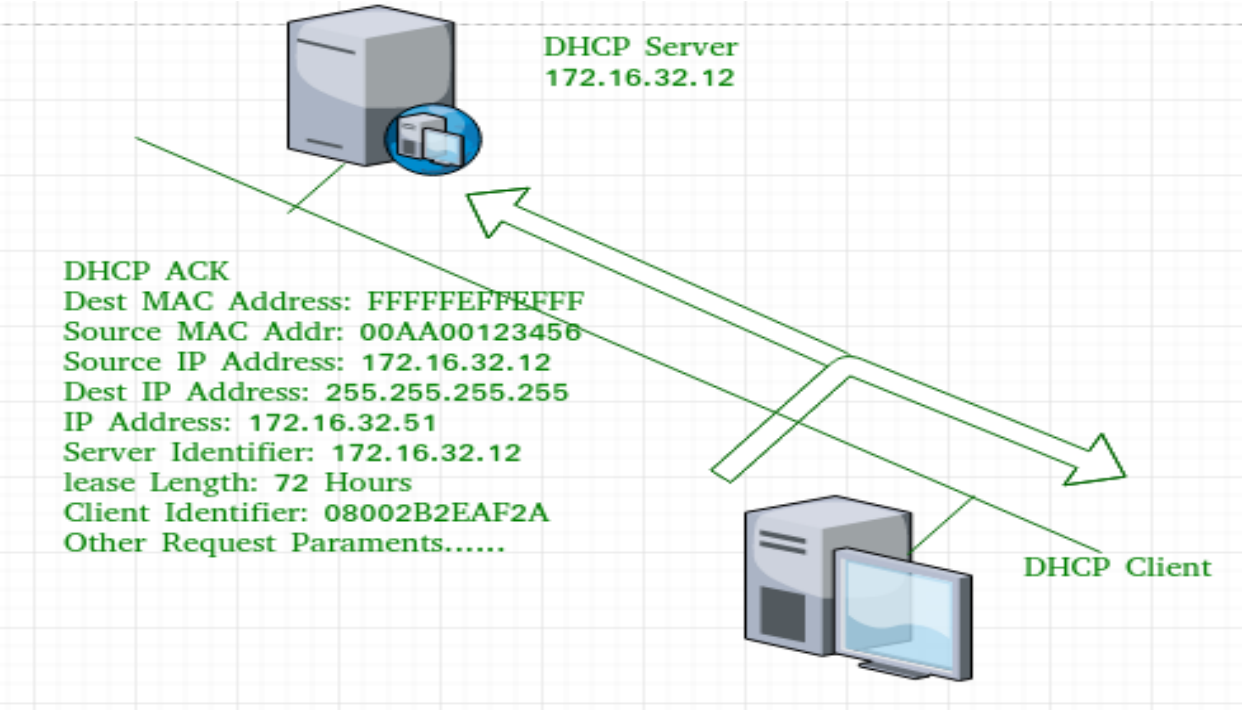


Fig.4.3 DHCP request

Now, the request message is broadcast by the client PC therefore source IP address is 0.0.0.0(as the client has no IP right now) and destination IP address is 255.255.255.255 (broadcast IP address) and source MAC address is 08002B2EAF2A (PC MAC address) and destination MAC address is FFFFFFFFFFFF.

4- DHCP ACK

A DHCP server sends this message to acknowledge a DHCP Request message sent from a DHCP client. After receiving a DHCP Ack message, the DHCP client obtains configuration parameters (including an IP address).



Now the server will make an entry of the client host with the offered IP address and lease time. This IP address will not be provided by server to any other host. The destination MAC address is FFFFFFFFFFFF and the destination IP address is 255.255.255.255 and the source IP address is 172.16.32.12 and the source MAC address is 00AA00123456 (server MAC address).

The advantages of using DHCP include:

1- centralized management of IP addresses.

2- ease of adding new clients to a network.

3- reuse of IP addresses reducing the total number of IP addresses that are required.

4- simple reconfiguration of the IP address space on the DHCP server without needing to reconfigure each client.

The disadvantage of using DHCP is:

1- IP conflict can occur

For example, when connecting devices to a switch with DHCP server which has ip 192.168.1.12/24 and DNS 192.168.1.11

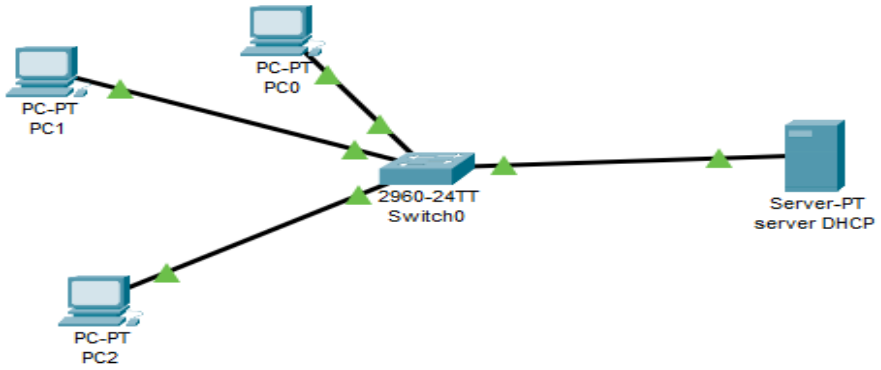
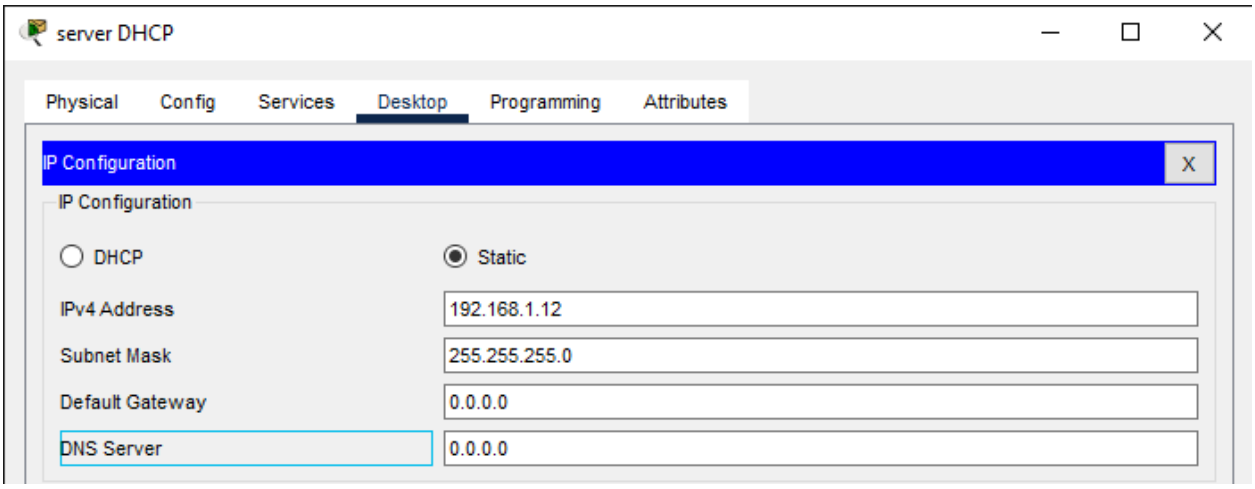
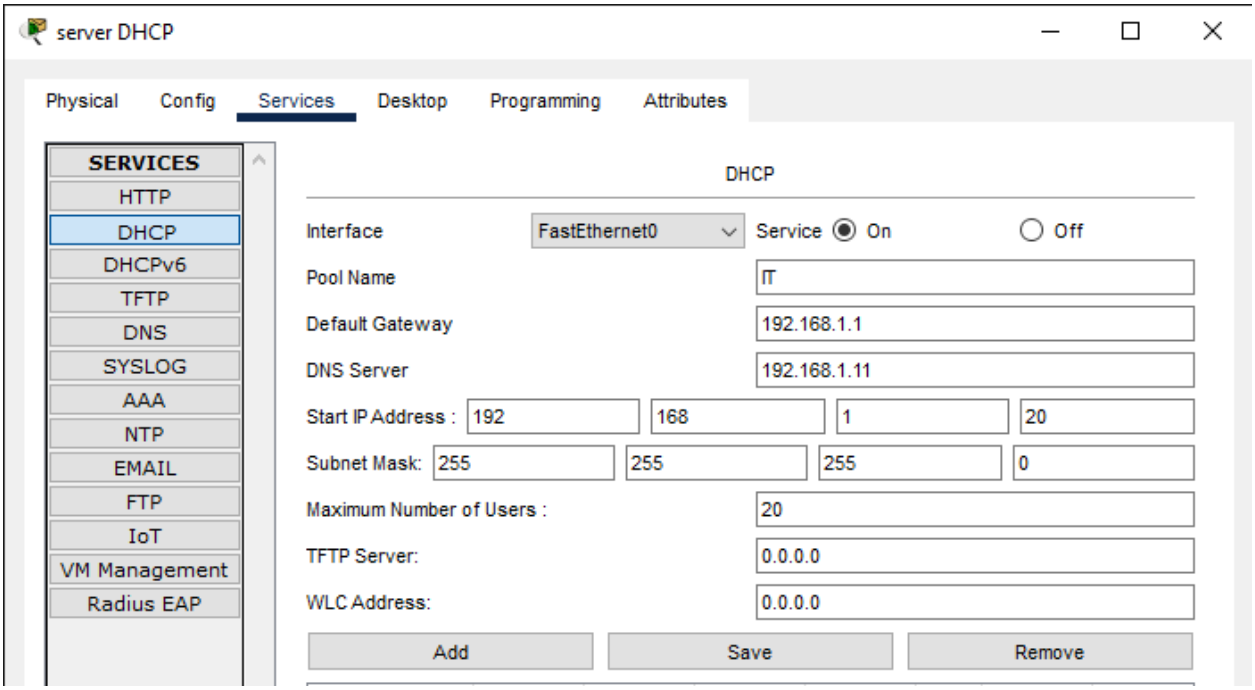
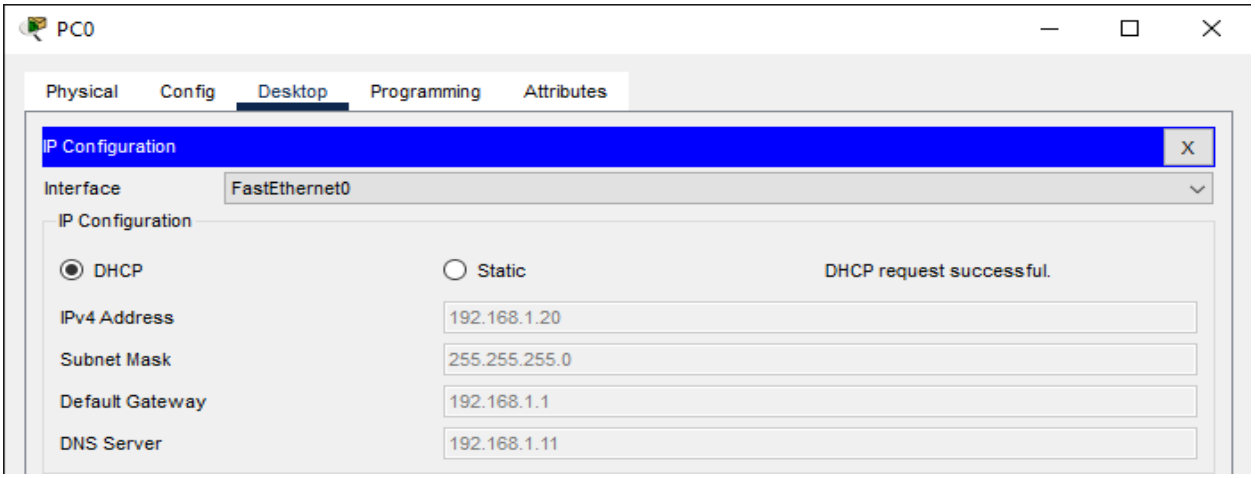


Fig4.5 implementationof DHCP Server

After finishing the topolgy of DHCP Server we put ihe ip of the server 192.168.1.12 and default gateway 192.168.1.1 and dns 192.168.1.11 and active DHCP Protocol. Put the start ip and maximum number of users. Then change the ip mode from static to dynamic







4.2 dns server

A DNS server is a computer server that contains a database of public IP addresses and their associated hostnames, and in most cases serves to resolve, or translate, those names to IP addresses as requested. DNS servers run special software and communicate with each other using special protocols.

The Purpose of DNS Servers

- The DNS server sits in the space between humans and computers to help facilitate their communication.

- It's easier to remember a domain or hostname like lifewire.com than it is to remember the site's IP address numbers 151.101.2.114. So when you access a website, like Lifewire, all you have to type is the URL https://www.lifewire.com.

- However, computers and network devices don't work well with domain names when trying to locate each other on the internet. It's far more efficient and precise to use an IP address, which is the numerical representation of what server in the network (internet) the website resides on.

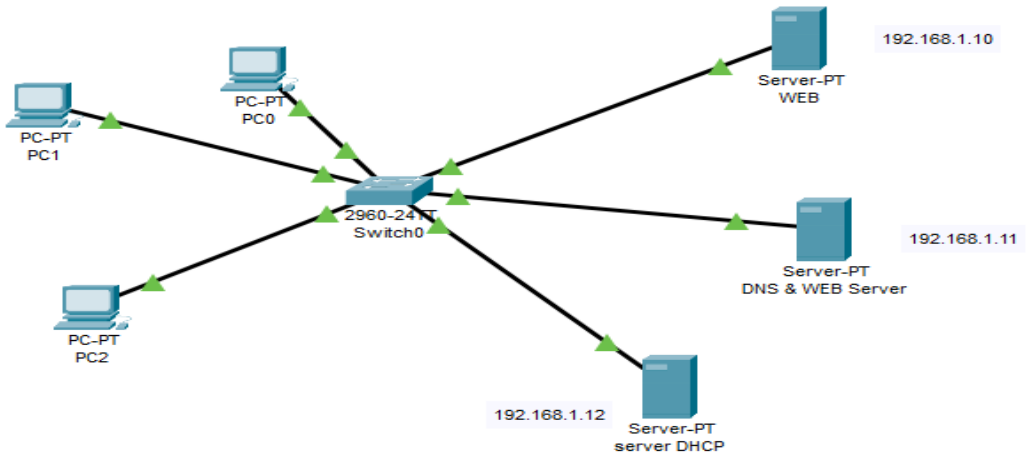
There are various kinds of DOMAIN:

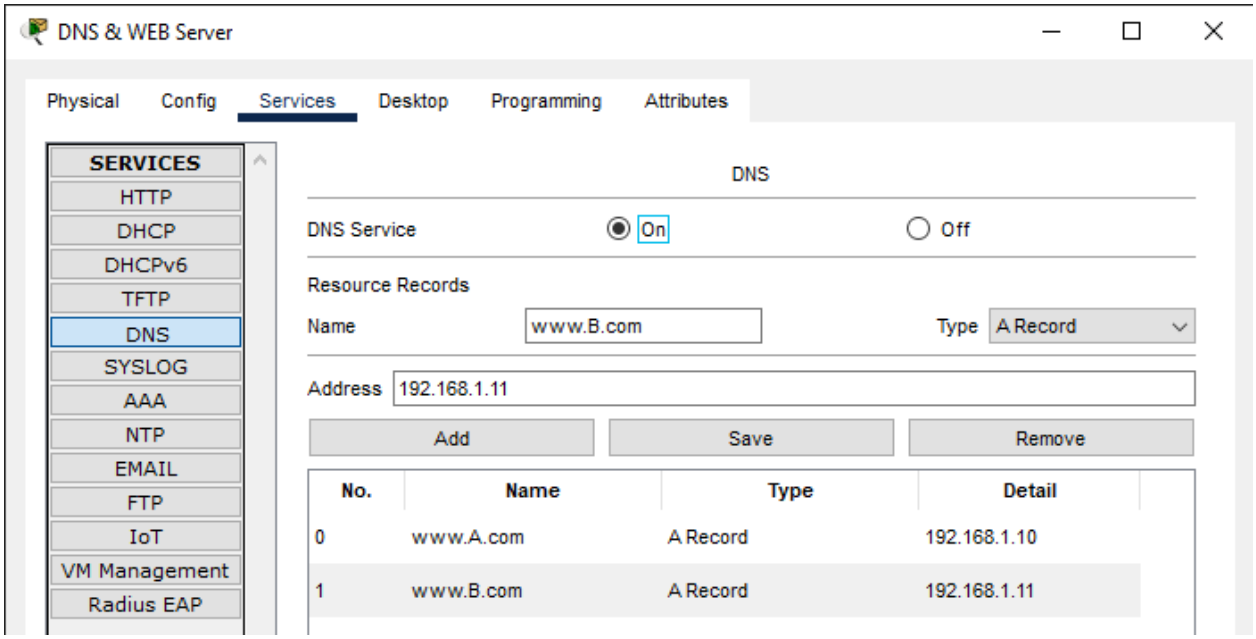
1- Generic domain: .com(commercial) .edu(educational) .mil(military) .org(non profit organization) .net(similar to commercial) all these are generic domain.

2- Country domain .in (india) .us .uk

3- Inverse domain if we want to know what is the domain name of the website. Ip to domain name mapping. So DNS can provide both the mapping for example to find the ip addresses of geeksforgeeks.org then we have to type nslookup www.geeksforgeeks.org.

⇨ When we return to the previous example, we will add a server for dns and another for web. We create a page which has URL www.A.com which has ip is 192.168.1.10 and www.B.com which has ip is 192.168.1.11 in DNS & WEB server.





and we can change in http because when we open the url, we can see like " Hello in the website" . after finishng it, we can go to any pc and open web browser and write any url like www.B.com, and see the sentence, which we wrote it.

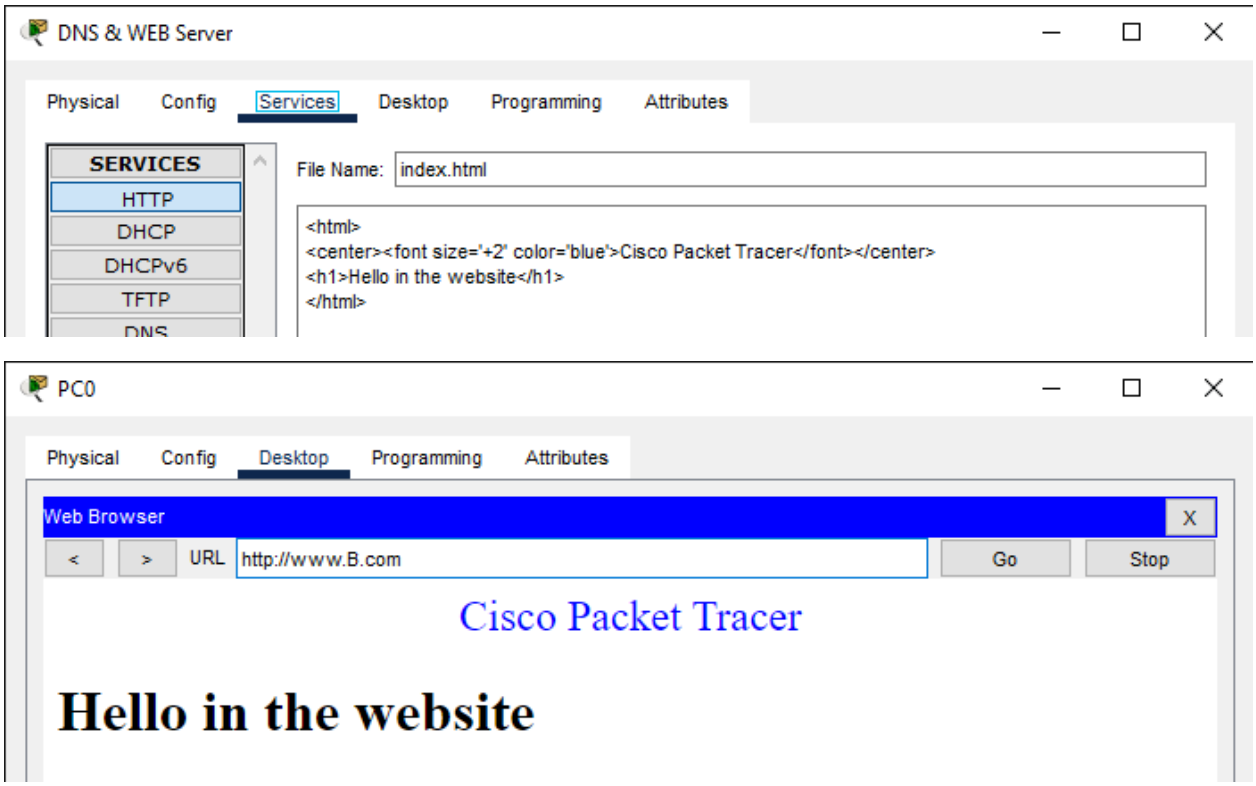


Fig.4.6 5 implementationof DNS Server & WEB

4.3 FTP Server

The computer which uses FTP to transfer data is called the FTP server. It stores and shares client data. Every day thousands of files on the Internet are transferred from one computer to another.

The FTP server stores the address of client files and creates a link to share these files. An FTP server requires a transfer control protocol network or internet protocol network to function. FTP server connection remains connected to FTP clients all the time. It helps in transferring files from one user to another via the Internet. Any user can access the data stored in the FTP server, while some files can be accessed by special users.

It can be considered as the middle layer between the user system and the data. When you transfer the file using the FTP, it is either uploaded or downloaded to the FTP server. The data is transferred from the user system to the FTP server if the user is uploading the data. The data is transferred from the FTP server to the user system if the user is downloading the data.

Types of FTP server

1- Anonymous Server

2- Non-Anonymous Server

Anonymous Server

Anonymous server is a common FTP server, that is for all FTP clients. There is no password required to access this server. Most FTP clients use it.

Non-Anonymous Server

The non-Anonymous server is a paid server. If the user uses the non-anonymous server,the user needs the password to access the file.

Feature of FTP server

1- It provides anonymous access, which means that it permits the user to download data from the server, but it prevents the uploading of the data to the server.
2- FTP server is very useful for those people whose internet speed is very slow.
3- If the download fails for any reason in the FTP server, you can resume that downloading.

Advantages of the FTP server

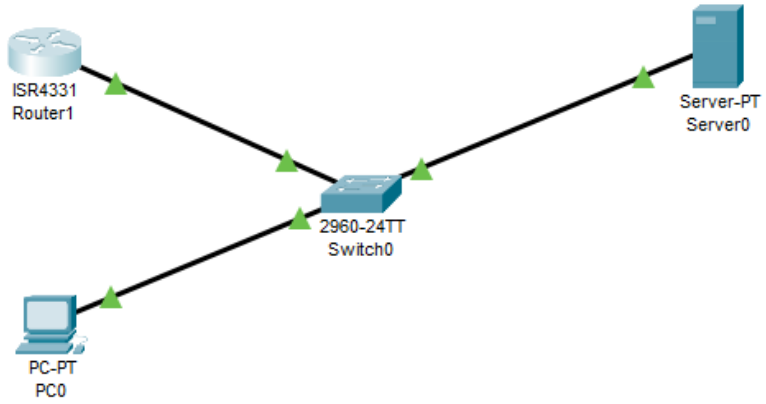
1- The FTP server provides ultimate protection for client data. It gives you the added assurance that your data won't fall into the wrong hands because it stores your data in the encrypted form.

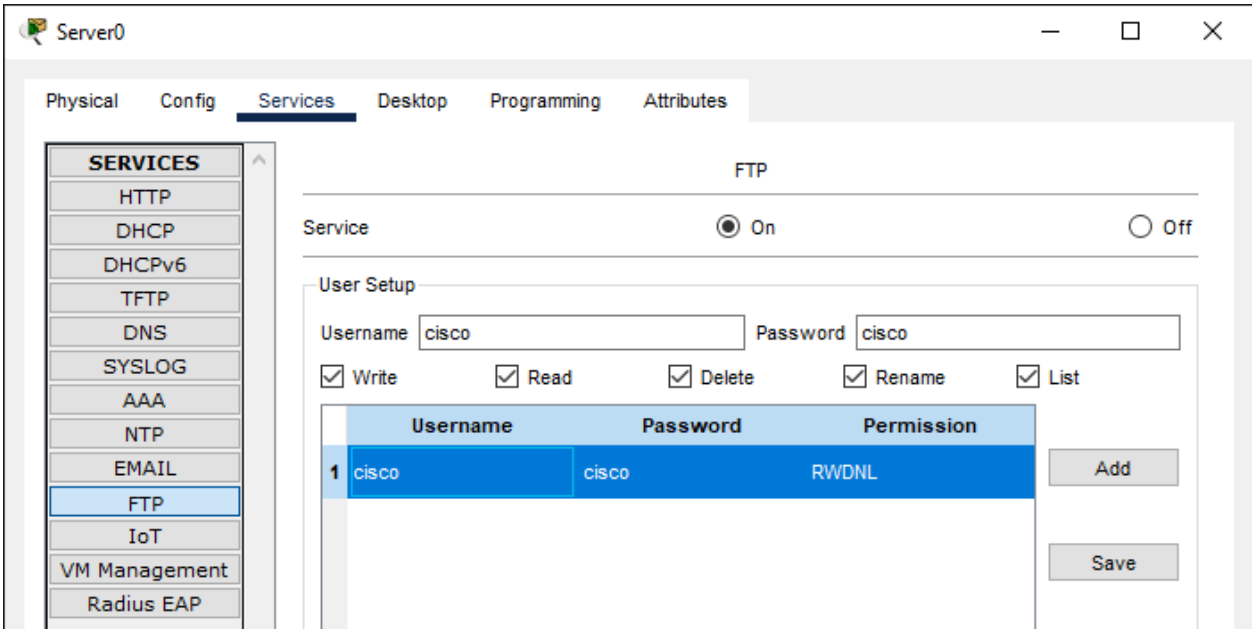
2- If the download fails for any reason in the FTP server, you can resume that downloading.

3- In an FTP server, there is no memory limit to store data.

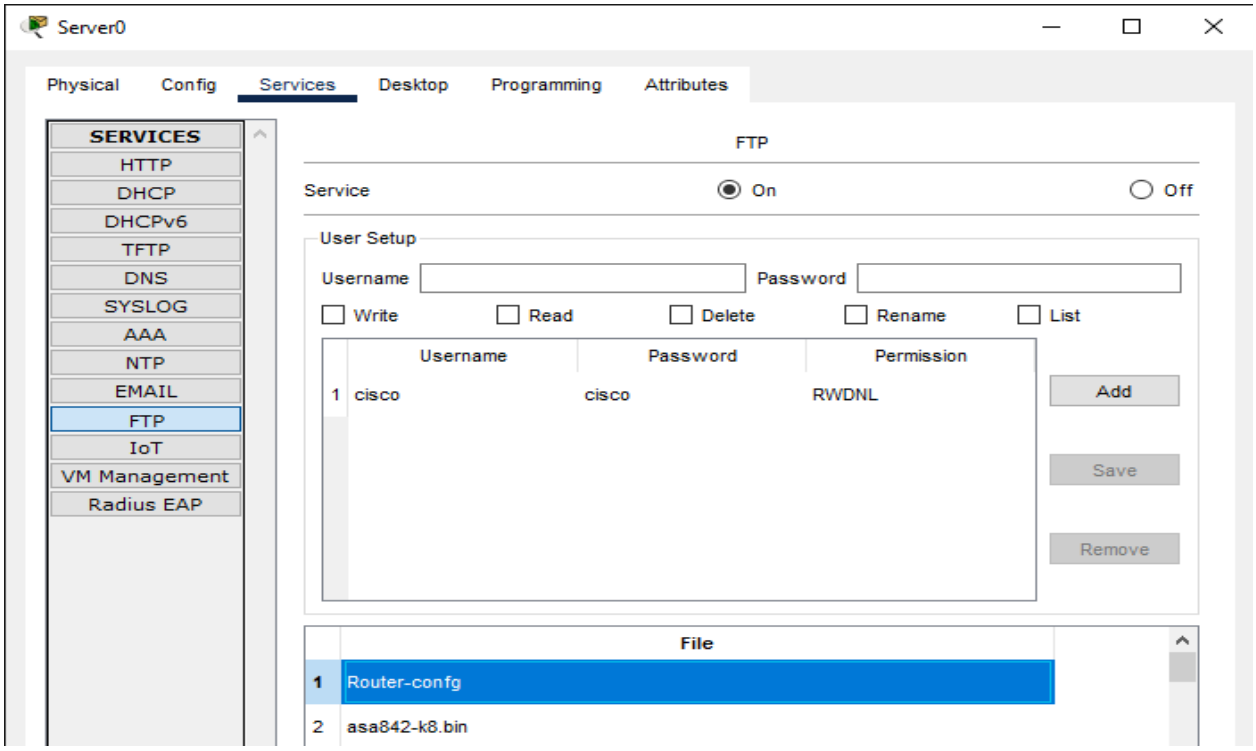
⇨ **For example,** when we connection device to switch and router and FTP Server.and put ip of a server 192.168.1.2/24 and ip of a router 192.168.1.1/24 and ip of a PC 192.168.1.3/24

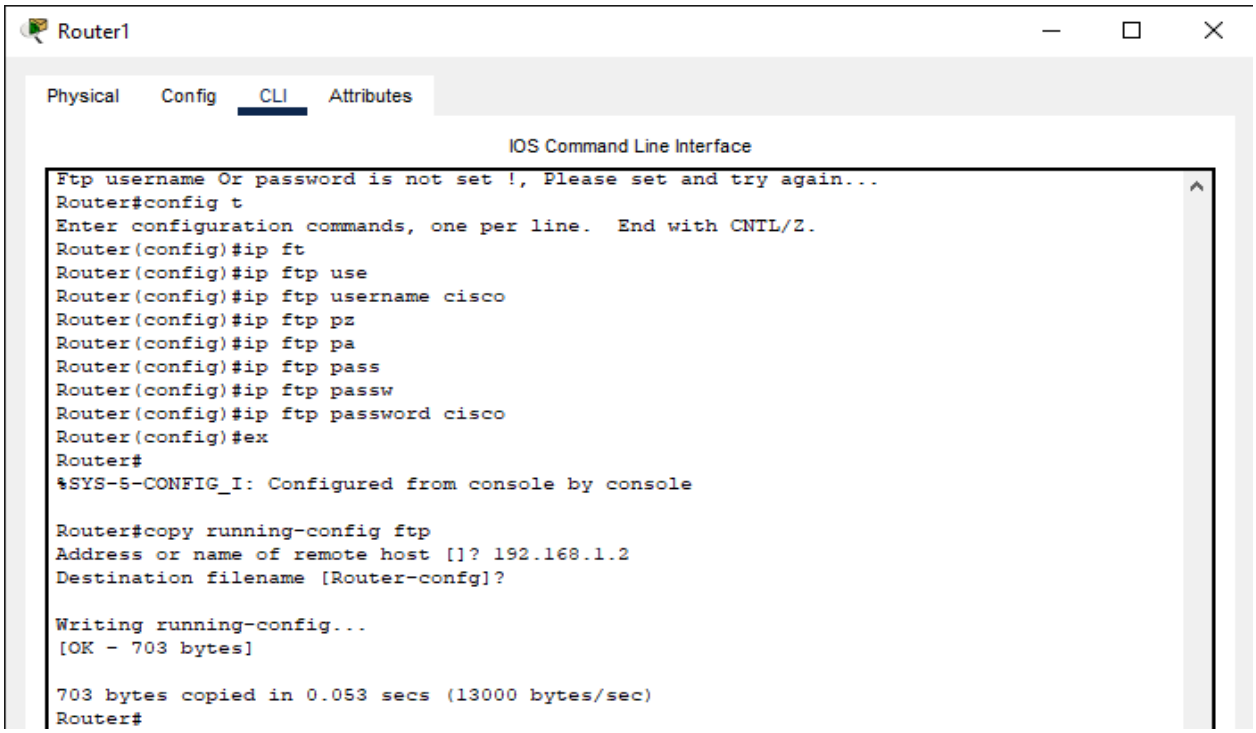
we active ftp server and running the default username and password cisco with have all permission**.**





so we copy the data of the router to ftp server





To confirm that we add the data, we can go to ftp server and check it.

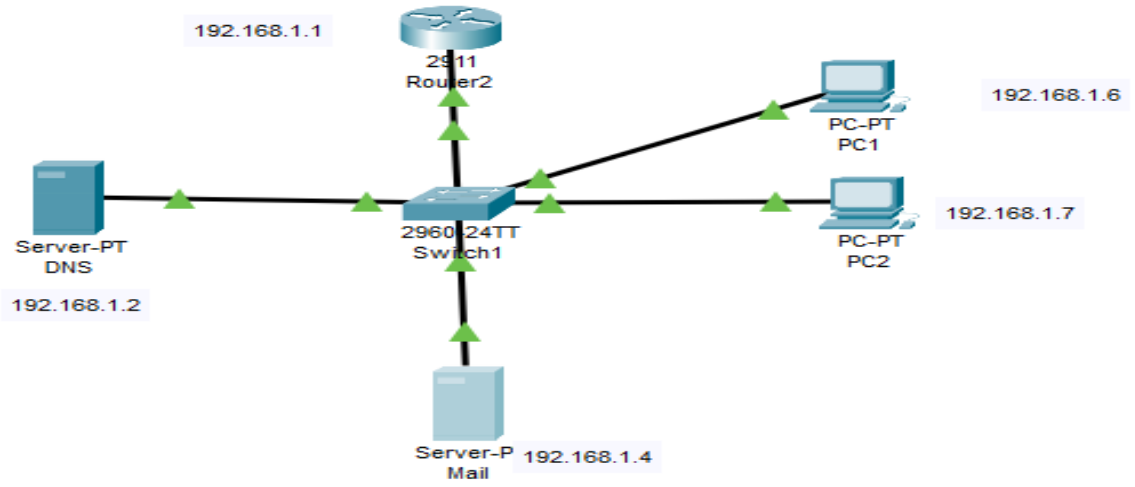
4.4 Mail Server

Mail Server : Mail Server, similar to the post office, is a computer system program responsible for receiving, routing, delivering e-mail. It is also known as MTA (Mail Transfer Agent) and store incoming mail for distribution to users and deliver e-mail to client computers.

Example: Yahoo!, Gmail incoming mail server, Gmail outgoing mail server, etc.

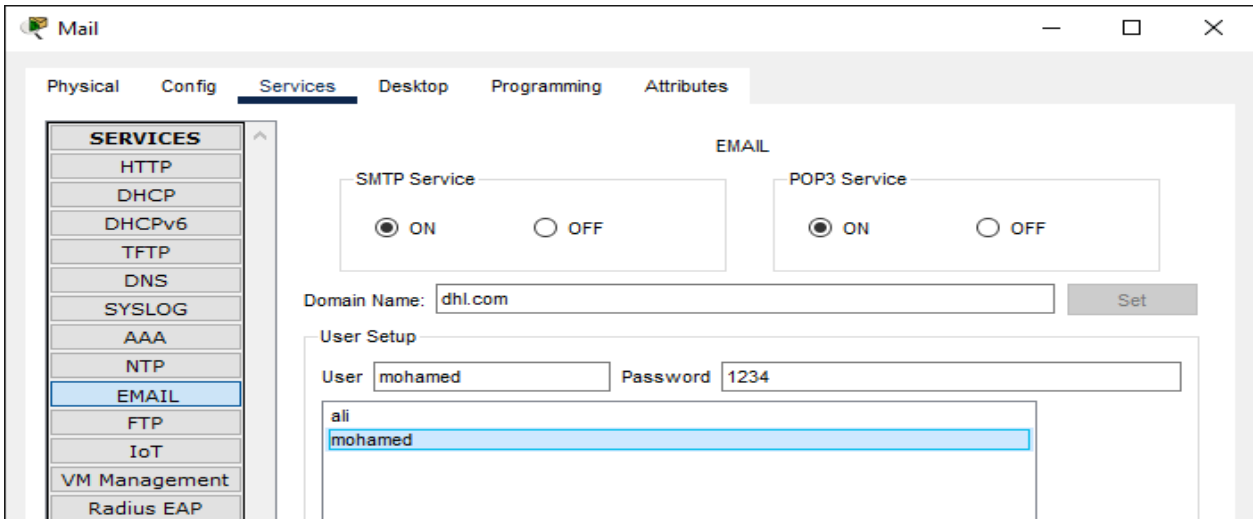
For example, we create a simple topology to explain how mail server is work.

First we put the ip in each device and switch and router as shown as in figure

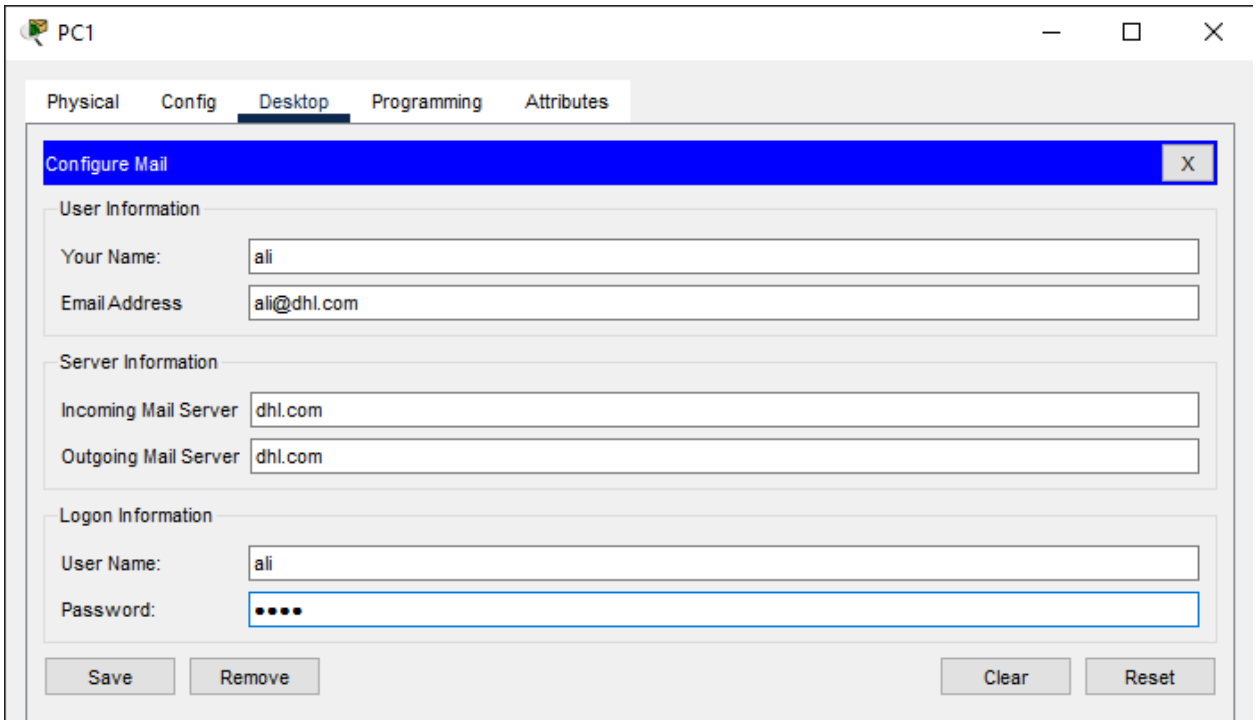


After that we create a website in DNS Server called www.dhl.com with have ip 192.168.1.4

and go to Mail Server and put domain name and the users



After that we go to the PC to put username and password



Finally, to send any message from user to user, we can go to any user like ali and open Email and click compose to send, therefore to check that the message was send, we go to another user like mohamed and open Email and click receive, so we see the message that was send.

CHAPTER (5)

Network Security

5.1 Introduction:-

We all know the importance of protection within the network, whether it is an enterprise network, medium or small network, and it is one of the basic components of any network, and dispensing with it leads to data breaches and exposing them to danger by hackers, due to the increase in cyber attacks in the recent period and the spread of viruses, worms and Trojans, which may lead to disasters

when we talk about protection within the network, we mean the firewall, as it is one of the most important protection tools through which we can protect and secure our network and preserve the data

5.2 Types of Security

- **Computer Security**
  - generic name for the collection of tools designed to protect data and to thwart hackers
- **Network Security**
  - measures to protect data during their transmission
- **Internet Security**
  - measures to protect data during their transmission over a collection of interconnected networks

5.3 Attacks Sources on the network

Active Attacks

Passive Attacks

- Active involves writing data to the network. It is common to disguise one's address and conceal the identity of the traffic sender

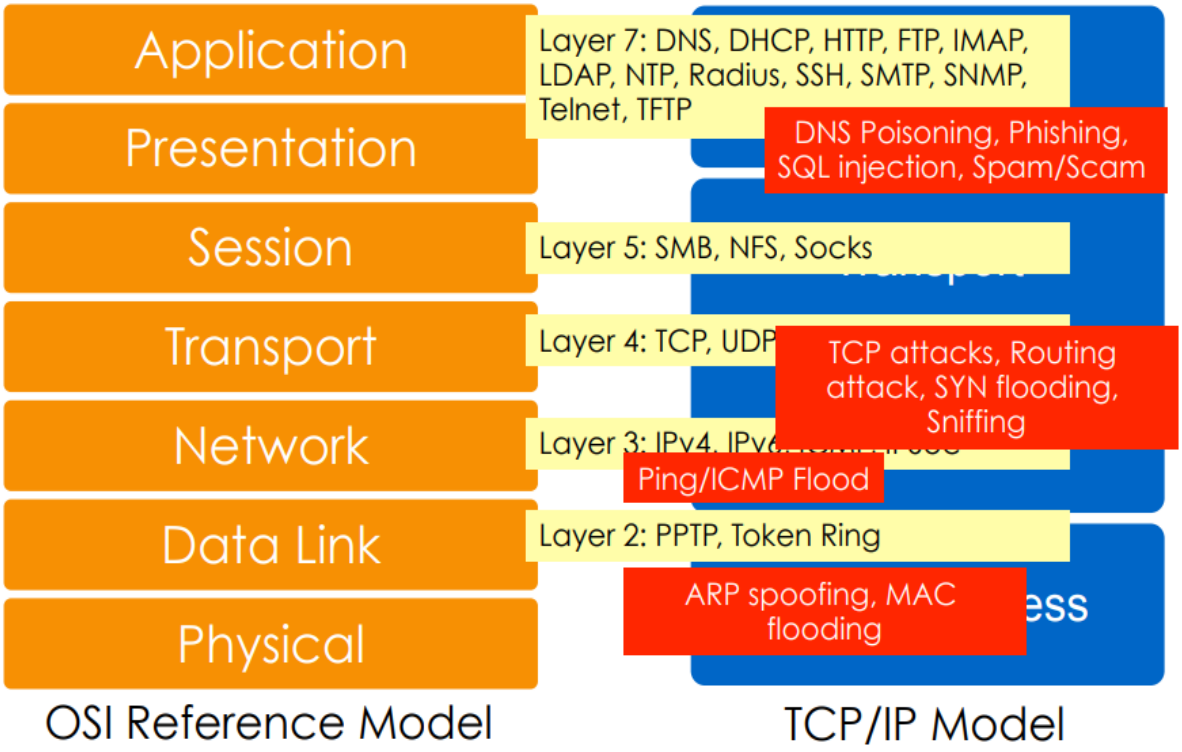
- Passive involves only reading data on the network. Its purpose is breach of confidentiality. This is possible if:
  - Attacker has gained control of a host in the communication path between two victim machines
  - Attacker has compromised the routing infrastructure to arrange the traffic pass through a compromised machine

Active Attacks	Passive Attacks
Denial of Service attacks	Reconnaissance
Spoofing	Eavesdropping
Man in the Middle	Port scanning
ARP poisoning	
Smurf attacks	
Buffer overflow	
SQL Injection	

➢ Man-in-the-Middle Attack

- Active eavesdropping
- Attacker makes independent connections with victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker
- Usually a result of lack of end-to-end authentication
- Masquerading - an entity claims to be another entity

○ Attacks on Different Layers



5.4 Standard defensive-oriented technologies

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

5.4.1 Firewall Definitions :-

A firewall is a hardware or software network security device that monitors all incoming and outgoing traffic based on a defined set of security rules, it accepts, rejects, or drops that specific traffic.

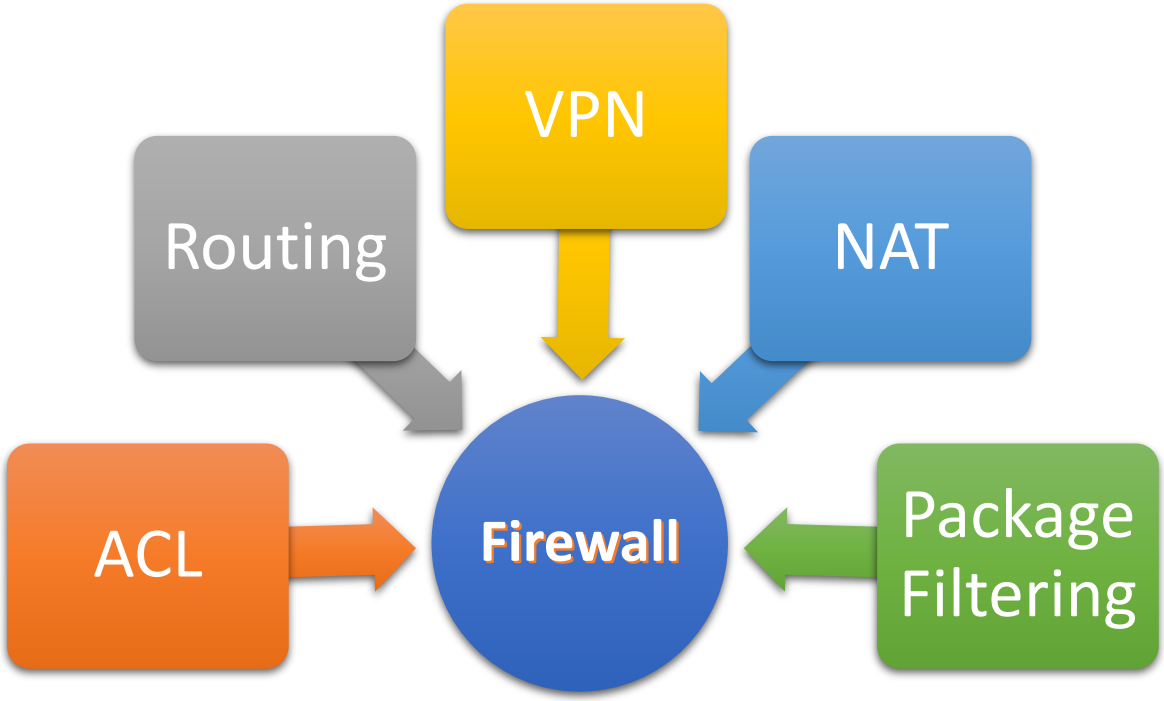
According that router does routing & VPN & NAT & Package filtering

To reduce this load on the router, the first independent Package filter was invented

It's called a firewall

- Accept: Allow traffic.
- Reject: Block traffic but respond with “reachable error”.
- Drop: Block unanswered traffic firewall establishes a barrier between secure internal networks and untrusted external networks, such as the Internet.
- Firewall has been a first line of defense in network security.
- They establish a barrier between secured and controlled internal networks That can be trusted and untrusted outside networks such as the internet.
- A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on defined set of security rules.
- A firewall can be Hardware or Software

5.4.2 Firewall Feature



Remote Access VPN

Remote access VPN provides remote and secure access to a company network to individual hosts or clients, such as telecommuters, mobile users, and extranet consumers. Each host typically has VPN client software loaded or uses a web-based client. Privacy and integrity of sensitive information is ensured through multi-factor authentication, endpoint compliance scanning, and encryption of all transmitted data.

Access Control List

Access control defines the people or groups and the devices that have access to network applications and systems thereby denying unsanctioned access, and maybe threats. Integrations with Identity and Access Management (IAM) products can

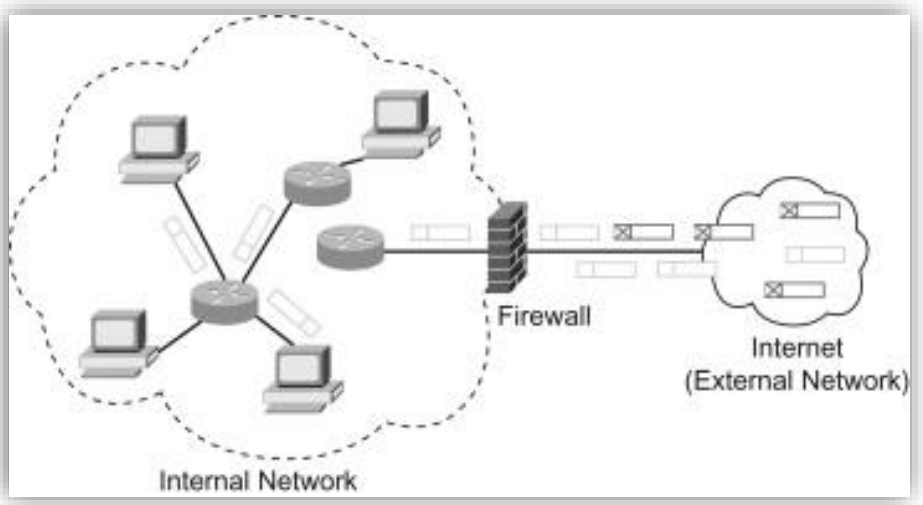
strongly identify the user and Role-based Access Control (RBAC) policies ensure the person and device are authorized access to the asset.

Not everyone needs access to your network. To keep out potential hackers, the access control center can make a note of each user and each device, and determine which ones are allowed in. They can also enforce security policies and parameters that you put in place. This is often referred to as network access control.

5.4.3 Firewall Position

In internal network (LAN)

- if my network received data from out, Firewall be after the router to control in data that come from out
- if my network rout data to out network, Firewall work as a gateway to control in data that out



5.5 Design Network Security

The first steps that we start 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:

1- **External public network**
2- **Internal Private network**
3- **DMZ**

External public network

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.

Internal Private network

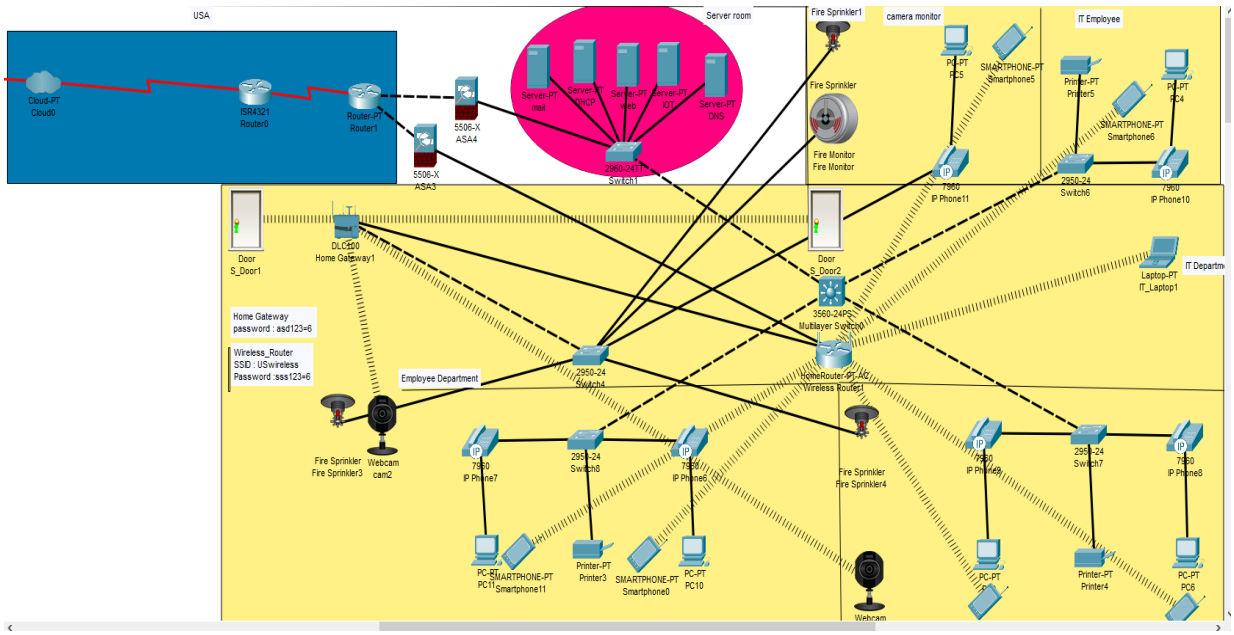
This part represents the devices that we trust and that we can control from the network that I am responsible for protecting. This part is where I put the server that contains the important data and programs of the organization that I want to protect from any external threat coming from the public network

It is very important to separate the internal network of my organization from the public network

DMZ

But most institutions are currently doing their own business through Internet services, so they have a website with services that we need to create access for customers inside the institution, or there is a mail server used by workers inside the institution. This type of services or servers exposed to the Internet, we put it inside a demilitarized zone

DMZ is the area that I allocate in the network for the server that needs access to the Internet, and this is an area other than the public network and the internal network



Out = 0

DMZ = 1-99

IN = 100

Note :-

Dividing the network into separate areas is an important step in security, but it is not sufficient

Therefore, we need to increase the layers of defense, i.e. use more than one layer to protect the security of the network

Every time I used different means of protection and placed them in different places on the network, this made it difficult for any hacker to attack, and the penetration process became slower and easier to detect, and it is possible that a way of them completely prevents the hacker from entering the network by stopping him before he causes any damage to the network

5.6 Port Security

PCs that allow it to connect to the machine can be used, and the machine allows it to connect to the unit of communication with you, and the Mac address through the network connection, so that the network can be connected to the network.

If we had a “HUB”, for example, what would happen if someone tried to access the network?

Port Security has three positions that it can take if the MAC Address of an unauthorized computer is networked to enter the network, and the cases are as follows:

- **The first case is shutdown:**

  In this case, the switch will close the port directly, and this situation is the default for Port Security.

- **The second case is protect:**

  In this case, the switch will drop all traffic coming from the unauthorized MAC Address, while keeping the port open for authorized devices.

➢ The third case is restrict :

The same as the previous case, but here the switch counts all the buckets that it has dropped.

The way to set it up is very easy, and it is done by only two things:

Cisco's IOSHide

```
Switch# conf t
Switch(config)# interface fastethernet 0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
```

As we can see, you first select the port and then choose mode access in order to tell the switch that this port is connected to the end device or a computer.

When we disable the Port Security, the natural state that the switch takes is to close the switch, in addition to allowing one Mac Address as a maximum, and in other words, the first Mac Address that will connect to the port will be the only one capable of connecting to the switch, and it helps us in deterring the "Mac" attack Flooding

In the event that we want to allow more than one MAC Address to connect to the switch, we write the following command:

```
Switch(config-if)# switchport port-security maximum 3
```

Here I have allowed 3 devices to access the switch through this portAnd in case you want to specify a specific MAC Address that is the only one that can enter the switch, I type the following command:

```
Switch(config-if)# switchport port-security mac-address 00-11-22-33-44-55-66
```

And if you find that this topic is very cumbersome and long, you can put the word Sticky in place of each MAC Address, which tells the switch to register the MAC Address currently connected to the port as Static Mac Address, and the command formula is:

```
Switch#show port-security address
```

```
Switch(config-if)# switchport port-security mac-address mac-address sticky
```

Finally, to change the reaction that the switch will take in the event of any violation, we write the following command:

```
Switch(config-if)# switchport port-security mac-address violation ?
```

5.7 Types of threats on the network

Robust Network Security Will Protect Against :

- **Virus**: A virus is a malicious, downloadable file that can lay dormant that replicates itself by changing other computer programs with its own code. Once it spreads those files are infected and can spread from one computer to another, and/or corrupt or destroy network data.
- **Worms**: Can slow down computer networks by eating up bandwidth as well as the slow the efficiency of your computer to process data. A worm is a standalone malware that can propagate and work independently of other files, where a virus needs a host program to spread.
- **Trojan**: A trojan is a backdoor program that creates an entryway for malicious users to access the computer system by using what looks like a

real program, but quickly turns out to be harmful. A trojan virus can delete files, activate other malware hidden on your computer network, such as a virus and steal valuable data.

- **Spyware**: Much like its name, spyware is a computer virus that gathers information about a person or organization without their express knowledge and may send the information gathered to a third party without the consumer's consent.
- **Adware**: Can redirect your search requests to advertising websites and collect marketing data about you in the process so that customized advertisements will be displayed based on your search and buying history.
- **Ransomware**: This is a type of trojan cyberware that is designed to gain money from the person or organization's computer on which it is installed by encrypting data so that it is unusable, blocking access to the user's system.

CHAPTER (6)

Smart Part (IOT)

6.1 Abstract

The technology has been growing from day to day in human life. The necessity for the development of technology is to lead human life comfortably

This paper gives the basic idea use cisco packet tracer to implement smart company. One is needed to create a smart company when electronic devices are switched on and off.

Smart company development is achieved by simulation via testing system, network setup and wireless home gateway computer network equipment required by a smart company network cisco packet tracer using Internet Thing (IoT)/IoE command.

The software chosen for the simulations is Cisco Packet Tracer, the tool's main strength is to offer a variety of network components that represent a real network, and then interconnect and configure devices to create a network. Cisco implemented (IoT) functionalities in the latest version of the platform, and now it is possible to add all the smart devices, sensors, actuators and also devices, which simulate microcontrollers to the network.

All IoT devices can be run on generic programs or modified by Java, Python or Blocky programming them. This makes Cisco Packet Tracer a perfect method to construct functional simulations for IoT

It aimed to improve safety, comfort and efficiency, which using various sensors (Temperature, Fire, Camera, smart door) to monitor the company environment. And there are usually monitoring tools, and the devices that are controllable and automatic this can be accessed via an internet-connected computer or smart mobile device

Instead of providing security that is safe, smart home can provide different features to provide automatic security using various alarm systems, as LCD

display and siren sound and by sending email to IT monitor if sensor detects security issues.

Through the simulation framework based **on cisco packet tracer** (version 7.2), smart company system can be implemented.

6.2 Methodology

Including various smart objects which are used for implementing company automation such as (chic windows, air cool, chic lights, chic doors, fire sprinklers, web cams and Fire sensors).

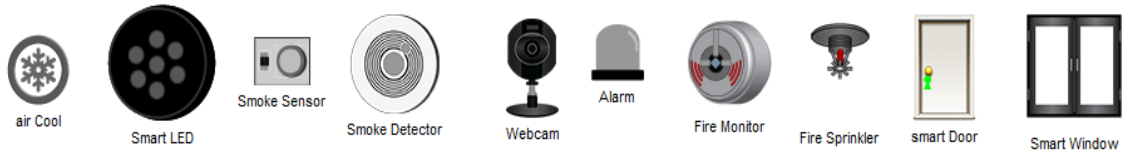


Fig (): shows IOT devices that we used in our company

Home Gateway are used for controlling the objects and sensors, which are providing programming environment for controlling objects that are connected and provide control mechanisms through the registration of Home Gateway smart devices.

HOME GATEWAY: The IoT can register directly with the IOT service on a Home gateway or network database. The Home Gateway offers 4 Ethernet ports and a wireless contact point on channel 6 equipped with the SSID "Home Gateway."

It is possible to configure WEP / WPA-PSK / WPA2 companies to wireless links are safe for connections. A home gateway and a web interface it is easy to manage the IOT system. The internal IP address of the Home Gateway (LAN) is 192.168.25.10, but it can be too reached via its IP address in front of the Internet. The smart objects are associated to the home gateway by Wireless medium and Ethernet cable for local and remote control of smart devices. Home

portal also acts as a DHCP server assigns IP addresses to any, connected smart device.

6.3 Smart Company Architecture

1- Branch 1 (USA)

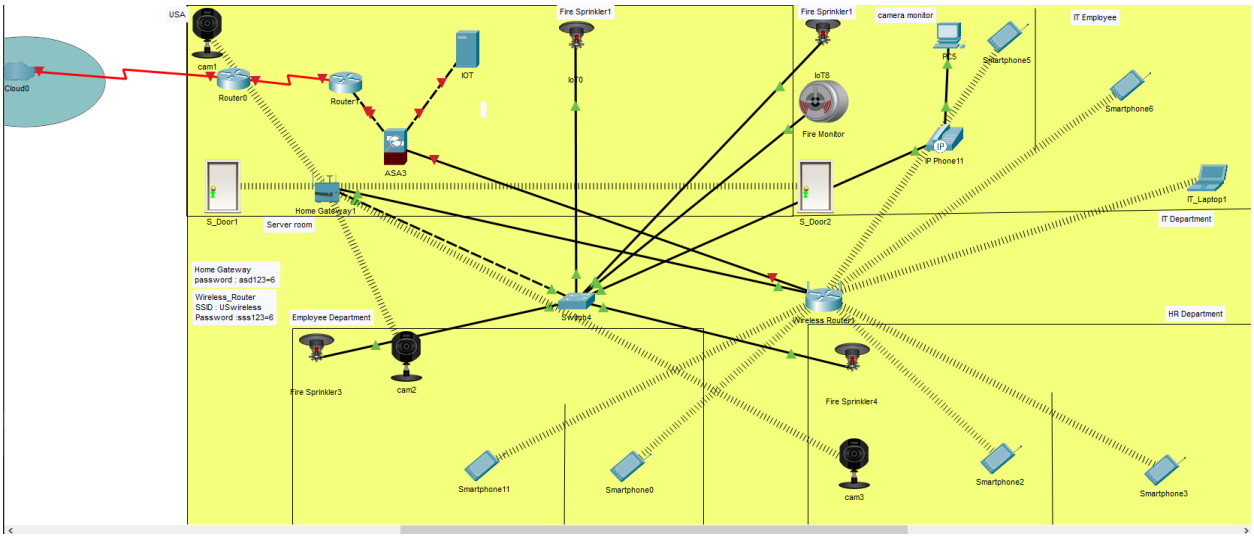


Fig (): shows the total schematic architecture of the design model for branch 2

2- Branch 2 (EG)

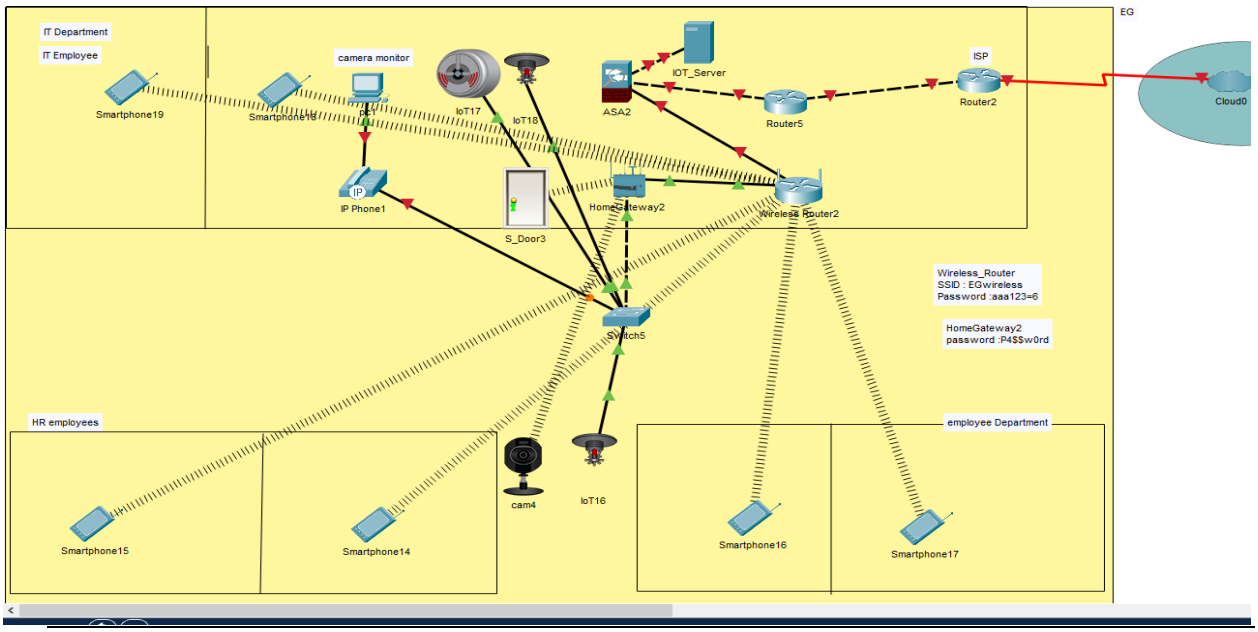
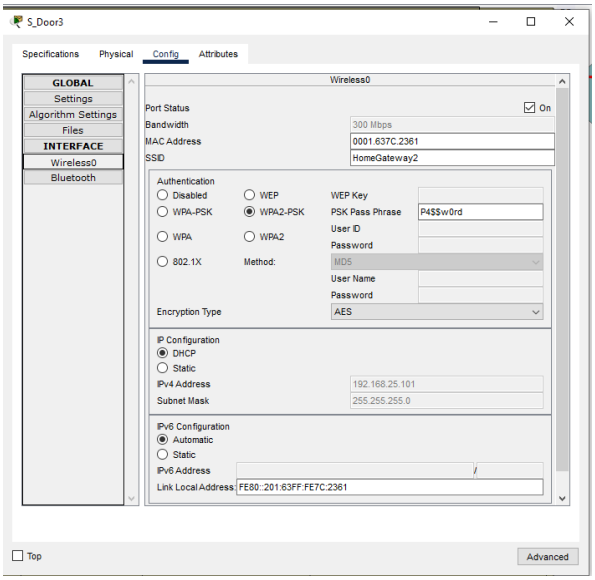
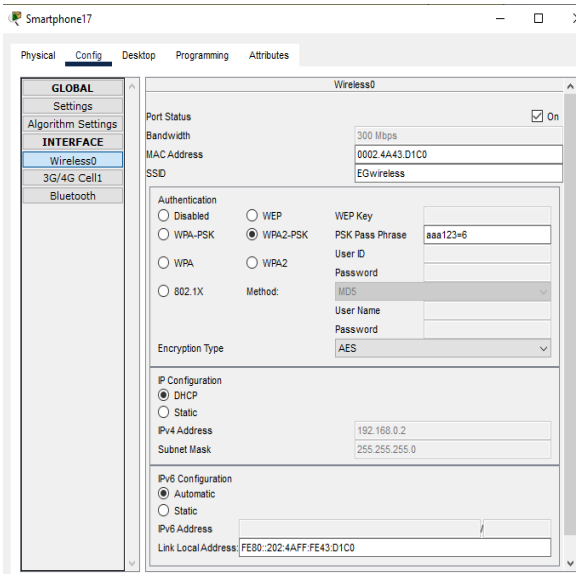


Fig (): shows the total schematic architecture of the design model for branch 2

And That fig represents the screenshots of the Cisco packet tracer of implementation of Smart Devices (Smart Phone) and the various stages involved in it.

But Smart Phone isn't connected with Home Gateway, It connected to the Router home with Ip address 192.168.1.0





We give to Wireless Router1 & Home Gateway in Branch 1

Wireless_Router1

SSID : USwireless
Password :sss123=6

Home Gateway1
Password : asd123=6

And give to Wireless Router2 & Home Gateway in Branch 2

Wireless_Router2
SSID : EGwireless
Password :aaa123=6

HomeGateway2
password :P4$$w0rd

6.4 USED DEVICE FOR DESIGN

Table 1. Device used for deployment

	Devices	Functions
1	Router	Used to link Wireless Router to the network of cloud and IOT server
2	Wireless Router	Used to link Personal devices for employees to the internet and Link Gateway with IOT server
3	Home gateway	Used to register smart objects and provide smart objects with IP addresses
4	IOT Server	To monitor intelligent things that are recorded on it and to have specific database features
5	PC	In IT department Link and monitor company destination to access intelligent objects
6	Webcam	Control and monitor
7	Smart door	Link to getaway and provide an event based on functions and put in sensitive places as servers room and IT Room Open / Close / Unlock / Lock
8	Fire Sprinkler	A Sprinkler that puts out fire.
9	Fire Monitor	Detect IR in the range of fire.
10	Alarm	Alarm is triggered with a value of HIGH, and its light turns red
11		

CHAPTER (7)

CLOUD

Abstract

During the past few years, cloud computing has become a key IT buzzword. Although the definition of cloud computing is still “cloudy”, the trade press and bloggers label many vendors as cloud computing vendors, and report on their services and issues.

Cloud computing is in its infancy in terms of market adoption. However, it is a key IT megatrend that will take root. This article reviews its definition and status, adoption issues, and provides a glimpse of its future and discusses technical issues that are expected to be addressed.

7.1. INTRODUCTION

Cloud computing is a topic that received a great deal of attention by individuals and organizations from different disciplines in the last decade [1-20].

This new environment implies great flexibility and availability of computing resources at different levels of abstraction at a lower cost.

Cloud Service Providers (CSPs) (e.g., Google, Microsoft, Amazon) are vendors who lease to their customers cloud computing resources and services that are dynamically utilized based on customer’s demand according to a certain business model .

General services in different application areas such as business, education and governance are provided to the customers online and are accessed through a web browser, while data and software programs are stored on the cloud servers located in the data centres [8].

These services are generally classified into three classes known as cloud service models and are shown in figure 1. Cloud service models [1,2,12,13,18,19,22,24,26-

29,34] are a Service-Oriented Architecture (SOA) that describe cloud services at different levels of abstraction.

These models are: Software as a Service (SaaS): In this model, CSPs are responsible for running and maintaining application software, operating system and computing resources.

The customer views the SaaS model as a web-based application interface where services and complete software applications are delivered over the Internet and are accessed via a web browser.

Customers can access hosted applications such as Gmail and Google Docs through different client devices such as laptops, iPads and cell phones. Unlike traditional software, SaaS has the advantage that the customer does not need to buy licenses, install, upgrade, maintain or run software on his own computer [26].

It has also other advantages such as multitenant efficiency, configurability and scalability [27].

Examples of SaaS providers are Zoho, Google Apps and Salesforce.com.

Platform as a Service (PaaS): In PaaS, a CSP provides, runs and maintains both system software (i.e., the operating system) and computing resources.

The customer manages and runs the application software under the operating system and on the virtual resources provided by the CSP. The customer has little or no control over the operating system and hardware resources [26].

Unlike SaaS that provides the customer with complete (ready to use) applications, PaaS gives him/her the opportunity to design, model, develop and test applications directly on the cloud; therefore, he/she can control the software lifecycle [27].

PaaS supports collaborative work between members of a project team.

For instance, a number of users located indifferent countries can collaborate in developing a website using a PaaS cloud service.

Examples of PaaS providers are windows Azure, Google Apps Engine and Aptana cloud.

Infrastructure as a Service (IaaS): In this model, the CSP provides a set of virtualized computing resources (e.g., network bandwidth, storage capacity, memory, processing power) in the cloud.

It is the responsibility of the customer to run and maintain the operating system and the software applications on these virtual recourses.

IaaS uses virtualization technology [15-1723] to convert physical resources into logical resources that can be dynamically provisioned and released by customers as needed.

Examples of IaaS providers are Drop Box, Amazon EC2 and Akamai. Table 1 shows the assignment of running and maintaining cloud resources to CSPs and cloud customers in different service models.

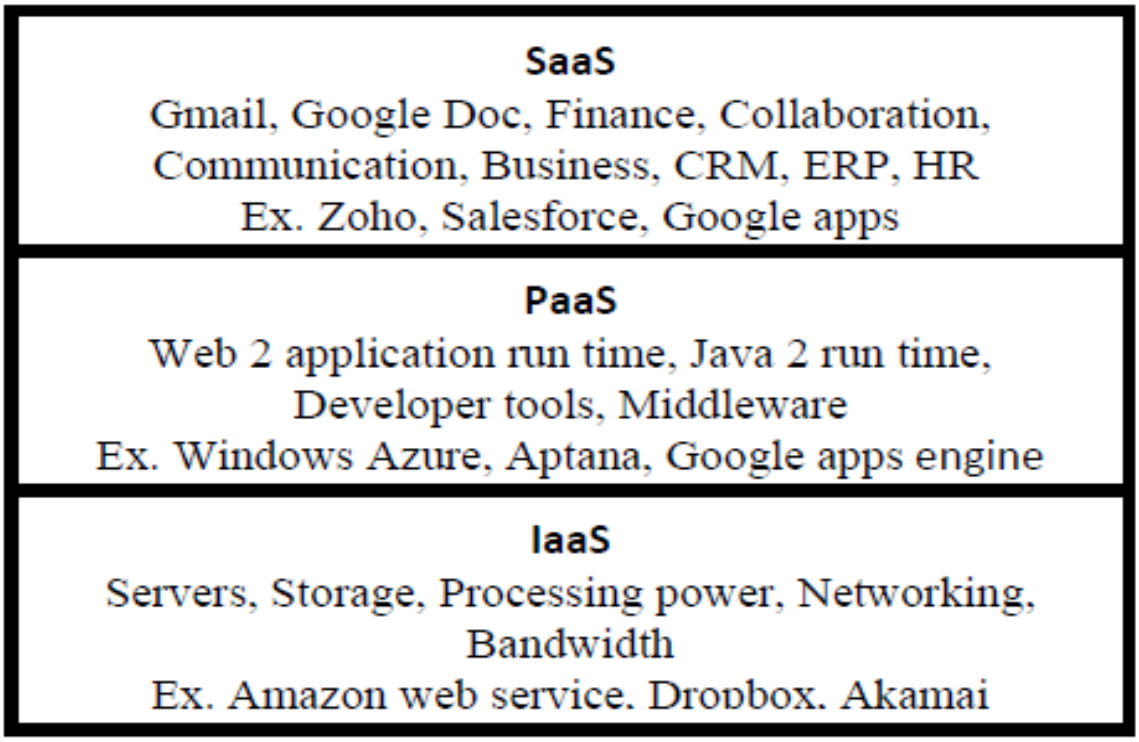


Fig 1: services provided in cloud computing environment

Table 1: resource assignment in cloud service models

	Application Software	Operating System	Virtual recourses/ HW
SaaS	CSP	CSP	CSP
PaaS	customer	CSP	CSP
IaaS	customer	customer	CSP

The cloud services described above can be provided to cloud customers by CSPs through different applications. In this paper, we explore cloud computing services and applications, we give examples for cloud services provided by the most common CSPs such as Google, Microsoft, Amazon, HP, and Sales force and we present innovative applications for cloud computing in egovernment, e-learning and Enterprise Resource Planning
(ERP).
The objective of our study is to help individuals and organizations understand how cloud computing can provide them with customized, reliable and cost-effective services in a wide variety of applications.

7.2. Analysis of Cloud Computing System

Cloud computing systems are classified as public cloud, private cloud, community cloud and hybrid cloud [1,12,19,22,24,28,30,34].
These classes are known as deployment models and they describe the scope of services offered on the cloud to the customers.

• Public Cloud :-

In public clouds the infrastructure and other cloud services are made available to the general public over the Internet.
The cloud is owned and managed by a CSP who offers services to consumers on a pay-per-use basis.
Public cloud users are by default treated as untrust worthy ;therefore, security and privacy are big concerns about this type of cloud [12].
Many popular cloud services are public including Amazon EC2, Google App Engine and Salesforce.com.

• Private Cloud :-

In private clouds the computing resources are operated exclusively by one organization. It may be managed by the organization itself or a CSP.

Private clouds are considered to be more secure than public clouds since their users are trusted individuals inside the organization.

The other two deployment models, community clouds and hybrid clouds, fall between public and private clouds [12].

• Community clouds :-

Community clouds are similar to private clouds but the cloud infrastructure and computing resources are shared by several organizations that have the same mission, policy and security requirements [24].

An example of a community cloud is the educational cloud used by universities and institutes around the world to provide education and research services.

• Hybrid Clouds:-

In hybrid clouds, the cloud infrastructure consists of a combination of two or more public, private or community cloud components.

The cloud components are bound together by standardized technology and managed as a single unit, yet each cloud remains a unique
entity [24, 28].

Hybrid clouds allow organizations to optimize their resources, so the critical core activities can be run under the control of the private component of the hybrid cloud while other auxiliary tasks may be outsourced to the public component.

Figure 2 below shows different cloud deployment models and table 2 compares these models with each other [30].

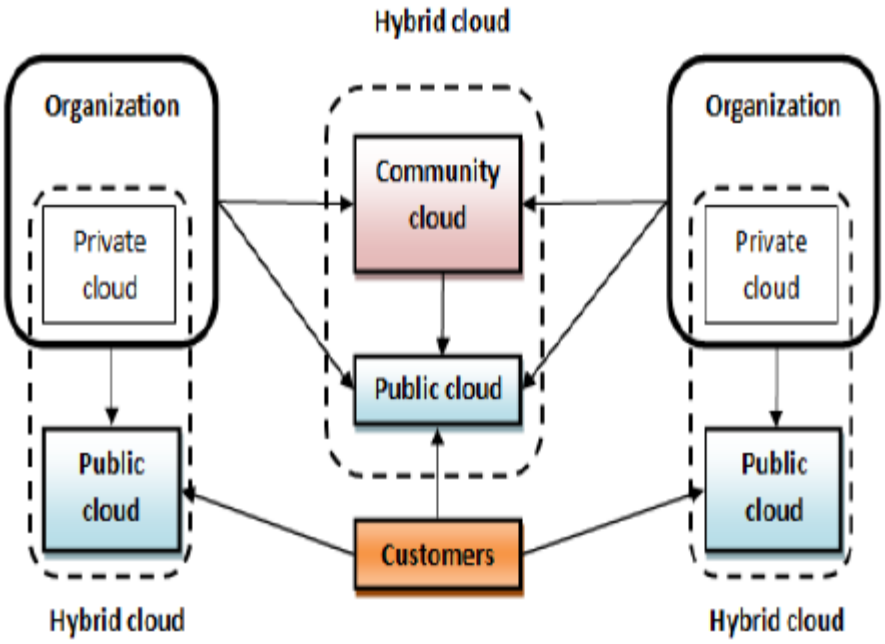


Fig 2: cloud computing deployment models

Table 2: A Comparison of Cloud Deployment Models

Deployment model	scope of services	owned by	managed by	security level	location
public	general public and large industry groups	CSP	CSP	low	off premise
private	single organization	single organization	single organization or CSP	high	off or on premise
community	organizations that share the same mission, policy and security requirements	several organizations	several organizations or CSP	high	off or on premise
hybrid	organizations and public	organizations and CSP	organizations and CSP	medium	off and on premise

7.3. Cloud Computing Services

Examples of cloud services provided by the most common CSPs are given in this section [32]:

a. Google Cloud Computing Services

Google integrates many applications and provides many services to cloud customers [36].

This integration makes Google one of the best CSPs since it allows cloud's customers to have their tasks accomplished easily.

It also saves money and time since developing and maintaining software to provide all of these services and applications is a time consuming and an expensive process.

Among the services provided by Google clouds are [36]:

• **Gmail:** is an email service that provides users with 25GB storage, less spam and mobile access. It has an integrated chat applet that stores conversation in the form of email.

• **Google Docs:** is a service that allows users to create spread sheets, word documents and power point presentations and store them on the cloud servers. The documents are available online so that they can be accessed from anywhere and at any time.

This helps team members located in different countries to cooperate in completing their work. Google docs are secure since the files are encrypted using advanced encryption technology and are only accessed by authorized users.

• **Google analytics:** is used to monitor the traffic come onto a website.

• **Google Ad words and Ad Sense:** which are advertising tools?

• **Picasa:** which is a tool used to exhibit product and uploading their images in the cloud.

b. Microsoft Cloud Computing Services

Microsoft provides a cloud platform called Windows Azure platform which consists of a set of cloud services offered to users and application developers.

All services run in Microsoft data centers located around the world.

These services include [37]:

• **Windows Azure:** a windows environment for storing data and running applications in the cloud.

• **SQL Azure:** is a relational database services in the cloud that use a special version of Microsoft SQL server.

• **Windows Azure App Fabric:** provides an infrastructure for applications that run in the cloud or inside an organization.

• **Windows Azure Marketplace:** is an online market to buy and sell application software and data.

c. Amazon Web Services (AWS)

AWS provides a cloud computing platform for all business sizes.

With AWS companies can provision a flexible and cost-effective IT infrastructure and services that can be scaled up and down based on their needs.

AWS helps companies select the platform that is suitable for the problem they have and pay only for what they use.

In addition, AWS applies advanced physical security and data privacy techniques to protect users' data.

AWS has security certifications and audits such as ISO 27001, FISMA moderate, HIPAA and SAS 70 Type II.

AWS is a comprehensive cloud service platform which provides many web services such as [33, 35]:

• **Amazon Elastic Compute Cloud (Amazon EC2):** is a web service that provides configurable computing resources in the cloud.

• **Amazon Simple Storage Services (Amazon S3):** Is a scalable, secure and reliable storage for the Internet that can be used to ubiquitously store and retrieve data of any size on the web.

• **Amazon Virtual Private Cloud (Amazon VPC):** connects the company's existing IT infrastructure to AWS cloud via a Virtual Private Network (VPN).

• **Amazon CloudFront:** is a web service for content delivery that transfers customer's data with high speed and minimum delay using a global network of edge locations.

• **Amazon Route 53:** is a scalable and highly available DNS service.

• **Amazon Relational Database Services (Amazon RDS):** is a web service that helps manage a relational database in the cloud.

7.4. Advantages

Cloud computing offers the following major advantages to the users.

1. The 3rd party provider owns and manages all the computing resources (servers, software, storage, and networking) and electricity needed for the services.

   The users only need to "plug into" the cloud. The users do not need to make a large upfront investment on computing resources; the space needed to house them; electricity needed to run the computing resources; and the cost of maintaining staff for administering the system, network, and database.

2. The users can increase or decrease the level of use of the computing resources and services flexibly and easily.

3. The users pay most likely much less for the services, because they pay only for the computing resources and services they use, and the subscription-based or payper- use charges are likely much lower than the cost of maintaining on premises computing resources. If the users are to maintain on premises computing resources, they also need to make the worst-case plan to account for the occasional or seasonal peak needs.

7.5. Frame Relay

Frame Relay is a packet-switching technology offered as a telecommunications service by telcos and long-distance carriers, used primarily for WAN links.

7.5.1. What is Frame Relay?

Frame Relay is a packet-switching technology offered as a telecommunications service by telcos and long-distance carriers, used primarily for WAN links. Frame relay can be used to encapsulate local area network (LAN) traffic such as Ethernet frames for transmission over digital data transmission lines for wide area networks (WANs) and can connect multiple LANs to form a multipoint WAN. Frame relay technology was originally an offshoot of Integrated Services Digital Network (ISDN) digital communication technology.

7.5.2. How It Works – Frame Relay

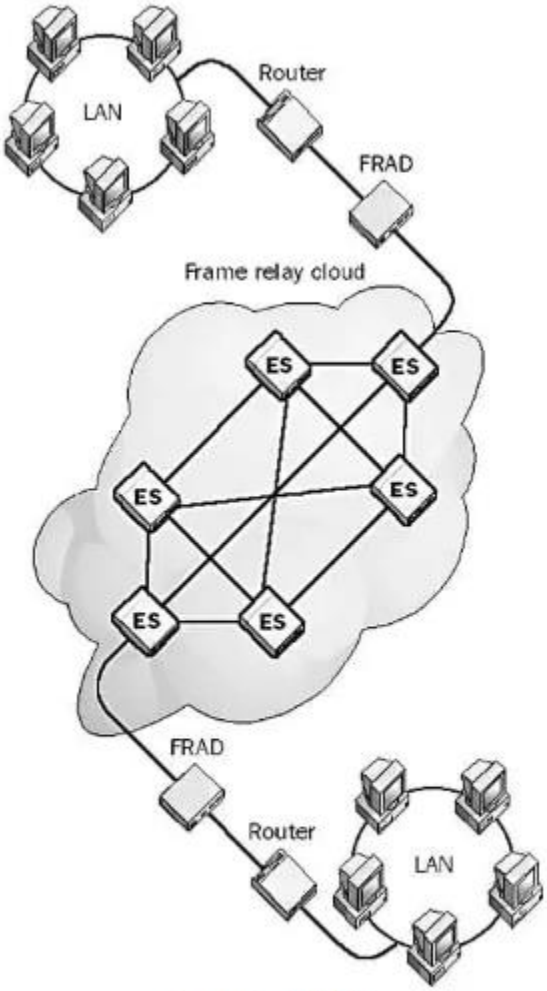
Frame relay technology is a packet-switching service that is similar in operation to, and considered the replacement for, the older X.25 packet-switching technology – but it provides higher performance and has a greater efficiency because it is a more streamlined protocol. For example, while X.25 includes error-correction functions, frame relay leaves error correction up to the station endpoints in order to speed up WAN communications. When errors do occur, frame relay drops the offending frame and retransmits the data. Frame relay also does not support the hop-by-hop flow control functions that X.25 supports, which further streamlines frame relay operation.

Frame relay implementations usually follow one of two networking topologies:

to connect a network to a telco Frame Relay Bearer Service (FRBS), use a special bridge, router, or CSU/DSU (Channel Service Unit/Data Service Unit) device called a frame relay access device (FRAD). The FRAD connects your customer premises to an Edge Switch (ES) on your provider's frame relay cloud (the

collection of all frame relay circuits belonging to your provider). See the illustration for an example.

Frame relay technology is more popular in North America than slower packet-switching technologies such as X.25, while in Europe, X.25 has traditionally been a more popular solution. Frame relay services were first offered in 1992 by AT&T, Sprint, and other carriers, which have installed frame relay points of presence (POPs) for connections to the central office (CO) of local telcos in major metropolitan locations around the United States.



Frame Relay WAN link

7.5.3 Frame Relay Configuration

be used. Cisco IOS Software uses the following defaults for Frame Relay:

- LMI Cisco IOS automatically senses the LMI type by default and this feature is referred to as LMI autosense. If you manually configure the LMI using the frame-relay lmi-type command, LMI autosense is silently disabled.
- IARP Cisco IOS automatically discovers the next-hop IP address associated with a DLCI or VC using Inverse Address Resolution Protocol (IARP). You can also create a mapping between a DLCI and next-hop IP address manually using frame-relay map ip command.
- Encapsulation Cisco IOS uses Cisco encapsulation for Frame Relay and if you are using only Cisco routers, this default setting works fine without any additional configuration.

You are familiar with the concept of physical and logical sub-interfaces. For example, you may configure several sub-interfaces on a single Fast Ethernet physical interface on a Cisco router. Frame Relay is a Layer 2 WAN protocol that cand be configured on physical serial links. In addition to physical interfaces, you can also configure two types of logical interfaces for Frame Relay – point-to-point and multipoint. We will introduce you to some of the specifics of Frame Relay configuration for these different interface types.

In certain cases, you may have a working Frame Relay connection by just using a single command encpsulation frame-relay, and leaving everything else to default values. However, you should be familiar with the many configuration options and

when they are used. Frame Relay is the source of many tricky questions on CCNA, CCNP, and beyond.

Here is your step-by-step guide to configuring Frame Relay:

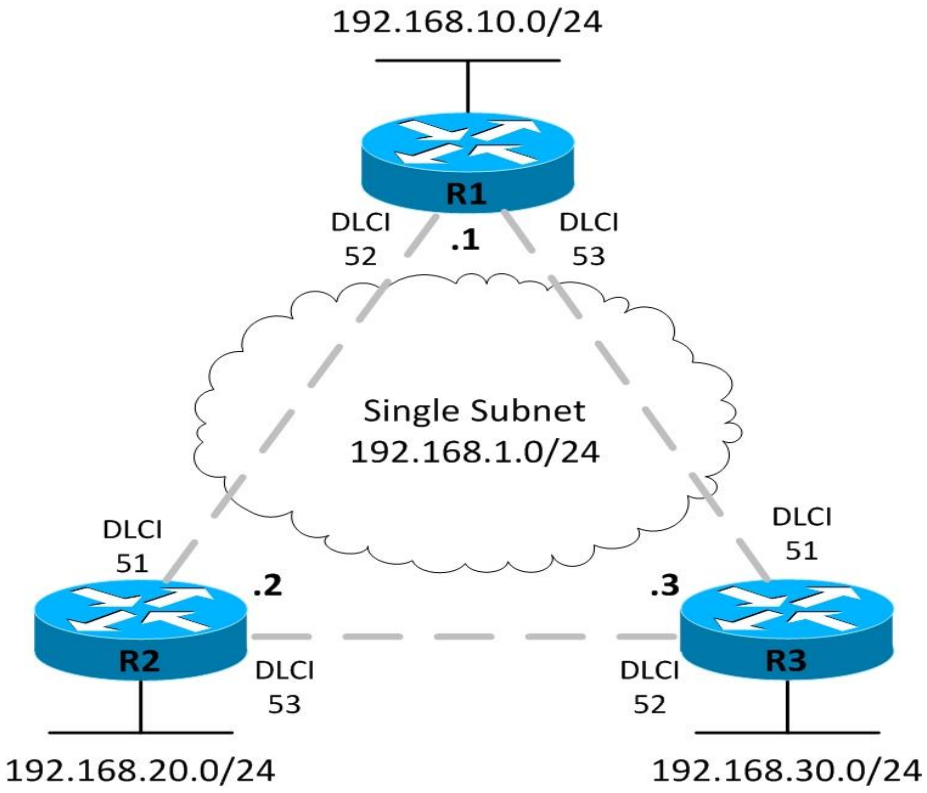
- The first step should always be to configure the physical interface to use Frame Relay encapsulation using the command encapsulation frame-relay in interface configuration mode.
- Configure an IP address on the interfaces or sub-interface using the good old ip address command.
- Optionally, configure the LMI type of each physical interace using the frame-relay lmi-type command.
- Optionally, change the default Frame Relay encapsulation using the command encapsulation frame-relay. If you use the command on the interface (or sub-interface), it will change the encapsulation for all VCs on the interface (or sub-interface. If you want to change the encapsulation only for a specific VC, you should use the ietf keyword with the command frame-relay interface-dlci (point-to-point sub-interfaces) or frame-relay map.
- The default is to use the Inverse ARP (IARP) to map the DLCI to the IP address of next-hop router. However, you can also configure static mapping using the frame-relay map ip *ip-address dlci* broadcast command.
- There are two ways to associate one DLCI to point-to-point or multiple DLCIs to multipoint interfaces. The first involves using the frame-relay interface-dlci *dlci* sub-interface command. The second involves using the frame-relay map ip *ip-address dlci* broadcast sub-interface command.

We are going to present three different Frame Relay configuration examples to see all those configuration steps in action. The examples correspond to the three Frame Relay scenarios we presented earlier in the chapter. We will also introduce you to several show commands that are useful to verify your configuration and troubleshoot if something is not working as expected.

Configuration – Single Subnet for all Routers

The first option involves a single IP subnet for all routers/DTEs, with IP addresses configured on physical serial interfaces, as shown in Figure 12-17.

Figure 12-17 Configuration – Single Subnet for all Routers



We will use a single class C private subnet 192.168.1.0/24 in this example. Table 12-5 should serve as a reference for all configuration in this section.

Table 12-5 Configuration Table

Router	**Interface / Type**	**DLCI**	**IP Address**
R1	Serial 0/0 / physical	Learned via InARP	192.168.1.1/24
R2	Serial 0/0 / physical	Learned via InARP	192.168.1.2/24
R3	Serial 0/0 / physical	Learned via InARP	192.168.1.3/24

We are going to configure IP addresses on physical serial interfaces of all three routers. Also, we will not configure or map any DLCIs manually. We will rather rely on Inverse ARP, enabled by default on serial interfaces with Frame Relay encapsulation, for learning DLCIs. The router connected to the Frame Relay network learns DLCI information from the LMI status messages sent by the Frame Relay switch to the router.

The ultimate goal of a Frame Relay network is to enable hosts on a LAN communicate with hosts on remote LANs. We will use EIGRP to propagate routing information to achieve that goal. The configuration is pretty simple here and we are just enabling Frame Relay encapsulation using the encapsulation frame-relay command.

Packet Tracer tutorial - Frame Relay configuration

Introduction

Frame Relay is a protocol standard for WAN internetworking which provides a fast and efficient method of transmitting packets through the network. Frame Relay offers an attractive alternative to both dedicated lines and X.25 networks for WAN links. The success of the Frame Relay protocol is based on the following two factors:

- Virtual circuits consume bandwidth only when they transport data. Consequently, many virtual circuits can exist across a given transmission line, which is an improvement compared to dedicated leased lines. In addition, each device can use more than the allowed bandwidth as necessary, and thus operate at higher speeds.
- The increased error-handling sophistication at end stations and the improved reliability of communication lines allows the Frame Relay protocol to discard bad frames and thus eliminate time-consuming error-handling processing.

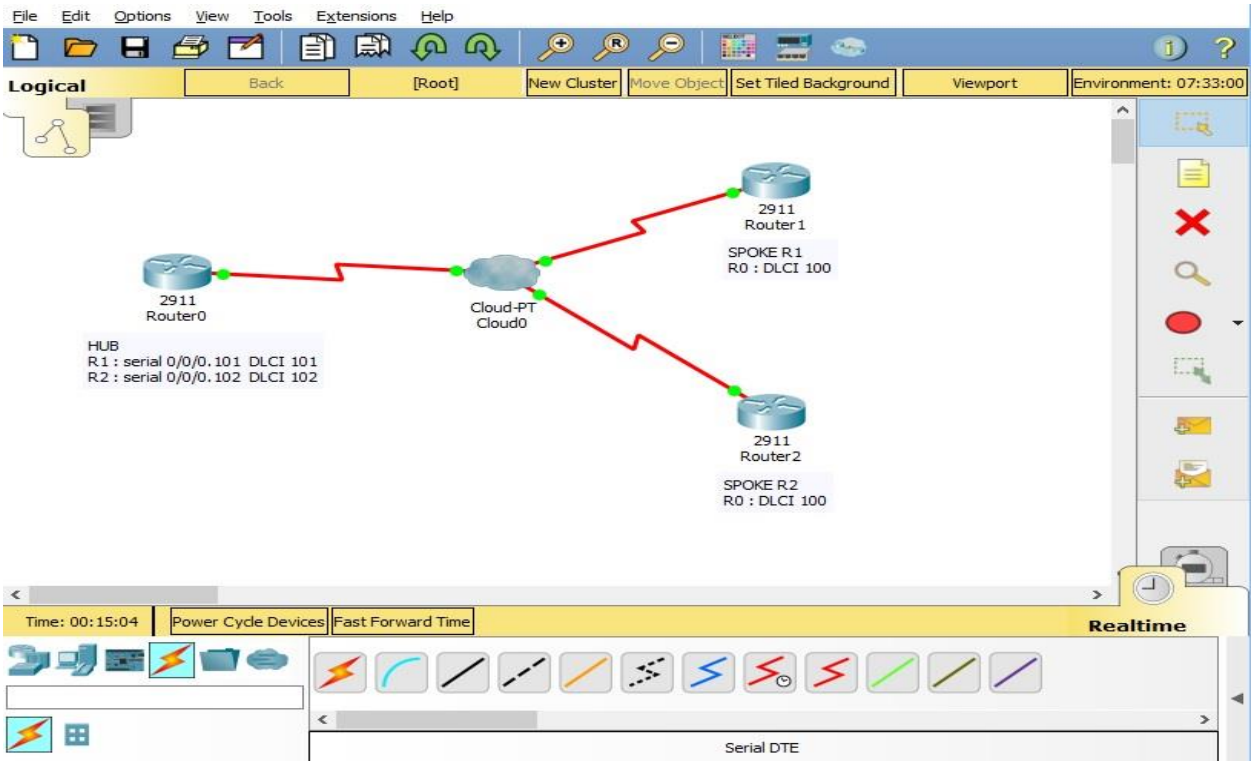
Cisco Packet Tracer includes a "Cloud-PT" device for WAN emulation. This device can be configured as a Frame Relay switch. Router are connected to the Frame Relay switch using serial connections. Virtual circuits, LMI types, and DLCI are configured using the Serial and Frame Relay tabs of the "Cloud-PT" device.

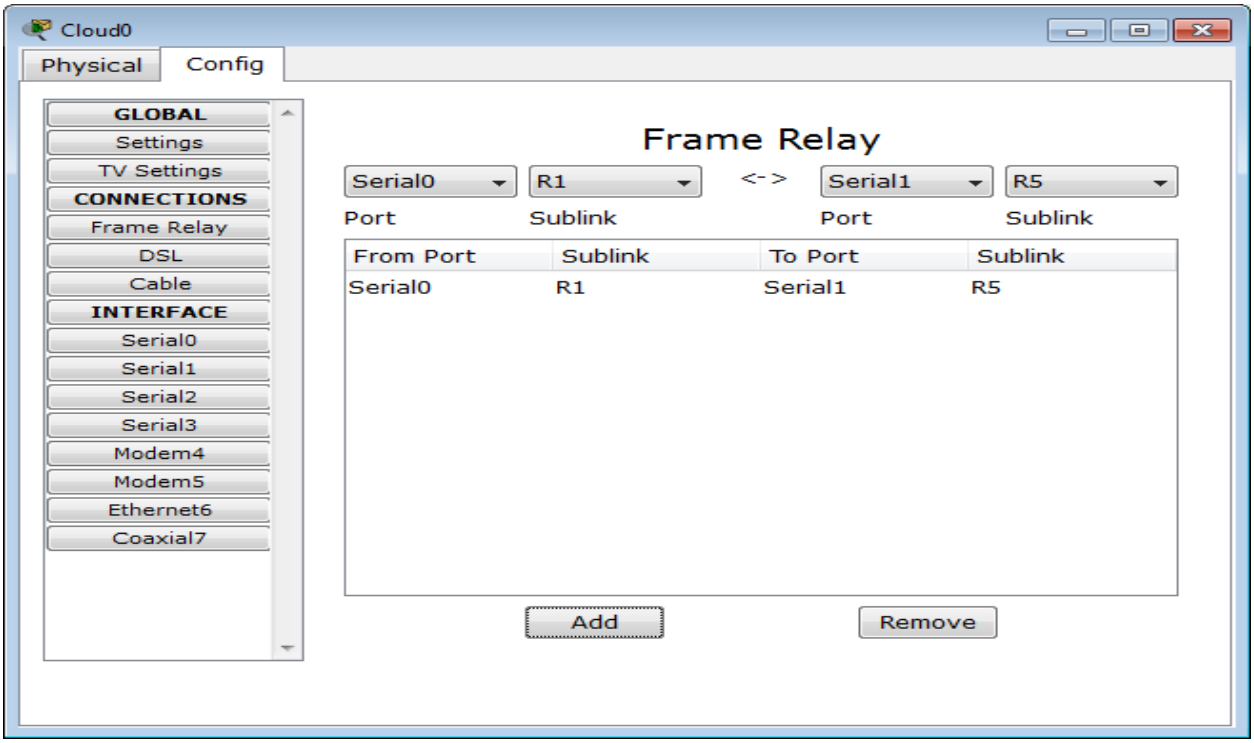
Network topology used in this tutorial

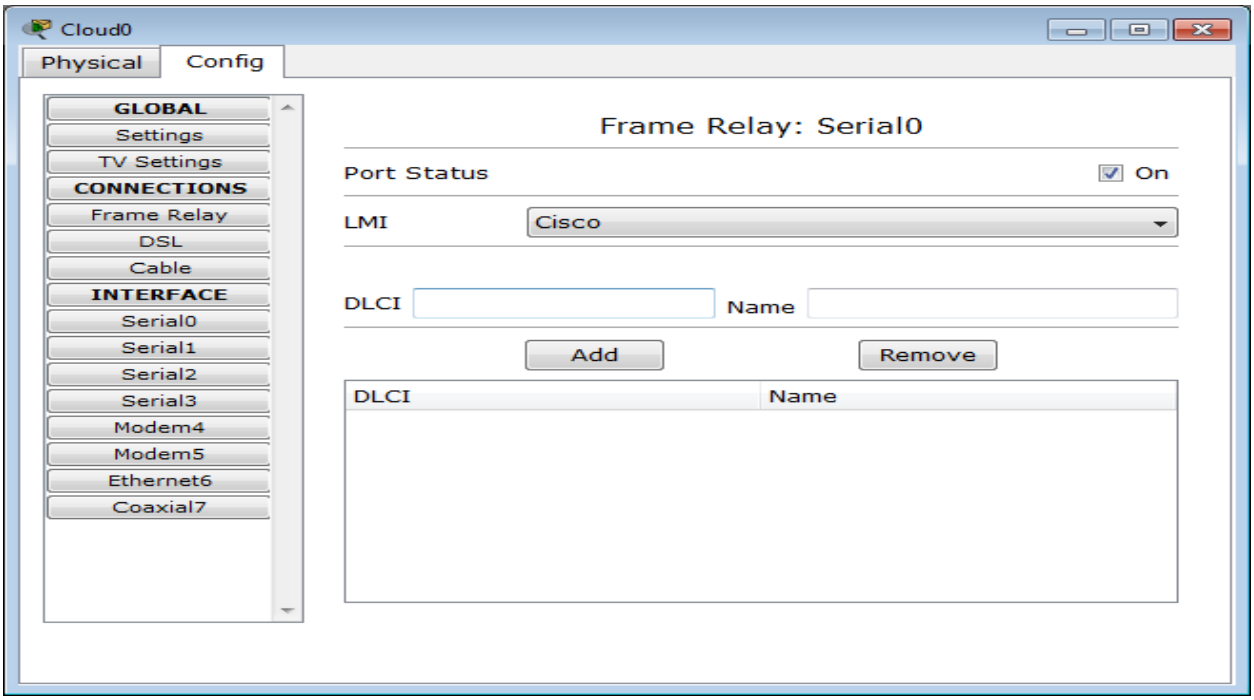
A hub and sopke sample network topology is created in Cisco Packet Tracer :

- R0 router is the spoke router
- R1 and R2 routers are frame-relay spokes

- All frame relay routers are interconnected through a Cisco Packet Tracer Cloud device which emulates frame relay circuits.







Create the virtual circuits one the "Frame Relay" tab. DLCI's need to be configured on the "Serial" tabs before creating virtual circuits.

Frame Relay configuration - ISR router configuration

Frame relay hub router configuration (R0)

The hub router is configured with two sub-interfaces to create a virtual circuit with each spoke. Each frame relay sub-interface is mapped with the DLCI number of the corresponding circuit configured in the Packet Tracer WAN emulation Cloud. The DLCI number defines a single virtual connection through the WAN and are the Frame Relay equivalent to a hardware address.

The encapsulation frame-relay command is mandatory on the main serial interface before configuring frame-relay sub interfaces.

The clock rate defines the speed on the serial interface

```
interface Serial0/0/0
 no ip address
 encapsulation frame-relay
!
interface Serial0/0/0.101 point-to-point
 ip address 192.168.101.1 255.255.255.252
 frame-relay interface-dlci 101
 clock rate 2000000
!
interface Serial0/0/0.102 point-to-point
 ip address 192.168.102.1 255.255.255.252
 frame-relay interface-dlci 102
 clock rate 2000000
```

Frame relay spoke routers configuration (R1 and R2)

The spoke routers have only one virtual circuit configured to reach the hub router. The DLCI configured on both spoke routers is the same as the DLCI is locally significant between the WAN Cloud and each customer.

Router R1 configuration

```
interface Serial0/0/0
```

ip address 192.168.101.2 255.255.255.252

encapsulation frame-relay

frame-relay interface-dlci 100!

Router R2 configuration

interface Serial0/0/0

ip address 192.168.102.2 255.255.255.252

encapsulation frame-relay

frame-relay interface-dlci 100

!

7.6. CONCLUSIONS AND FUTURE WORK

Cloud computing is a new emerging technology

that is expected to significantly change the field of IT in the

next few years and lead it for the coming decades. Numerous

services and applications can be provided in the Cloud due

to its many interesting and promising characteristics

REFERENCES

1- Computer network - Wikipedia

2- David D. C., Kenneth T.P., David P.R, An introduction to local area networks, Proc. of the IEEE conf., Vol. 66, 1978

3- **https://maharatech.gov.eg/mod/hvp/view.php?id=1354**

4- **https://customersso1.fortinet.com/saml-idp/login/?**

5- **Fundamentals Of Computer Security Technology by Edward G. Amoroso.**

6- **Network Security by Mario Devargas.**

7- GTSI Group, "Cloud Computing - Building a Framework for Successful Transition," White Paper,GTSI Corporation, 2009.

8- Michael Miller, "Cloud Computing Pros and Cons for End Users", microsoftpartnercommunity.co.uk, 2009.