z

Saif edeen kharouf

ID : 19110044

(COVID-19) Vaccine Centres

Contents

[**Part 1:** 3](#_Toc74933825)

[Network types: 3](#_Toc74933826)

[1) Local area network (LAN): 3](#_Toc74933827)

[2) Personal area network (PAN): 3](#_Toc74933828)

[3) Metropolitan area network (MAN): 4](#_Toc74933829)

[4) Wide area network (WAN): 4](#_Toc74933830)

[Network topologies: 5](#_Toc74933831)

[1) Bus topology 5](#_Toc74933832)

[2) Star topology 5](#_Toc74933833)

[3) Ring topology 6](#_Toc74933834)

[4) Tree topology 7](#_Toc74933835)

[5) Mesh topology 7](#_Toc74933836)

[Network protocols: 9](#_Toc74933837)

[1) HTTPS: 9](#_Toc74933838)

[2) SMTP 10](#_Toc74933839)

[3) POP3 10](#_Toc74933840)

[4) DNS 11](#_Toc74933841)

[5) FTP 11](#_Toc74933842)

[Network devices: 11](#_Toc74933843)

[1) Router 11](#_Toc74933844)

[2) Switch 12](#_Toc74933845)

[3) NIC 12](#_Toc74933846)

[4) Access Point 13](#_Toc74933847)

[Server types 14](#_Toc74933848)

[1) Web server 14](#_Toc74933849)

[2) Mail server 14](#_Toc74933850)

[3) FTP Server 15](#_Toc74933851)

[4) DHCP server 16](#_Toc74933852)

[5) DNS server 16](#_Toc74933853)

[Inter-dependences of the hardware with network software: 17](#_Toc74933854)

[**Part 2.1:** 18](#_Toc74933855)

[2.1.a&b: blueprint and configuration 18](#_Toc74933856)

[2.1.c: services installed: 19](#_Toc74933857)

[2.2: my choice of network services and devices 20](#_Toc74933858)

[2.3: test plan 20](#_Toc74933859)

[2.4: maintenance schedule 21](#_Toc74933860)

[**Part 2.2** 21](#_Toc74933861)

[2.2.1: implementation of the network system: 21](#_Toc74933862)

[2.2.2&3: conducting a verification and analyzing the tests with their excepted results 21](#_Toc74933863)

[2.2.4&5: suggestions about potential enhancements for the network: 24](#_Toc74933864)

[**References:** 25](#_Toc74933865)

[**Declaration:** 26](#_Toc74933866)

# **Part 1:**

# Network types:

The computer network is a way to link a group of computers that enables them to communicate with each other and to share data, applications, and resources. There are four main types of networks: (Javatpoint, 2020) (Guru99, 2021)



1. Local area network (LAN): This computer network is used in a small area like an office and building which are connected to two computers or more through twisted pairs and coaxial cables. Its benefits lay in:

Low-cost because of the inexpensive network hardware like hubs, network adapters, and Ethernet cables.

Its high transition rate to transfer data.

The security it provides.

However, there are some problems with LAN such as:

As I discussed earlier it is cost-effective, but the initial cost of installing it is high.

It doesn’t provide privacy to the users, because the admin can check each user's files.

The critical data of an organization could be accessed by unauthorized users unless the admin secured the centralized data repository.

It requires constant administration if there is any problem in the network software or hardware related.



1. Personal area network (PAN): this idea was brought up by research scientist Thomas Zimmerman. And the reason behind calling it a personal area network that it is used for connecting personal devices within an individual person in ten meters range (around thirty feet). There are two types of PAN:

Wireless personal area network: its low-range network developed by wireless technologies like Wi-Fi, Bluetooth.

Wired personal area network: which is created by connecting it to a USB device.

Examples of PAN:

Body area network: it is a network that moves with the person like the mobile network. When a person establishes a connection it creates a connection with another device to share data.

Offline network: it also called a home network because it is created inside of homes. It integrates with printers, computers, and televisions but is not connected to the internet.

Small home office: it used to connect different devices using different devices with the internet and the corporate network with VPN.

Benefits of PAN:

Relatively secure and safe.

Provides short range up to ten meters.

Strictly restricted to a small area.

However, there are problems with using this network type:

Might establish a bad connection to other networks in the same range-bound.

It got limitations to distance.



1. Metropolitan area network (MAN): its geographic area is large and it forms a larger network by connecting multiple LAN networks. It is used by government agencies to connect to civilians and private industries. Moreover, its uses can go far over such as communications between banks in a city, airline reservations, colleges within a city, and in the military to each other. It is important for the following reasons:

Its fast communication by using the high speed carries like the fiber optics cables.

It provides excellent support for greater access to WAN and the extensive size networks.

It has a dual bus which means that it can transmit data in both ways synchronously.

It can include parts of the city or the whole city.

Still, there are problems with this network type:

It needs more cable to establish a connection from one place to another.

It is hard to make the system secure from hackers.

1. Wide area network (WAN): this network type I will consider implementing in the vaccine centres for the following reasons:

It extends over a huge geographical area like states and countries which is important for our case because we have 11 countries we need to connect.

Not limited to a single area, but it spans over a large geographical area through satellite links, fiber optics, and telephone lines.

The data is centralized as a result you don’t need to buy emails, files, and backup servers.

The programmers get updated files within seconds because the software companies are working on live servers.

Massages transmit fast.

We can share resources like a hard drive, and ram.

Doing business globally over the internet.

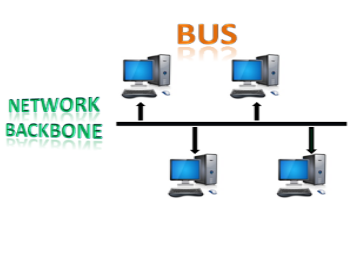
If the leased lines are used it will give higher bandwidth.

But, there are drawbacks of this network type it got security issues the reason behind it that it combines LAN and MAN which leads to the need of installing anti-virus and firewalls so that hackers can’t change the data or inject a virus into the network. Furthermore, it is not cost-effective considering we need to buy routers and switches and install them. And the big area it covers can cause troubleshooting problems and will be hard.



# Network topologies:

It is the structure of the network of how all the components are interconnected to each other. There are five mains types: (Javatpoint, 2020)



1. Bus topology: this topology is designed that all stations connected to a single cable which is called the backbone. The nodes have two ways of connecting, one directly to the backbone cable the other is by drop cable. When a device wants to send a message over the network all the available stations will receive it even if it is not addressed. The configuration of the topology is simpler than other topologies. It uses two IEEE standards the 802.3(Ethernet) or 802.4 standard networks.

This topology is beneficial because of these reasons:

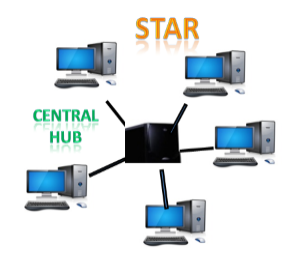
1. The initial cost of the installation is low the reason behind that the nodes are connected directly without any hub.
2. Its speed is moderate because it uses a coaxial cable or twisted pair which gives up to 10 Mbps.
3. Its arability of components and hardware, the familiarity of the technologies used, the installation and troubleshooting are widely used.
4. When a node fails it will not affect the rest nodes.

However, it has certain problems that need consideration:

1. It is simple but, it needs more cabling.
2. Specialized test equipment is required to determine the failures in the cables which can disrupt the communication between nodes.
3. If two nodes send massages together the signal will collide.
4. The network would slow down when adding a new device.
5. Repeaters are used to regenerate the signal because of the attenuation.

The common access method that is used in this topology is the CSMA (Carrier Sense Multiple Access) which is a media access control used to control the data flow to maintain the data integrity and the packets do not get lost. It got two different ways to handle the errors that occur when two nodes send messages at the same time:

* + - * 1. CSMA CD (collision detection): this is based on detecting the collisions, when the collision gets detected the sender will stop transmitting data. Thus, it works on “recovery after the collision”.
        2. CSMA CA (collision avoidance): it avoids the collision by checking the transmission media if it is busy or not. If it is busy it will hold the sender until the media becomes idle. Therefore, this will reduce the possibility of collisions.



1. Star topology: it is the most common network topology implementation and it is defined as the arrangement of the network which connects the nodes (also called clients) to a hub, switch, and central computers (also called servers). The type of cables that are used in this topology either Coaxial or RJ-45.

It is helpful in specific situations:

1. This topology is efficient the reason behind it that the stations are connected to a centralized network. Thus, the administrator only goes to a single station to troubleshoot the issue. The opposite from the bus topology which you need inspect kilometres of cables.
2. The changes can be automatically accommodated. Moreover, complex control features are easily implemented.
3. A failure in one cable will not affect the whole network because the stations are connected to a central hub that has it is own cable.
4. It is cost-effective for the familiar technologies it is using and the coaxial cables.
5. New stations can be easily added to open ports in the hub.
6. It is the bandwidth that can get approximately 100Mbps because of the Ethernet 100baseT that it uses.

Despite the advantages it has, it got issues:

1. All connected nodes will not be able to communicate if the central hub or switch goes down.
2. When a significate routing is needed the cable routing will be harder.



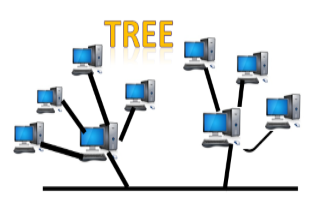
1. Ring topology: it is like the bus topology, but with connected ends and when a node receives a message from the previous computer it will retransmit it to the next node also each node is connected to the other with no termination point. The flow of the data in this topology unidirectional, the data moves in an endless loop, and it flows in a clockwise direction.

Its advantages:

1. Faulty devices can be removed without shutting down the network.
2. There are many tools for network operation and monitoring are available.
3. The installation cost is low as it uses twisted pair cables which is inexpensive.
4. The communication system is reliable because it does not rely on a single host computer.

Its disadvantages:

1. The same as bus topology, it requires specialized test equipment to determine the failures in the cables which can disrupt the communication between nodes.
2. When one station breakdown the network will fail.
3. The same as bus topology, the network would slow down when adding a new device.
4. Adding new devices will lead to more communication delays because it is directly proportional to the number of nodes.
5. Tree topology: this topology combines the characteristics of the bus topology and the star topology. It is a hierarchical structure in which all computers are connected to each other. Also, the nodes have different names such as, root node which is the top-most node, and descendants which are the rest of the nodes. The reason behind that is parent-child hierarchical, that there is only one path to transmit data between two nodes.



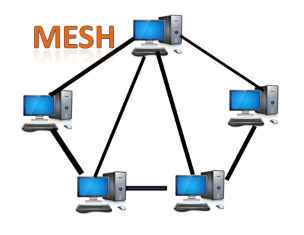
I would be implementing this topology in the network for the following reasons:

1. It is mainly used to provide broadband transmission meaning, the signals will not get attenuated in long distances.
2. It is easily expandable as we can add new devices to the network.
3. This network is divided into segments called star networks that are easily maintained and managed.
4. Error detection and correction are very easy in this topology.
5. The breakdown of one station will not affect the entire network.
6. It has point-to-point wiring for individual segments.

But, there are issues in this topology that needs consideration:

1. It will be hard to troubleshoot an issue if any fault occurs in one node.
2. Devices for broadband transmission are expensive.
3. Because of its reliability on the bus cable and if it failed the whole network will go down.
4. It is hard to reconfigure if a new device is added.

This physical topology uses the IEEE 802.4 (token ring) **logical topology**, and this is another reason I chose the tree topology. This logical topology got very high throughput and efficiency and supports priority to the stations. Also, it can handle short minimum frames, and applicable to Real-time traffic, the size of the file format is 8202 bytes and the size of the data field is between 0 and 8182 bytes. (*Difference between IEEE 802.3, 802.4 and 802.5 - GeeksforGeeks*, no date)



1. Mesh topology: an arrangement in which computers are interconnected with each other through various redundant connections. There are multiple paths from one computer to the other. There are no switches, hubs, or any central computers that act as a central point of communication. It is mainly used for WAN implementations because communication failures are critical and it is used in wireless networks an example would be the internet. This network topology can be formed in a formula: n=number of nodes.

There are two types of mesh topology:

1. Full mesh topology: all of the available computers are connected together.
2. Partial mesh topology: certain computers connected to those computers with which they communicate frequently.

This topology is helpful because of these reasons:

1. When a link breakdown it will not affect the rest of the communications thus it is reliable to use.
2. It is a fast communication between the nodes
3. When adding a new device it won’t disrupt the communications between the existing devices.

But, you will get certain issues when you use this topology:

1. Because it contains a large number of connected devices like routers and transmission media more than any network topology it will be expensive
2. This topology is very big and very difficult to manage and maintain therefore if it didn’t monitor carefully there will be detected communication link failure.
3. The efficiency of this topology is low because the number of redundant connections is high.

Contrasting the difference between two topologies:

|  |  |  |
| --- | --- | --- |
|  | Star topology | Bus topology |
| Cost | It is cost-effective as it uses coaxial cables. | It is also cost-effective as the cost of installation is low. |
| Troubleshooting | All the stations are connected to a centralized network therefore, the administrator only goes to a single host computer. | Specialized test equipment is needed to determine cable faults. |
| Bandwidth | 100Mbps. | 10Mbps. |
| Failures | It is limited if one cable failed that it will not affect the network. But, it will be a central point failure if the central hub goes down. | Limited when a node fails it will not affect the rest. However, if a cable failed the whole network will be affected. |

# https-communicationNetwork protocols:

1. HTTPS: this protocol that I will use instead of the normal HTTP. The following table will show the differences between them. (*HTTP vs HTTPS - javatpoint*, no date)

Source:(*https-communication.png (684×451)*, no date)

|  |  |
| --- | --- |
| HTTPS | HTTP |
| It stands for Hypertext Transfer Protocol Secure. | **It stands for Hypertext Transfer Protocol.** |
| It wrote in the address bar https://. | It wrote in the address bar http://. |
| Its port number 443. | **Its port number 80.** |
| It sends secured which makes it more secure (which we need). | It sends the plain text as it is thus this will not be secure. |
| It is used to transmit sensitive data like the bank account or in our case the national ID number and other personal information. | **It is only used in blogs.** |
| It uses SSL thus the data is encrypted. | It does not use SSL. |
| Google gives it a preference because that is a secure website. | **Google does not give it a preference because it is not a secure website.** |
| Because of the security and other features, it will be slower. | It is faster because of the lack of features and security. |
| Transport layer protocol. | **Application layer protocol.** |

Referring to the table, it is clear now why I will use HTTPS. The security features it has and the SSL (Secure Sockets Layer) encryption.

1. SMTP: stands for Simple Mail Transfer Protocol, and it is a “set of communication guidelines that allow the software to transmit an electronic mail over the internet”. (*SMTP - Simple Mail Transfer Protocol - javatpoint*, no date) Its characteristics:
2. It sends messages to other computers using e-mail addresses.
3. It provides mail exchanges between users on the same or different computers.
4. It supports sending a message to one or more recipients, the message can include text or video or graphics, and sending messages outside the internet.
5. It sets up communication rules between servers. Servers can identify themselves and announce what kind of communication they are trying to perform. Also, they can handle errors like incorrect email addresses.

\***I will explain more when I talk about the server.**

1. POP3: this protocol I will use instead of the IMAP. And here is the differences between them: (*IMAP vs. POP3 | Difference between IMAP and POP3 - javatpoint*, no date)

|  |  |
| --- | --- |
| POP3 | IMAP |
| Stands for post office protocol3. | Stands for Internet Messages Access Protocol. |
| Simple protocol and used only for downloading messages from the inbox to the local computers. | Advanced protocol compared to the POP3. It allows a user to check all the folders on the mail server and it is used to retrieve the emails. |
| It listens on port number 110, and POP3DS\* listens on port 995. | Listens on port 143, IMAPDS\* listens on port 993. |
| Mail can be accessed by a single device at a time. | Messages can be accessed using different devices. |
| We can read the message only when it is downloaded. | We can read messages partially before finishing the download. |
| Mail updated by local email software. | Mail updated by a software or web interface. |
| It does not allow the user to create, delete, or update the mailboxes on the mail server. | It allows the user to create, delete, or update on the mail server and also allows to create a hierarchy of mailboxes in the folder. |
| It does not allow to organize the mails on the server. | It allows organizing the mails on the server. |
| All messages can be downloaded at once. | The message header is previewed before the message is downloaded. |
| Emails are stored on the server and synced and can be accessed by multiple devices. | Emails are stored on a single device once they are downloaded and removed from the server. |

\*SD: the same protocol with the SSL encryption.

1. DNS: it stands for Domain Name System and it works on the fourth layer of the TCP/IP model the application layer. Its main characteristics:(*DNS - Domain Name System - javatpoint*, no date)
   1. It is a directory service that provides a mapping between the name of a host and its numerical address on the network
   2. It is required for the functioning of the internet.
   3. It is a service that does not let you remember the IP address of the website is being translated to a name and makes it more user-friendly.

\***I will explain more when I talk about the server.**

1. FTP: it stands for File Transfer Protocol and it works on the fourth layer of the TCP/IP model the application layer. Its main characteristics: (*FTP - File Transfer Protocol - javatpoint*, no date)
   1. It is mainly used to transfer files from their creator to the computer which is a server for other computers on the internet.
   2. It is used to download files to computers from other servers.
   3. Transfer the data more reliable and efficient and this one of its advantages.
   4. It encourages to use on remote computers.
   5. It is the fastest way to transfer files.
   6. It provides the security the reason behind it that it asks for the username and password.
   7. It provides transfer files back and forth. For example, the admin sends a message then the users' reply.

\***I will explain more when I talk about the server.**

# C:\Users\saif\AppData\Local\Microsoft\Windows\INetCache\Content.Word\router.pngNetwork devices:

1. Router: it is either a physical or virtual internetworking device its job to receive, analyse, and forward data packets between computer networks. It can decide the best way to transfer the packets by examining the IP address of the given data pocket and uses the forwarding tables and headers. The popular companies to develop routers Cisco, 3Com, HP, Juniper, D-Link, Nortel. The main characteristics of this device:(*What is Router - javatpoint*, no date)
2. It is used in [LAN](#_Network_types:) or [WAN](#_Network_types:) environments.
3. It shares information with other routers in the network.
4. It uses routing protocols like OSPF, BGP, IGRB, EIGRB, EGB, and RIP to transfer the data.
5. It is more expensive than other network devices.
6. It works on the third layer of the OSI model (network layer).
7. Because it can calculate the best route to pass the network packets from the source to the destination automatically it is called an **intelligent device**.



1. Switch: provides the facility to share information and resources by connecting different network devices. There are two types of the switch: (*Switch Vs. Router | Difference between Switch and Router - javatpoint*, no date) picture: (*Ethernet Switches |*, no date)
2. Unmanaged switches: it is used for basic connectivity and in small networks or wherever only a few ports are required. And it is plug and play which means that is no need to configure.
3. Managed switches: they are more secure. And they are easily configured thus they are more flexible and it has greater control.

Advantages of switch:

1. Enhances the available bandwidth and the performance of the network.
2. It can be directly connected to the workstations or devices.
3. It will reduce frame collision because it develops the collision domain for each network.
4. It reduces the workload on the individual host such as PCs.

Characteristics of switch:

1. It works on the second layer (data link).
2. It is used within the [LAN](#_Network_types:) environment.
3. It can’t perform NAT or Network Address Transition.
4. It works either on half-duplex or full-duplex transition mode.
5. It is considered a semi-intelligent device.
6. Cannot be worked on wireless networks.
7. It uses the CAM (Content Addressable Memory) table for the source and destination MAC address.
8. NIC (Network Interface Card): it’s a hardware component that the computers or any network device cannot ignore. It is also called network interface controller, network adapter, or LAN adapter. Its purposes: (*What is network interface card (NIC)?*, no date)
9. It allows both wired and wireless communications
10. It allows communications between computers connected via [LAN](#_Network_types:) and in a large-scale network through internet protocol (IP).
11. Works on physical and data link layers.



There are two types of NIC:

1. Internal Network Cards: the motherboard has a slot to insert the network card which can be inserted by Peripheral Component Interconnect (PCI) connection or it is inserted Industry Standard Architecture (ISA).



1. External Network Cards: it used in devices that do not have NIC installed. And they are two types either wireless and USB based.



1. Access Point (AP): it works on the second layer of the OSI model the data link layer. Its characteristics: (*Network Devices Explained*, no date)
2. It creates a Wireless LAN (WLAN) because it contains a transmitter and a receiver.
3. It provides a connection point between WLANs and Ethernet [LAN](#_Network_types:)s by using wireless infrastructure network mode.
4. It has several ports to be able to expand the network and to add additional clients.
5. It used to allow access to expand the range of the wireless network, therefore, allowing to access it more wireless clients.

Access points have two types:

1. Fat APs: it sometimes referred to as autonomous APs, the network and security settings are needed to be manually configured. Moreover, they are essential to be left alone to serve clients until they cannot function.
2. Thing APs: they can be controller-based or stand-alone. Also, they allow remote configuration using a controller. And they are easily reconfigured and monitored because they do not need to be manually configured.

# Server types

1. Web server: it is hardware and software that uses HTTP (or [HTTPS](#_Network_protocols:)) protocol and other protocols to respond to client requests over the internet. The hardware is connected to the internet and allows data to be exchanged with connected devices. And it is an example of the **client/server model**. To host the websites you must have web server software. They are used in web hosting, or to host the data for websites and web applications. It uses also, sends and receives emails, downloads requests for the [FTP](#_Network_protocols:) files, and it builds and publishes webpages. It has two types: (*What is a Web Server and How Does it Work?*, no date)
2. Static web server: it is static because it sends hosted files as is to the browser. And it contains a computer and HTTP software.
3. Dynamic web server: it contains a web server and other software like an application server and database. The reason behind calling it dynamic that the application server can be used to update hosted files before sending them to the browser. And the web server can generate content when the database requests it. Though this is more flexible it is more complicated.

Web server software:

1. Apache HTTP Server: Developed by Apache Software Foundation, it is a free and open-source web server for Windows, Mac OS X, UNIX, Linux, Solaris, and other operating systems; it needs the Apache license.
2. Microsoft Internet Information Services (IIS): Developed by Microsoft for Microsoft platforms; it is not open-sourced, but widely used.
3. Nginx: A popular open source web server for administrators because of its light resource utilization and scalability. It can handle many concurrent sessions due to its event-driven architecture. Nginx also can be used as a proxy server and load balancer.
4. Lighttpd. A free web server that comes with the FreeBSD operating system. It is seen as fast and secure while consuming less CPU power.
5. Sun Java System Web Server. A free web server from Sun Microsystems that can run on Windows, Linux, and UNIX. It is well-equipped to handle medium to large websites.
6. Mail server: it works on [POP3](#_Network_protocols:) and [SMTP](#_Network_protocols:) protocols and in the server/client model. its main characteristics that it handles and delivers e-mails over the internet and it can receive e-mails from client PCs and send them to other mail servers and vice versa. (*What is a Mail Server and How Does it Work? (Article)*, no date)

Open sources mail servers software:(*16 Free open-source email servers for enterprise and individuals*, no date)

1. IRedMail: it runs on Linux servers like RedHat, Ubuntu, CentOS, Debian, FreeBSD, and OpenBSD. And it supports secure connections with full support for POP3, IMAP, and SMTP. Emails are encrypted using TLS. Also, it features a web client and supports external webmail clients like Reoundcube. It also helps users to manage calendars (CalDav), address books (CardDav). Server admins can choose their favourite database store backends like MySQL, MariaDB, PostgreSQL, and OpenLDAP. Moreover, it has iRedMail has a built-in antispam and antivirus support with third-party extensions like SpamAssassin, ClamAV, SPF, and DKIM.
2. Postal: Postal is a complete Libre free mail server for the enterprise. It is the open-source equalivent for Sendgrid, Mailgun and Postmark. Postal supports all known protocols comes integrated with spam and virus protection. It offers a developer-friendly API.
3. Haraka: Haraka is an open-source SMTP server built with Node.js. It is highly scalable, extensible through plugins. Also, it runs seamlessly on Windows and Linux servers, and it requires minimal configuration.
4. Salmon: Salmon, also known as Python mail server is a free open-source mail server for developers who wish to create robust and complex server-based mail applications. Also, it is released under GNU GPLv3 and works seamlessly with Python web frameworks and libraries like Django and SQLAlchemy.
5. FTP Server: it is a computer that uses [FTP](#_Network_protocols:) to transfer data and it works on the client/server model. It needs either a transfer control protocol network or an internet protocol network to function. Its main characteristics:(*FTP Server - javatpoint*, no date)
6. It stores the address of the client files and creates a tunnel to share them.
7. Its connection remains connected all the time.
8. It helps to transfer files via the internet from one user to another.
9. It allows the users to access the data on the server however their some files cannot be accessed only by special users.
10. It provides anonymous access, which lets the user download from the server but not upload.
11. It is useful for people who got bad internet speed.
12. If the download failed you can resume the download.
13. It stores the data in encrypted form to protect it so that it does not fall in the wrong hands.
14. It has no memory limit to store data.

The FTP server got two types:

1. Anonymous server: common FTP server, for all FTP clients, there is no password required to access it.
2. Non-anonymous server: it is a paid server, the user needs a password to access the files.

Free open-source software for the FTP server:

1. FileZilla Server.
2. Xlight FTP Server.
3. Core FTP / SFTP Server.
4. ProFTPD.
5. Rebex Tiny SFTP Server.
6. DHCP server: it stands for Dynamic Host Configuration Protocol, which is a network management protocol. It dynamically assigns an IP address and other network configuration parameters to each device on the network to communicate with other IP networks. DHCP is an enhancement of an older protocol called BOOTP. However, this given IP address is valid for a limited period of time, and this is called the DHCP lease, and the period of validity is called the DHCP lease time. You can extend the lease rent via the DHCP lease renewal cycle. To avoid havening impacts from the DHCP server for not being available at the end of the lease time, clients generally start renewing their lease halfway through the lease period. This ensures robust IP address allocation to devices. If any device did not receive an answer for a new IP version 4 it will use automatic private internet protocol addressing (APIPA) to select an address. These addresses are in the network range 169.254.0.0/16. It usage scenarios: (*What is DHCP and why is it important? | EfficientIP*, no date)
7. Initial client connection: the client asks for an IP address to access the network services
8. IP usage extension: the client contacts the server to extend the usage of its current IP address.
9. Client connection after reboot: it contacts the server to confirm that it can use the same IP address as before the reboot.
10. Client disconnection: the client requests its IP address.

This server is being implemented and offered by the Internet Systems Consortium (ISC). It offers a complete open source solution to implement DHCP servers, rely agents, and clients. The DHCP service can be enhanced by DHCP failover to bring high availability and load balancing of traffic. The ISC DHCP Failover relies on having a pair of collaborating servers – a primary (master) server and a secondary (backup) server. A TCP-based communication channel called a failover channel, then has to be set up between the two servers. (*What is DHCP and why is it important? | EfficientIP*, no date)

1. DNS server: it uses the [DNS](#_Network_protocols:) protocol. the server divides into four types to load a webpage: (*What is DNS, How it Works + Vulnerabilities | Varonis*, no date)
2. DNS recursor: this server is responding to a DNS query and asks another DNS server for the address, or already has the IP address for the site saved.
3. Root name server: it is the name server for the root zone. It responds to direct requests and returns a list of authoritative name servers for the corresponding top-level domain.
4. TLD (Top-Level Domain) name server: it is a high-level DNS server on the internet when a search for a website that ends with a generic domain like com or gov will respond first to the name of the website.
5. Authoritative name server: The authoritative name server is the final stop for a DNS query. The authoritative name server has the DNS record for the request.

Free DNS servers: (*Best Free DNS Servers | 14 Options to Check Out | Allconnect*, no date)

1. Cloudflare: IP address 1.1.1.1. It features unmetered mitigation for DDoS, global CDN, shared SSL certificate, three-page rules, and unlimited bandwidth. And it is designed for mobile devices.
2. Google public DNS: IP address 8.8.8.8. It focuses on the “speed, security, and validity of results.” It only offers DNS resolution and caching — there is no site-blocking with Public DNS.
3. Yandex DNS: IP address 77.88.8.7. It is Russian-based, features faster internet access, and blocks malware and bots.

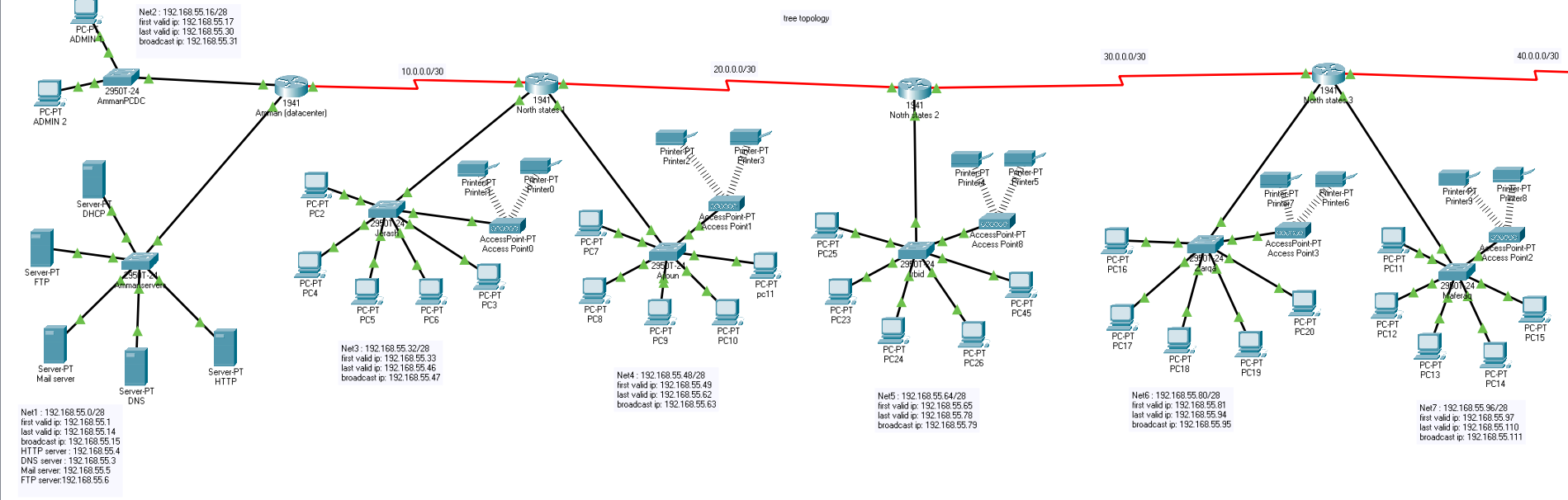
# Inter-dependences of the hardware with network software:

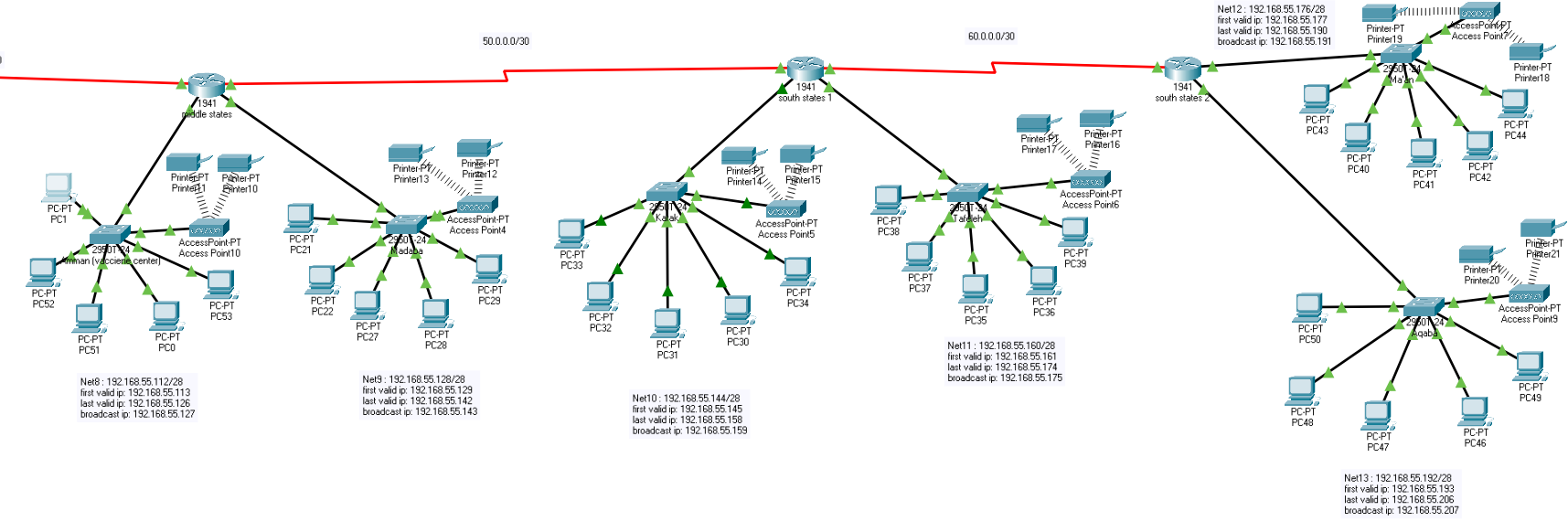
Every device needs software and vice versa, so I will highlight important devices and software:

1. Clients' PC: to enable the [protocols](#_Network_protocols:) and use the services from the [servers](#_Server_types) they need to install certain apps to use them. For example to use email servers and their protocols you need to install Gmail, Microsoft outlook, and yahoo mail. And to use the web server and DNS server you need to install chrome, Firefox, and Microsoft Edge. And to use the FTP servers and protocols to download files or upload or transfer them you need to go to websites or apps that support it like the E-learning system that we upload and download files.
2. Servers: to enable the protocols you need to install software on them. Like web server needs for example Apache server. Also, the FTP server needs a FileZilla server. And the mail server needs IRedMail. And for DHCP server needs Internet Systems Consortium (ISC). And the DNS server needs Cloudflare.
3. Network devices: [network devices](#_Network_devices:) need software to work on like the router it needs pfsense software to work and make configuration. (*13 Best Open Source Router OS for Small to Large Networks (2021)*, no date)

# **Part 2.1:**

## 2.1.a&b: blueprint and configuration





|  |  |  |  |
| --- | --- | --- | --- |
| Network address | First valid IP(gateway) | Last valid IP | Broadcast IP |
| 192.168.55.0 | 192.168.55.1 | 192.168.55.14 | 192.168.55.15 |
| 192.168.55.16 | 192.168.55.17 | 192.168.55.30 | 192.168.55.31 |
| 192.168.55.32 | 192.168.55.33 | 192.168.55.46 | 192.168.55.47 |
| 192.168.55.48 | 192.168.55.49 | 192.168.55.62 | 192.168.55.63 |
| 192.168.55.64 | 192.168.55.65 | 192.168.55.78 | 192.168.55.79 |
| 192.168.55.80 | 192.168.55.85 | 192.168.55.94 | 192.168.55.95 |
| 192.168.55.96 | 192.168.55.97 | 192.168.55.110 | 192.168.55.111 |
| 192.168.55.112 | 192.168.55.113 | 192.168.55.126 | 192.168.55.127 |
| 192.168.55.128 | 192.168.55.129 | 192.168.55.142 | 192.168.55.143 |
| 192.168.55.144 | 192.168.55.145 | 192.168.55.158 | 192.168.55.159 |
| 192.168.55.160 | 192.168.55.161 | 192.168.55.174 | 192.168.55.175 |
| 192.168.55.176 | 192.168.55.177 | 192.168.55.190 | 192.168.55.191 |
| 192.168.55.192 | 192.168.55.193 | 192.168.55.206 | 192.168.55.207 |
| 192.168.55.208 | 192.168.55.209 | 192.168.55.222 | 192.168.55.223 |
| 192.168.55.224 | 192.168.55.225 | 192.168.55.238 | 192.168.55.239 |
| 192.168.55.240 | 192.168.55.241 | 192.168.55.254 | 192.168.55.255 |

Subnet mask = 255.255.255.240 / 28.

I will use different public networks between every router (and I will use to connect the networks Rip configuration):

Amman datacentre – north states1: 10.0.0.0/30 Middle state – south states1: 50.0.0.0/30

North states1- north states2: 20.0.0.0/30 south states1 – south states2: 60.0.0.0/30

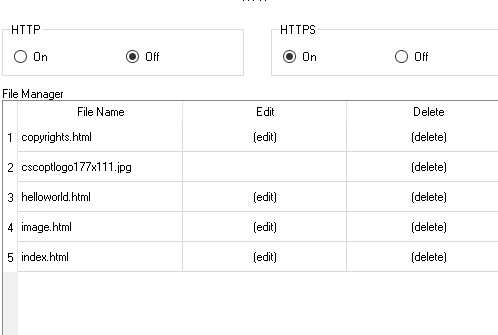
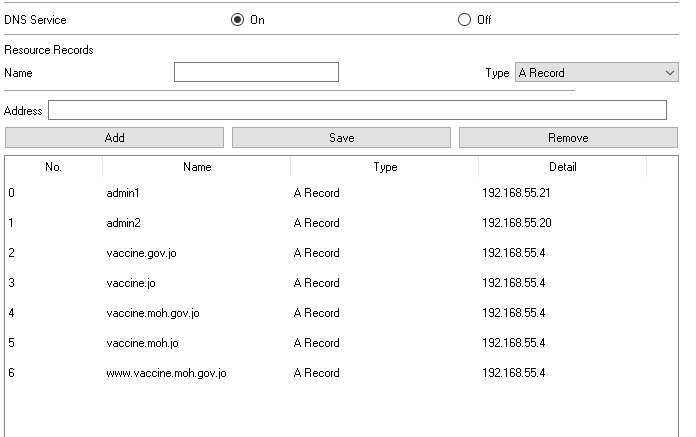
North states2 – north states3: 30.0.0.0/30

North states3 – middle state: 40.0.0.0/30

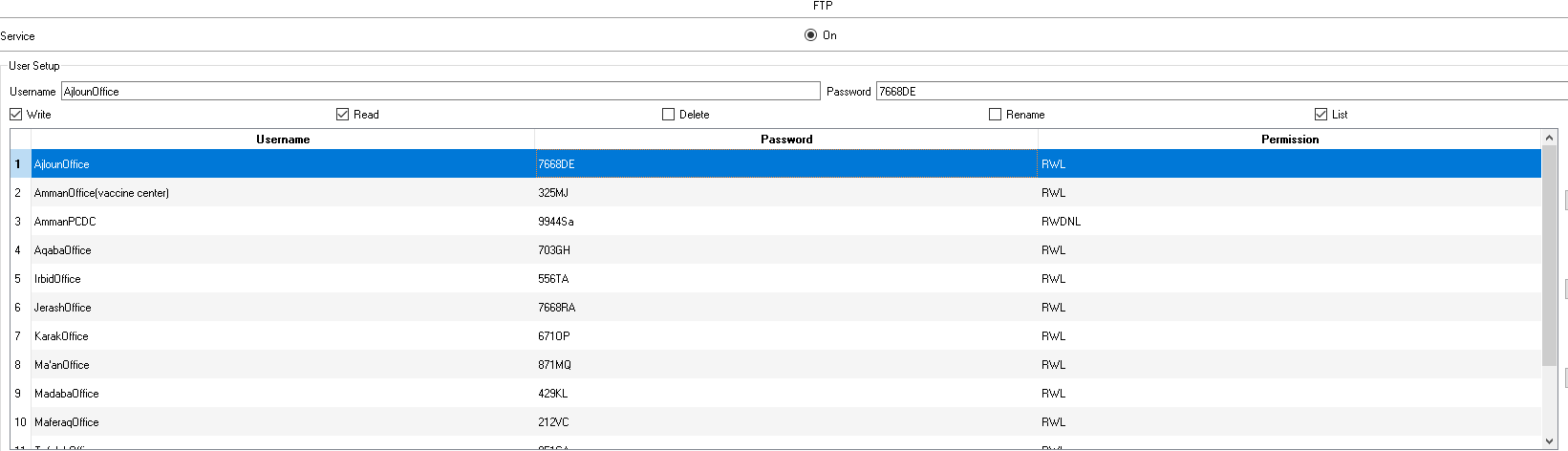
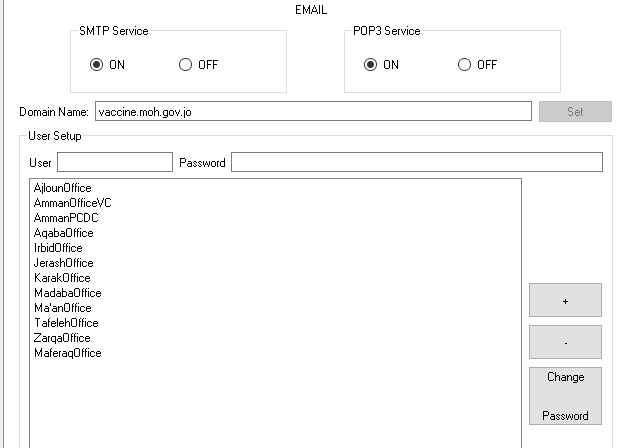
## 2.1.c: services installed:

1. HTTP server: 192.168.55.4
2. DNS server: 192.168.55.3
3. Mail server: 192.168.55.5
4. FTP server: 192.168.55.6
5. DHCP server: 192.168.55.2

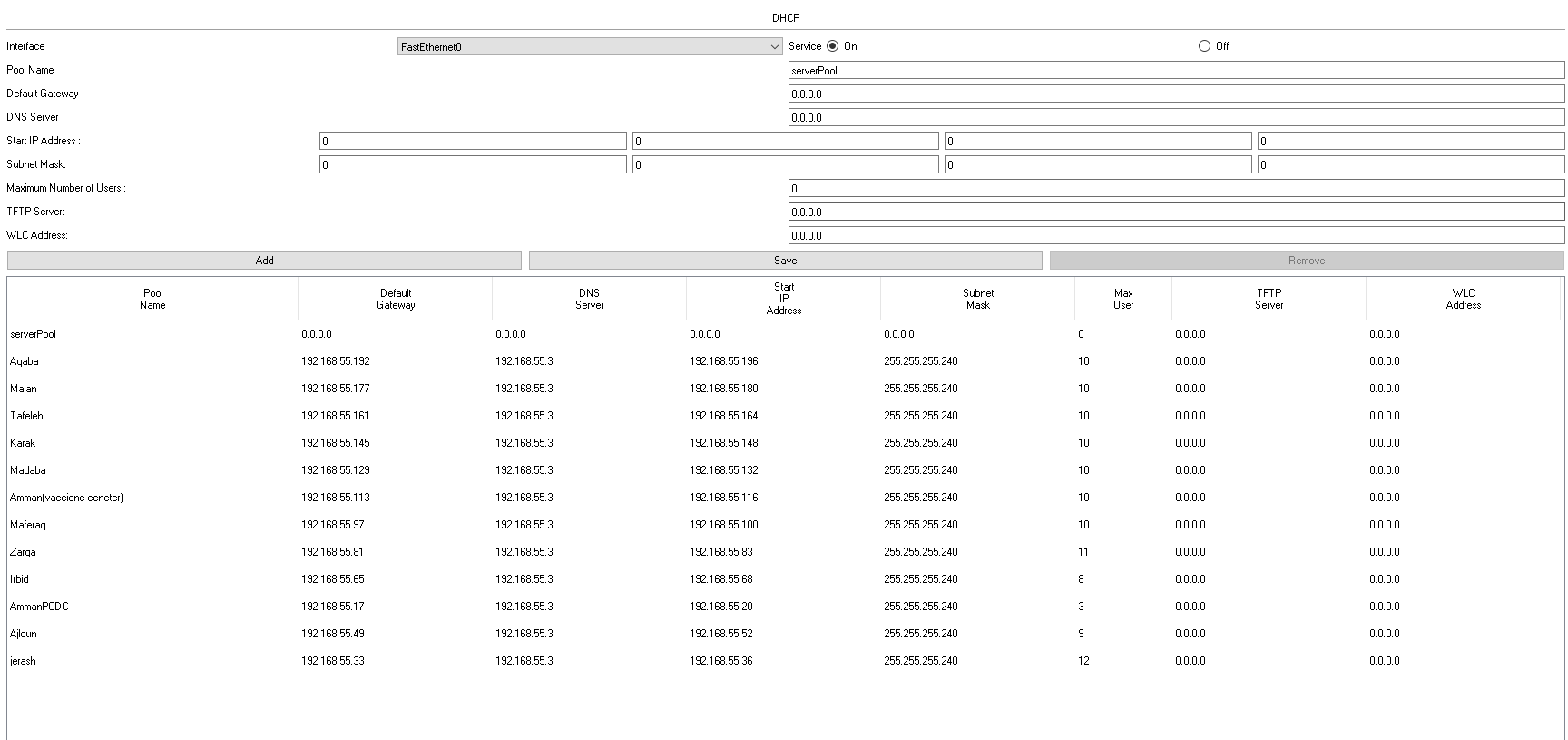
HTTP DNS



E-mail FTP



DHCP



## 2.2: my choice of network services and devices

I explained my choices in [network services](#_Network_protocols:) and [network devices](#_Network_devices:) sections in [part 1](#_Part_1:).

## 2.3: test plan

1. The connection between devices is tested using the ping command and it is expected to reply to the packets that are being sent.
2. The path or the route between devices using the tracert command and is expected to give all networks it hoped on to arrive at the destination (without any request timed out).
3. To check that we have no problems with the DNS service we use the nslookup command is being used and it is expected to give us the address of the domain name.
4. To check there are no problems with the FTP server we test all the permissions that are given to users using these commands to enter them we use the ftp command, put for upload, get for download, dir for the list, delete for delete, and rename for rename. And the expected result that the files are downloaded or listed or renamed or deleted or uploaded depending on the permission and the command entered.
5. To check if the router configurations are configured properly we use the sh run command and the sh ip route and we expect to see all the configurations are on and running.
6. To check if the email server is working we will use two computers or devices to send to each other emails’ and we will expect to see messages is being sent and received.
7. To check if the web server is working and the HTTPS is working I will search the domain name into the web browser and the expected results is to work and it should not give us an error code.

## 2.4: maintenance schedule

There should be certain maintenance to the overall network and here is the list of these maintenances:(*What Is Network Maintenance? | Network Maintenance Plans & Tips*, no date)

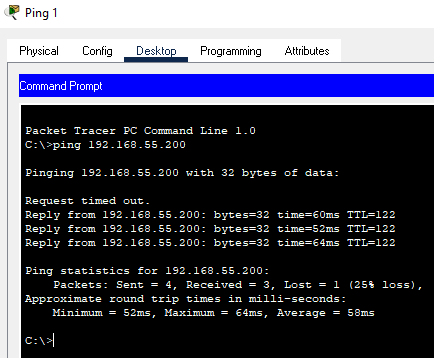
1. 24/7 monitoring and defense: robust monitoring includes defenses like advanced breach and threat detection, antivirus protections, comprehensive and calendar-set data back-up, and robust security software.
2. Device maintenance: to properly maintain the physical devices, organizations should have accurate gauge of what and where the devices are, and track their health and activates.

# **Part 2.2**

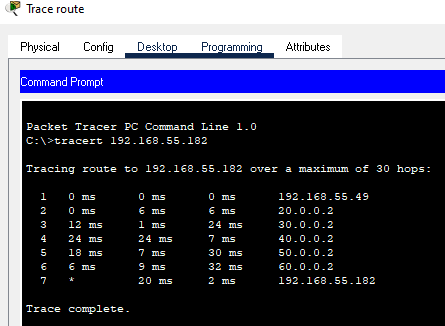
## 2.2.1: implementation of the network system:

**Available on e-learning**

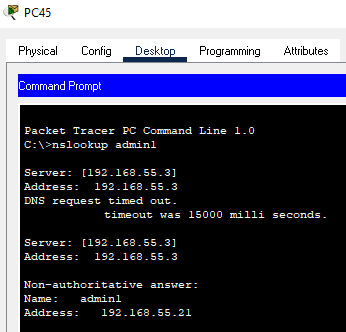
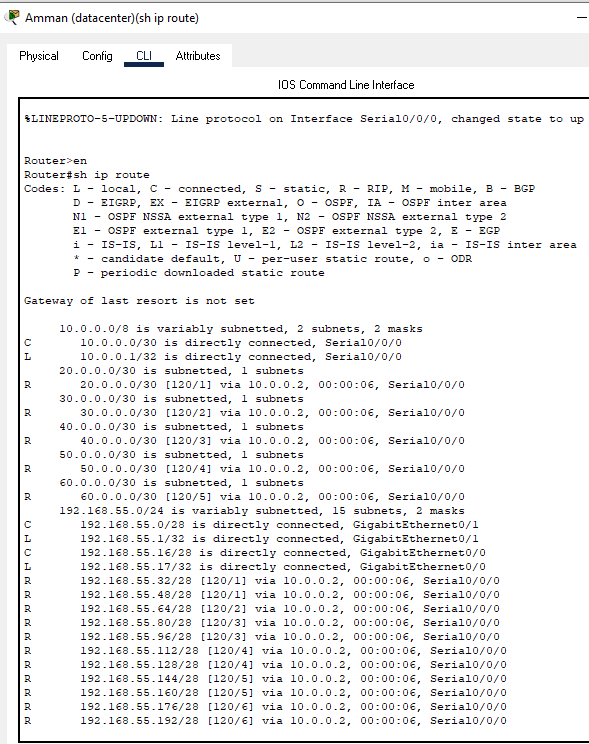
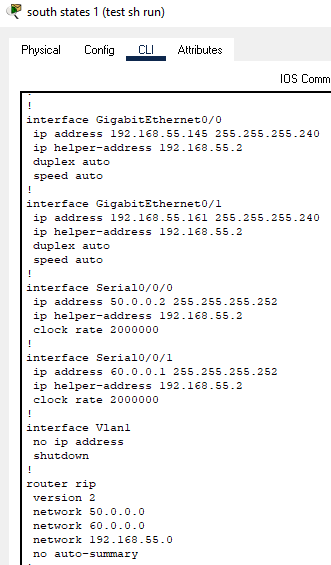
## 2.2.2&3: conducting a verification and analyzing the tests with their excepted results

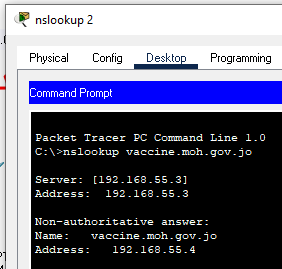


The first test I did that I checked between two devices using the ping and it met the expected results to reply to the packets as this picture shows.

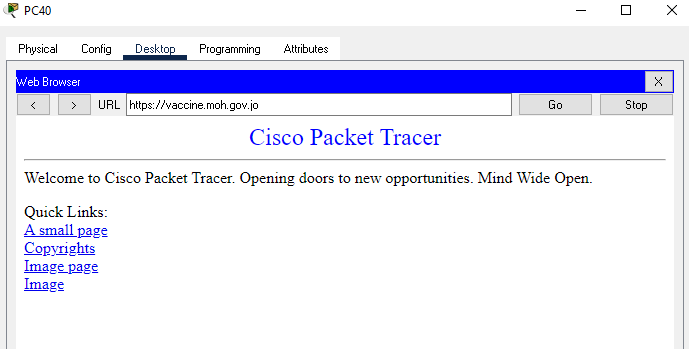
The second test I did that I tested the paths or routes between two devices and it met the expected results that it showed every network it hoped on as this picture shows.

The third test I did if the routers configured properly and it met the expectation that all configurations are on and working as these pictures shows.

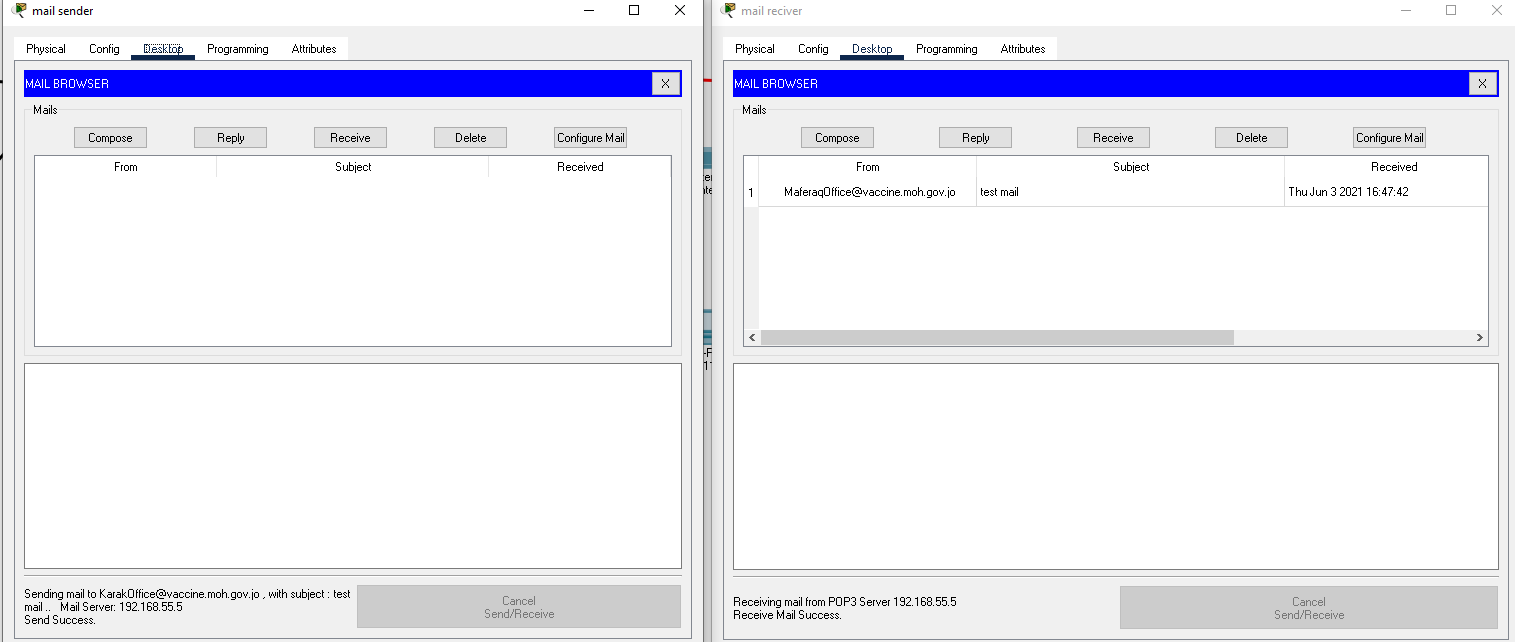


The fourth test I did that I checked for the DNS service is working I tested it on two domain names and it met the expected result that it gave us both the IP address and the domain name as these pictures shows.

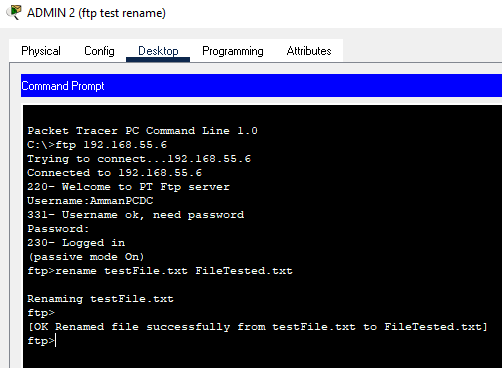
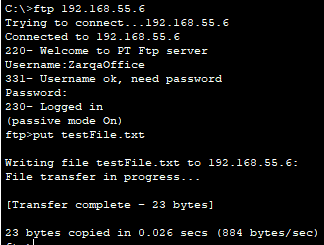
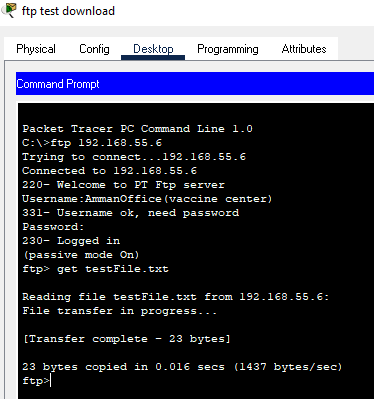
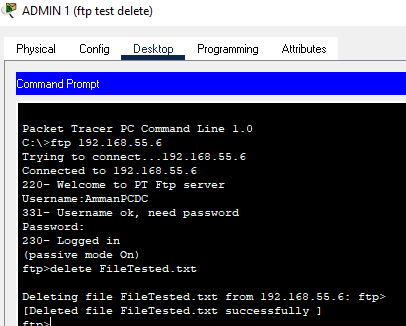
The fifth test I did that I checked for the web server and looked it up on the web browser and it gave me the expected results without any error codes as this picture shows.

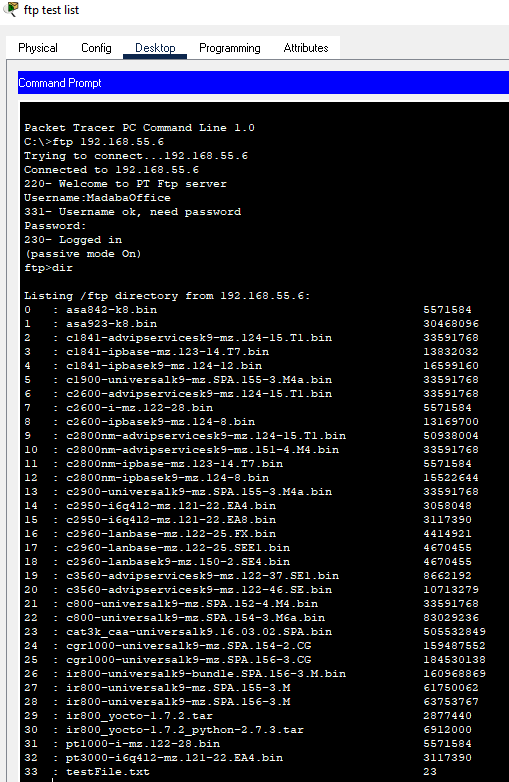


The sixth test I did that I checked if the email service is working by sending and receiving a message between two devices and it met the expected results that the messages are being sent and received as this picture shows.



The seventh and the last test I did that I checked for the ftp server and the service was working and it met the expected result for each device and users’ permissions and it they are working as these pictures shown.



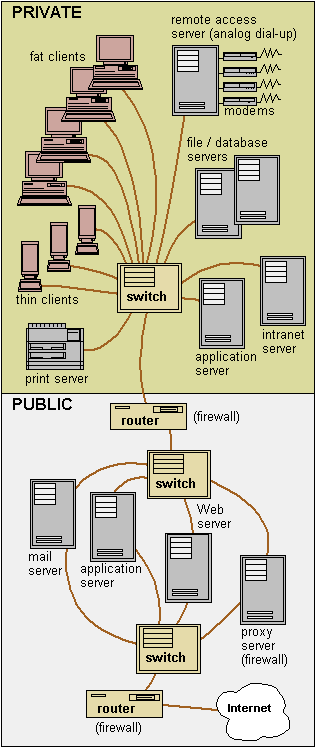


## 2.2.4&5: suggestions about potential enhancements for the network:

(*What Is A Proxy Server? | PCMag*, no date)

I would suggest putting a proxy server in the network to add an extra layer of security. And it is a computer system or router that works like rely between client and server and all of the requests from the internet go to the proxy server first then it checks for the request and forwards into the internet. This prevents any attacks on the private network and one of its tools uses to build a firewall.

In this example, the proxy server functions as a firewall in the public side of a company network, which is called the "demilitarized zone"



# **References:**

*13 Best Open Source Router OS for Small to Large Networks (2021)* (no date). Available at: https://www.networkstraining.com/best-open-source-router-os/ (Accessed: 17 June 2021).

*16 Free open-source email servers for enterprise and individuals* (no date). Available at: https://medevel.com/list-os-mail-server/ (Accessed: 16 June 2021).

*Best Free DNS Servers | 14 Options to Check Out | Allconnect* (no date). Available at: https://www.allconnect.com/blog/best-free-dns-servers (Accessed: 17 June 2021).

*Difference between IEEE 802.3, 802.4 and 802.5 - GeeksforGeeks* (no date). Available at: https://www.geeksforgeeks.org/difference-between-ieee-802-3-802-4-and-802-5/ (Accessed: 7 June 2021).

*DNS - Domain Name System - javatpoint* (no date). Available at: https://www.javatpoint.com/computer-network-dns (Accessed: 15 June 2021).

*Ethernet Switches |* (no date). Available at: https://signamax.com/switches/ (Accessed: 14 June 2021).

*FTP - File Transfer Protocol - javatpoint* (no date). Available at: https://www.javatpoint.com/computer-network-ftp (Accessed: 15 June 2021).

*FTP Server - javatpoint* (no date). Available at: https://www.javatpoint.com/ftp-server (Accessed: 17 June 2021).

Guru99 (2021) *Types of Computer Networks: LAN, MAN, WAN, VPN*, *guru99*. Available at: https://www.guru99.com/types-of-computer-network.html (Accessed: 18 May 2021).

*HTTP vs HTTPS - javatpoint* (no date). Available at: https://www.javatpoint.com/http-vs-https (Accessed: 12 June 2021).

*https-communication.png (684×451)* (no date). Available at: https://www.tutorialsteacher.com/Content/images/https/https-communication.png (Accessed: 14 June 2021).

*IMAP vs. POP3 | Difference between IMAP and POP3 - javatpoint* (no date). Available at: https://www.javatpoint.com/imap-vs-pop3 (Accessed: 13 June 2021).

Javatpoint (2020) ‘Types of Computer Network - javatpoint’. Available at: https://www.javatpoint.com/types-of-computer-network (Accessed: 18 May 2021).

*Network Devices Explained* (no date). Available at: https://blog.netwrix.com/2019/01/08/network-devices-explained/ (Accessed: 15 June 2021).

*SMTP - Simple Mail Transfer Protocol - javatpoint* (no date). Available at: https://www.javatpoint.com/simple-mail-transfer-protocol (Accessed: 13 June 2021).

*Switch Vs. Router | Difference between Switch and Router - javatpoint* (no date). Available at: https://www.javatpoint.com/switch-vs-router (Accessed: 14 June 2021).

*What is a Mail Server and How Does it Work? (Article)* (no date). Available at: https://www.samlogic.net/articles/mail-server.htm (Accessed: 16 June 2021).

*What Is A Proxy Server? | PCMag* (no date). Available at: https://www.pcmag.com/encyclopedia/term/proxy-server (Accessed: 18 June 2021).

*What is a Web Server and How Does it Work?* (no date). Available at: https://whatis.techtarget.com/definition/Web-server (Accessed: 16 June 2021).

*What is DHCP and why is it important? | EfficientIP* (no date). Available at: https://www.efficientip.com/what-is-dhcp-and-why-is-it-important/ (Accessed: 17 June 2021).

*What is DNS, How it Works + Vulnerabilities | Varonis* (no date). Available at: https://www.varonis.com/blog/what-is-dns/ (Accessed: 17 June 2021).

*What is network interface card (NIC)?* (no date). Available at: https://www.tutorialspoint.com/what-is-network-interface-card-nic (Accessed: 14 June 2021).

*What Is Network Maintenance? | Network Maintenance Plans & Tips* (no date). Available at: https://worldwideservices.net/network-maintenance-guide-upkeep/ (Accessed: 18 June 2021).

*What is Router - javatpoint* (no date). Available at: https://www.javatpoint.com/router (Accessed: 14 June 2021).