/Users/apple/Library/Containers/com.microsoft.Outlook/Data/Library/Caches/Signatures/signature_2105988401

**Networking**

**40302211**

**H/615/1619**

**Section (2)**

**Submitted to:**

Eng. Elham Derbas

**Submitted by:**

**Imad Addin**

**Spring –2024**

Contents

[Introduction 3](#_Toc168669876)

[1. Subnetting 3](#_Toc168669877)

[1.1 The WAN subnetting 3](#_Toc168669878)

[1.2 The LAN subnetting 5](#_Toc168669879)

[1.3 Subnetting table 6](#_Toc168669880)

[2. Putting devices and wiring 7](#_Toc168669881)

[3. Routers configuration 8](#_Toc168669882)

[3.1Giving IP addresses 8](#_Toc168669883)

[3.2 Routing 9](#_Toc168669884)

[4Servers 11](#_Toc168669885)

[4.1 DHCP 11](#_Toc168669886)

[4.2 FTP 14](#_Toc168669887)

[4.3 HTTPs 15](#_Toc168669888)

[4.4DNS 17](#_Toc168669889)

[4.5 Email 19](#_Toc168669890)

[5.Adding extra devices 21](#_Toc168669891)

[6.Testing 24](#_Toc168669892)

[7.self-regulation 25](#_Toc168669893)

[7.1Topology evaluation 25](#_Toc168669894)

[7.2 Improvement 25](#_Toc168669895)

[8.Maintenance Schedule 26](#_Toc168669896)

[9.Scalability Plan 26](#_Toc168669897)

[10.Logical Topology 27](#_Toc168669898)

[11.Interdependencies 27](#_Toc168669899)

# Introduction

This report includes my work for the programming source and it showcase my understanding of this course starting from showing what I went through while doing this assignment including all steps and how did I think in each step of this assignment, after reading the it and understanding every single point in it, and then mentioning the reason behind putting each devise and how to make sure that it works as needed , and then evaluating my work and look for possible improvements , and finally connecting what I took theoretically to what I implemented by show the packet trip and explain it using my networks.

# 1. Subnetting

## 1.1 The WAN subnetting

After reading the assignment brief 8 LAN networks have to be made ;Amman ,Amman (HQ) ,Ankara ,Riyadh ,Dubai ,Beirut ,Doha ,Kuwait and as the assignment brief said there is a possibility of a future expansion so this should be considered while subnetting ,the main IP address that is given to subnet is 201.0.0.0/24 , this IP address should be subneted to give each router interface an IP address so in each subnetwork we need 4 IP addresses (two for the interfaces and one as a network ID and one as a broadcast IP), and as the assignment brief mentioned no IP address should be wasted ;so I will subnet this IP address based on the hosts number as the following :

To find how many bits can be taken for the hosts we should find the value of x in this equation:

2^x-2=2 (number of hosts needed)

And here the value of x is two so two bits can be taken for the host so the form of the new subnetworks will be like this:

201.0.0. nnnnnnhh

n=bits for subnetworks

h=bits for hosts

note: the last octet is in binary and the rest are in decimal.

So to make the first subnetwork we should find the form of the first network which would be (200.0.0.000000hh) In this case , and in order to find the details of it we should find the first , last ,broadcast ,network IP address and I found them as the following :

network ID 🡪 replace all the host’s bits with zero.

first IP 🡪 replace the all the bits with zero except the last one make it one.

last IP 🡪 replace the all the bits with one except the last one make it zero.

broadcast IP🡪 replace all the host’s bits with one.

network ID 🡪 201.0.0.00000000

first IP 🡪 201.0.0.00000001

last IP 🡪 201.0.0.00000010

broadcast IP🡪 201.0.0.00000011

Now we should change the last octet from binary system to decimal system so the IP addresses will be like this:

network ID 🡪 201.0.0.0

first IP 🡪 201.0.0. 1

last IP 🡪 201.0.0.2

broadcast IP🡪 201.0.0.3

And they will be over thirty because there are thirty bits for the network.

network ID 🡪 201.0.0.0/30

first IP 🡪 201.0.0. 1/30

last IP 🡪 201.0.2/30

broadcast IP🡪 201.0.0.3/30

This is how I sonneted the WAN’s IP, but I am not sure how many subnets I need since I did not choose the logical topology yet.

## 1.2 The LAN subnetting

Moving to LAN’s subnetting the assignment mentioned the all the offices can’t have more than 100 employee except the HQ office it can’t have more than 70 employees so based in this case I will have to subnet the given IP which is 130.10.0.0/16 while trying to waste as least IP addresses as possible since the number subnetworks can expand by time but the employees number can’t as we said before we should find how many bits are there for the hosts by finding the value of x knowing that I will try to make 100 host’s IP addresses so it can cover all the offices including the HQ

2^x -2=100

As we can see there is no integer value that can solve this equation so we are left with two values 6 and 7 if we use 6 then we will have 62 IP addresses which is not enough but if we chose 7 we will have 126 IP addresses which is more than enough and there are not that much of waste, so the best value of x is 7 so seven bits can be taken for the host so the form of the new subnetworks will be like this:

130.10. nnnnnnnn. nhhhhhhh

n=bits for subnetworks

h=bits for hosts

note: the last two octets are in binary and the rest are in decimal.

So to make the first subnetwork we should find the form of the first network which would be (200.0.000000000.0hhhhhh) In this case , and in order to find the details of it we should find the first, last ,broadcast ,network IP address and I found them as the following :

network ID 🡪 replace all the host’s bits with zero.

first IP 🡪 replace the all the bits with zero except the last one make it one.

last IP 🡪 replace the all the bits with one except the last one make it zero.

broadcast IP🡪 replace all the host’s bits with one.

network ID 🡪 130.10.000000000.00000000

first IP 🡪 130.10.000000000.00000001

last IP 🡪 130.10.000000000.01111110

broadcast IP🡪 130.10.000000000.01111111

Now we should change the last two octets from binary system to decimal system so the IP addresses will be like this:

network ID 🡪 130.10.0.0

first IP 🡪 130.10.0. 1

last IP 🡪 130.10.0.126

broadcast IP🡪 130.10.0.127

And they will be over twenty-five because there are twenty-five bits for the network.

network ID 🡪 130.10.0.0/25

first IP 🡪 130.10.0. 1/25

last IP 🡪 130.10.0.126/25

broadcast IP🡪 130.10.0.127/25

Eight sub networks should be made like this because there are 8 LAN networks in the given scenario.

## 1.3 Subnetting table

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Network id | First IP | Last IP | Broadcast IP | Masked IP | Prefix |
| Amman (HQ) | 130.10.0.0 | 130.10.0.1 | 130.10.0.126 | 130.10.0.127 | 255.255.255.128 | 25 |
| Amman | 130.10.0.128 | 130.10.0.129 | 130.10.0.254 | 130.10.0.255 | 255.255.255.128 | 25 |
| Ankara | 130.10.1.0 | 130.10.1. 1 | 130.10.1.126 | 130.10.1.127 | 255.255.255.128 | 25 |
| Doha | 130.10.1.128 | 130.10.1.129 | 130.10.1.254 | 130.10.1.255 | 255.255.255.128 | 25 |
| Riyadh | 130.10.2.0 | 130.10.2. 1 | 130.10.2.126 | 130.10.2.127 | 255.255.255.128 | 25 |
| Dubai | 130.10.2.128 | 130.10.2.129 | 130.10.2.254 | 130.10.2.255 | 255.255.255.128 | 25 |
| Kuwait | 130.10.3.0 | 130.10.3. 1 | 130.10.3.126 | 130.10.3.127 | 255.255.255.128 | 25 |
| Beirut | 130.10.3.128 | 130.10.3.129 | 130.10.3.254 | 130.10.3.255 | 255.255.255.128 | 25 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Network id | First IP | Last IP | Broadcast IP | Masked IP | Prefix |
| Amman (HQ)  Kuwait | 201.0.0.0 | 201.0.0.1 | 201.0.0.2 | 201.0.0.3 | 255.255.255.252 | 30 |
| Amman (HQ)  Ankara | 201.0.0.4 | 201.0.0.5 | 201.0.0.6 | 201.0.0.7 | 255.255.255.252 | 30 |
| Amman (HQ)  Doha | 201.0.0.8 | 201.0.0.9 | 201.0.0.10 | 201.0.0.11 | 255.255.255.252 | 30 |
| Amman (HQ)  Riyadh | 201.0.0.12 | 201.0.0.13 | 201.0.0.14 | 201.0.0.15 | 255.255.255.252 | 30 |
| Amman (HQ)  Dubai | 201.0.0.16 | 201.0.0.17 | 201.0.0.18 | 201.0.0.19 | 255.255.255.252 | 30 |
| Amman (HQ)  Beirut | 201.0.0.20 | 201.0.0.21 | 201.0.0.22 | 201.0.0.23 | 255.255.255.252 | 30 |

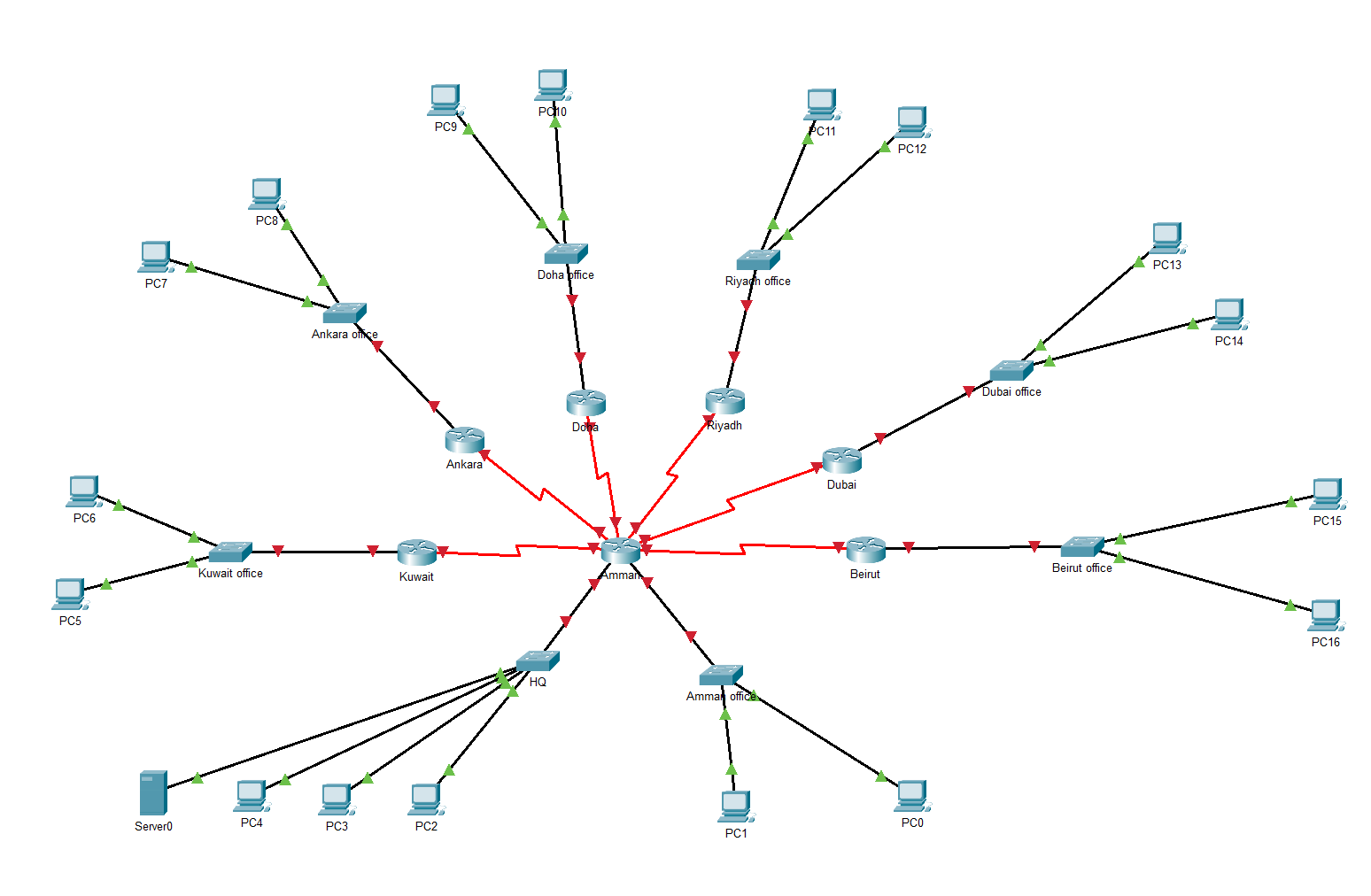
# 2. Putting devices and wiring

I have decided to make the network as a full mesh due to its reliability and security since it’s easy to add any routers in the future and if one connection between two routers get effected, they whole network won’t get effected, but due to lack of time I will make the topology as a hub and spoke.

The centered router of the network will be Amman’s router and two switches will be included so two networks can be there one for the HQ and the other is for the office.

In conclusion, the topology will be six routers each one of them is connected the Amman’s router and in each office, there will be 2 PCs, one network printer, Wi-Fi access, one laptop, and the HQ will have 3 PCs, all servers.

Here are the wired devices by using crossover wires for same devices and straight through wires for different devises and the serial wire between routers:



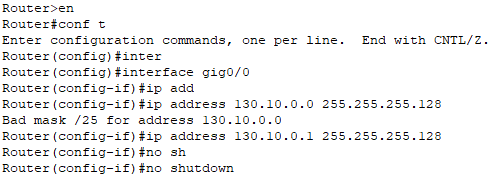
Note: this topology is not the final one it includes one server and pcs and router more servers laptops access points and printers will be added in later

Note : HWIC-2T were added to all routers to ass a serial port

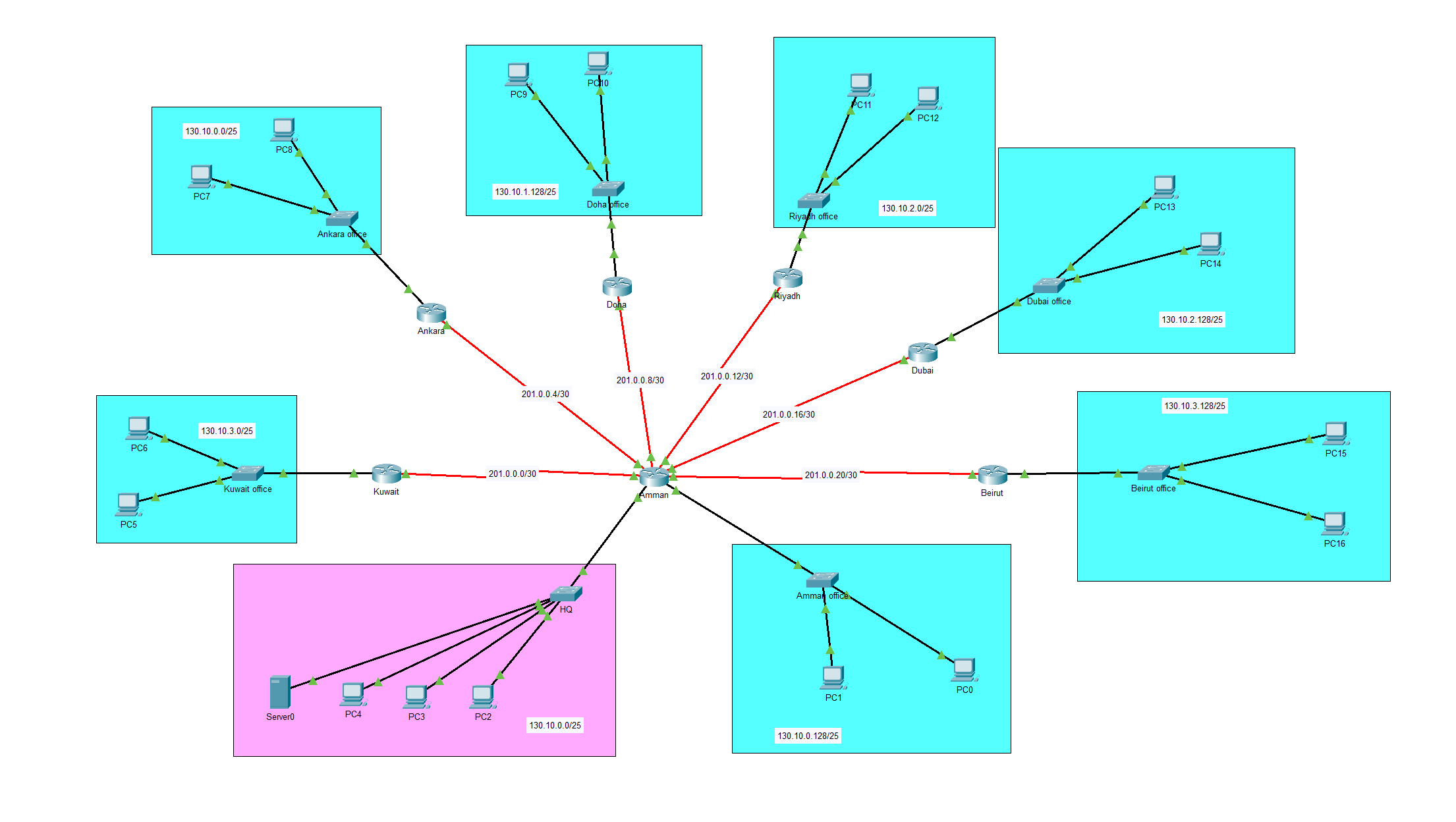
# 3. Routers configuration

## 3.1Giving IP addresses

Now moving to the routers configuration, I will add each interface IP address statically as the question asked and based on the subnetting table that I have already done; this can be done by entering the interface them give it an IP address and open it and this can be done by implementing the following commands:



After configuring all the routers this is the topology:

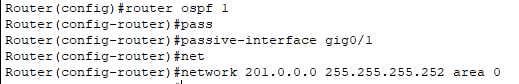


## 3.2 Routing

Routing needs to be implemented to make it possible for devices from different networks to communicate, and it is done by telling the router about any network that is not directly connected to it.

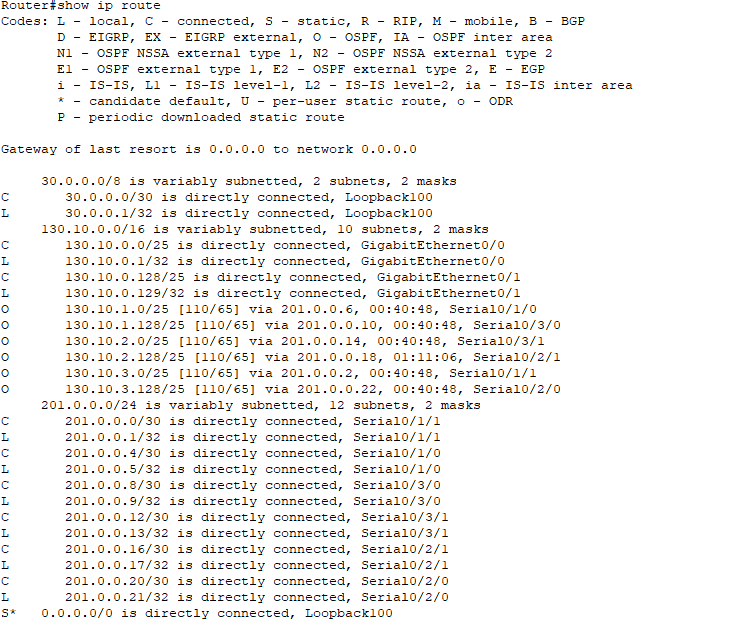
I have chosen OSPF as a routing protocol due to its low cost which with limit and minimize the latency on the network and it provides more flexibility for adding new networks and make it easier for the company to expand in the future, it works by putting and directly connected network in a table and all routers will exchange this table to make possible to communicate from different networks.

And here is how to implement OSPF using commands:



1. Putting the routers protocol.
2. Setting the LAN network interface as passive since it does not need data of other networks IP address.
3. Then put the network id to add it to the table.

Finally, I made sure that my routing was correct by seeing the routing table and checking the connectivity of each device:



A screen shot of a computer

Description automatically generated

Note: this photo was taken after the activating the DHCP server and the loopback interface

# Servers

Firstly, here is a table including each server and their ip addresses ,cost, infrastructure requirements ,hardware specification ,operating system and performance optimization

|  |  |  |
| --- | --- | --- |
| Server | Ip address | Masked ip |
| DHCP | 130.10.0.10 | 255.255.255.128 |
| FTP | 130.10.0.20 | 255.255.255.128 |
| EMAIL | 130.10.0.30 | 255.255.255.128 |
| HTTPS | 130.10.0.40 | 255.255.255.128 |
| DNS | 130.10.0.50 | 255.255.255.128 |

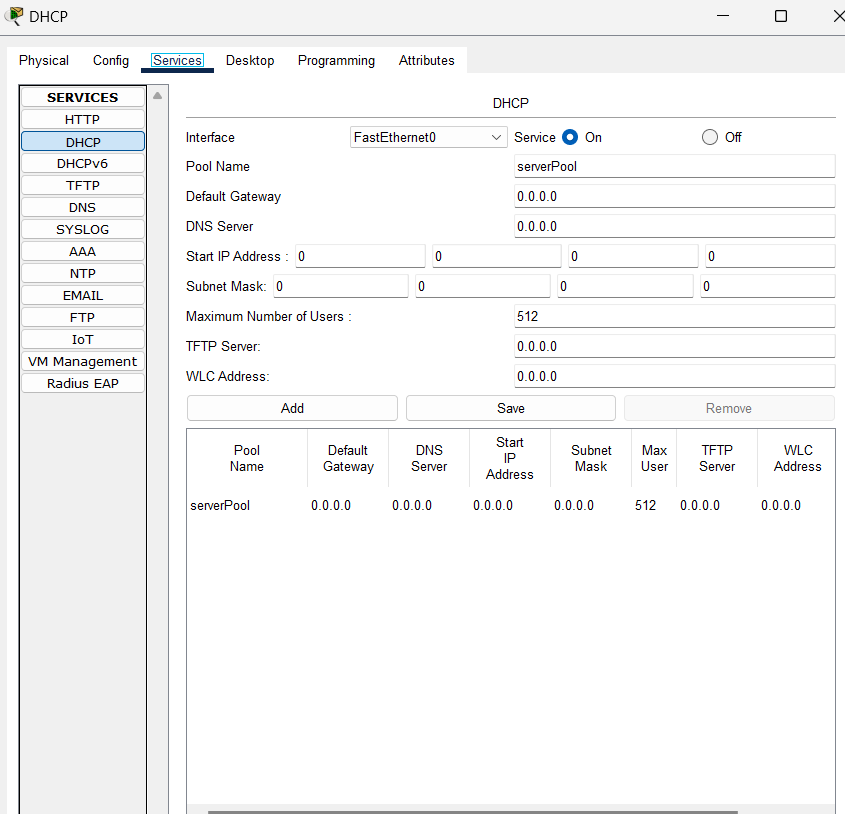
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Server | Operating System | Hardware Specifications | Infrastructure Requirements | Cost | Performance Optimization |
| DHCP | Windows Server | CPU: Intel Xeon E-2236 RAM: 16GB DDR4 Storage: 500GB SSD | 1U rack space Gigabit Ethernet connection | $1,200 | Optimized for high availability and load balancing Regular updates and patches Efficient IP address allocation strategies |
| FTP | Ubuntu Server | CPU: Intel Xeon E-2246G RAM: 8GB DDR4 Storage: 1TB HDD | 1U rack space Gigabit Ethernet connection | $900 | Use of RAID for data redundancy Regular maintenance of FTP logs Secure file transfer protocols (SFTP) |
| Email | Microsoft Exchange Server | CPU: Intel Xeon E-2278G RAM: 32GB DDR4 Storage: 2TB SSD | 2U rack space Redundant power supply Gigabit Ethernet connection | $3,000 | Mailbox database optimization Anti-spam and anti-malware protection Load balancing across multiple servers |
| HTTPS | Ubuntu Server | CPU: Intel Xeon E-2236 RAM: 16GB DDR4 Storage: 500GB SSD | 1U rack space Gigabit Ethernet connection | $1,200 | SSL/TLS certificate management HTTP/2 for improved performance Load balancing and failover mechanisms |
| DNS | Windows Server | CPU: Intel Xeon E-2236 RAM: 16GB DDR4 Storage: 500GB SSD | 1U rack space Gigabit Ethernet connection | $1,200 | Caching and recursive DNS optimization Implementation of DNS security extensions (DNSSEC) Regular updates and monitoring |

## 4.1 DHCP

Now each router can send a packet to any other router, but pcs can communicate with each other yet because they don’t have IP addresses and a protocol is needed to give pcs IP addresses dynamically and this protocol is called DHCP or Dynamic Host Configuration Protocol and this server powered by this service or protocol do the job of giving IP addresses for each pc in every network and here are the steps of doing this :

after giving the server an IP address, we should:

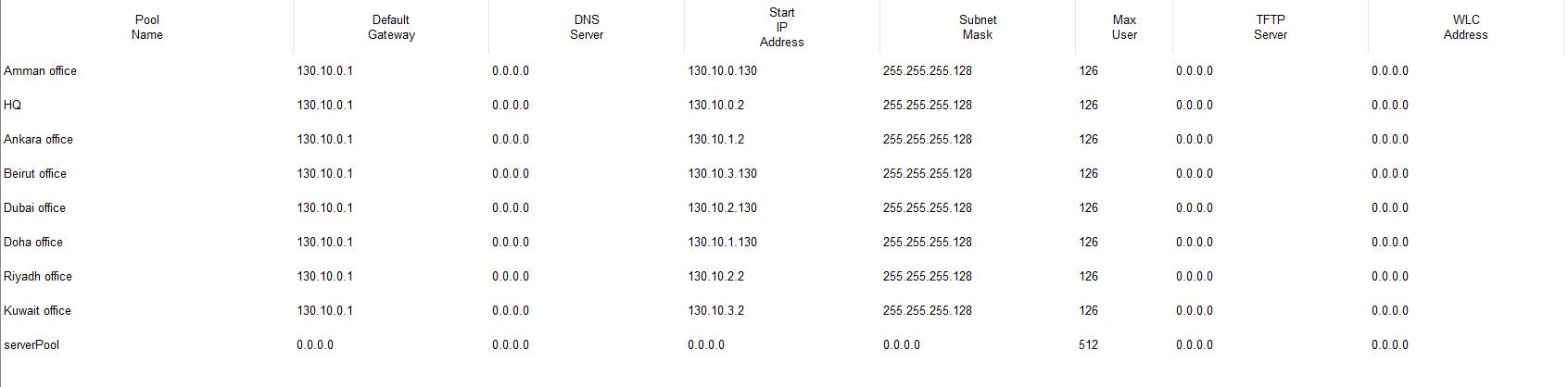
1. Run the service in the server



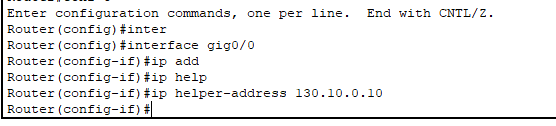
2.Put the asked information for each LAN network in the whole network  
A screenshot of a computer

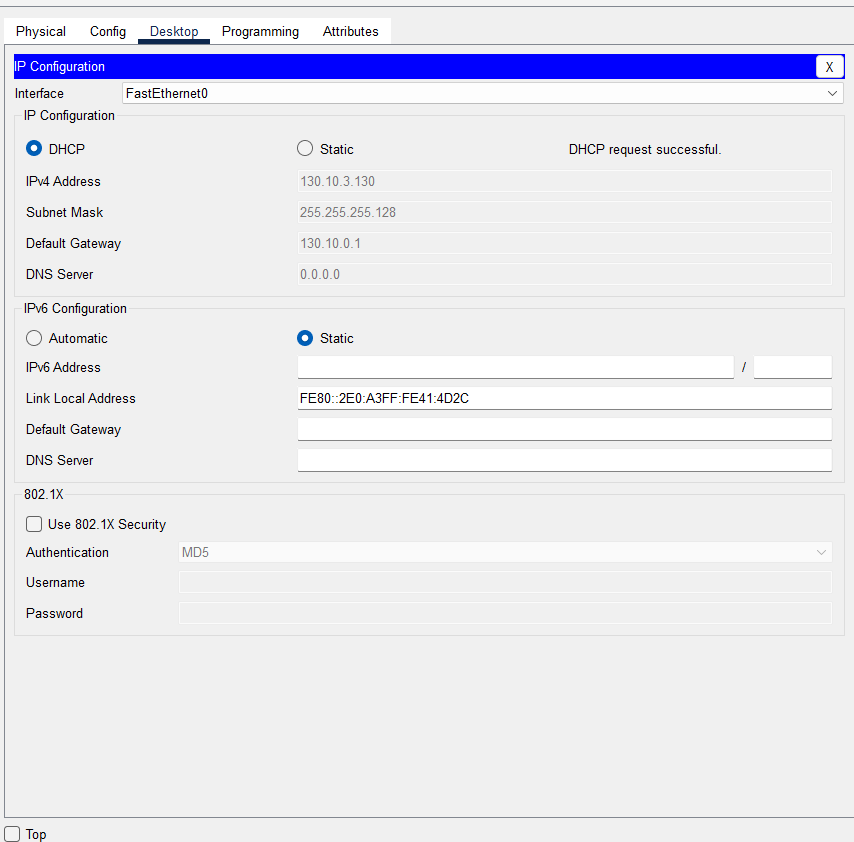
Description automatically generated

3.Make sure that all networks are in the table



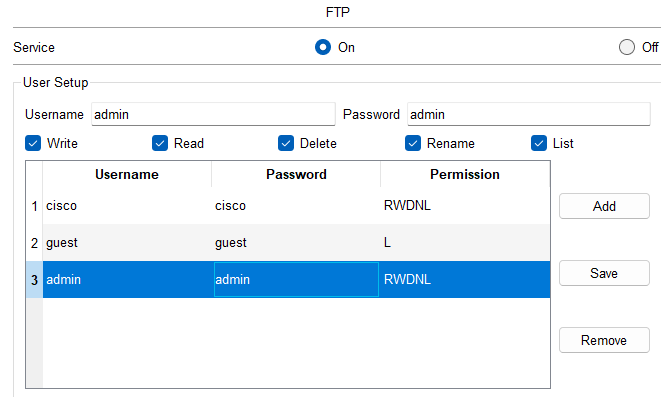
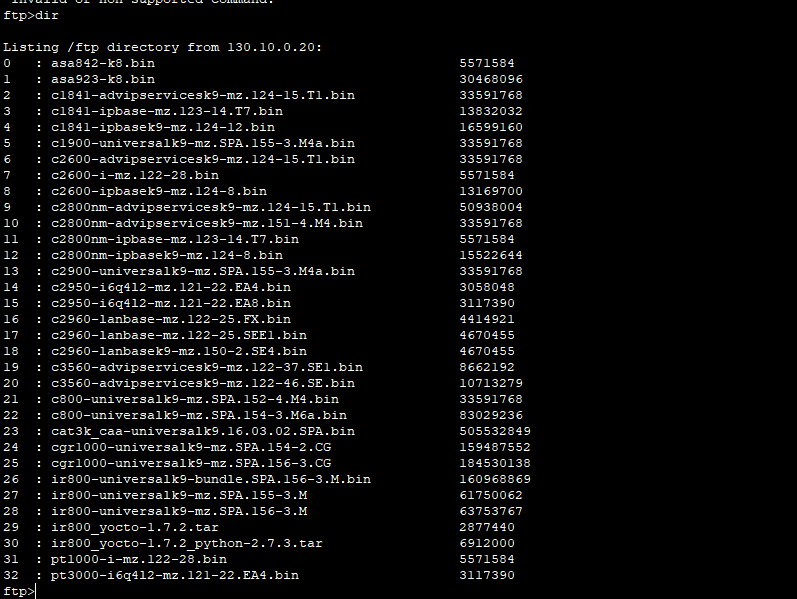
4. To make the routers know where to get IP address from we should put these commands on each router on the network



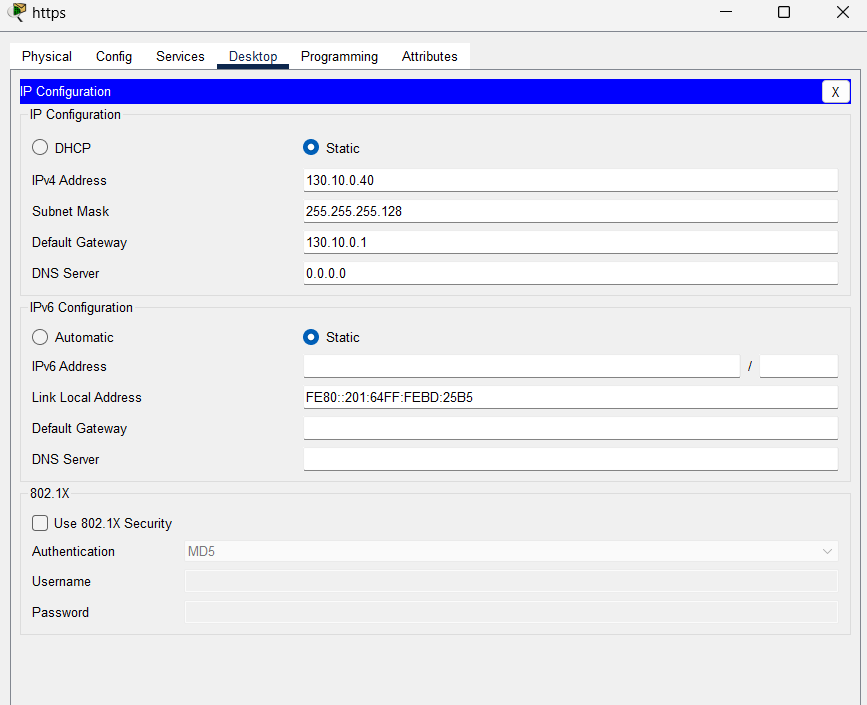
5. Now we should go to each pc and turn on the DHCP option so it can take an IP add res dynamically

## 4.2 FTP

One of the requirements based on the assignment brief is to Have the capability to share and transfer various files (such as reports, images, etc.) across all remote offices, ensuring effective communication and resource sharing and this can be done by using the file transfer protocol, Firstly I will add another server in the HQ and use the FTP service in it , I have added two types of users one is admin and this account will be to any employee in the company and the other is guest which will be for the view only just if anyone want to visit or see the names of files we have

  
And I can access the ftp service using any device and I cannot put any command that align with the permissions   


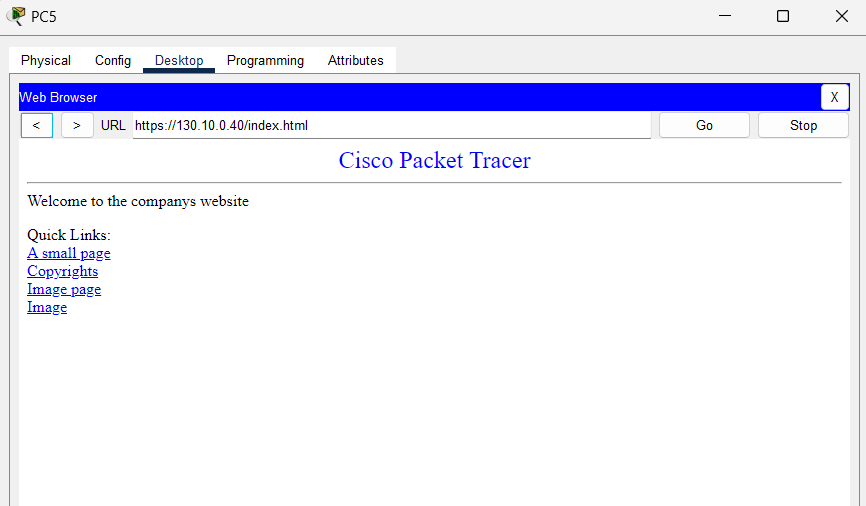
## 4.3 HTTPs

Gain access to the company’s internal system, utilized for sharing project tasks and data, through a secure website (https://eis.DataTech.com.jo/). Access to this system should be facilitated using a FQDN (Fully Qualified Domain Name) and to make that a https server is needed firstly I will give the server and ip address statically and turn on the http service in it   


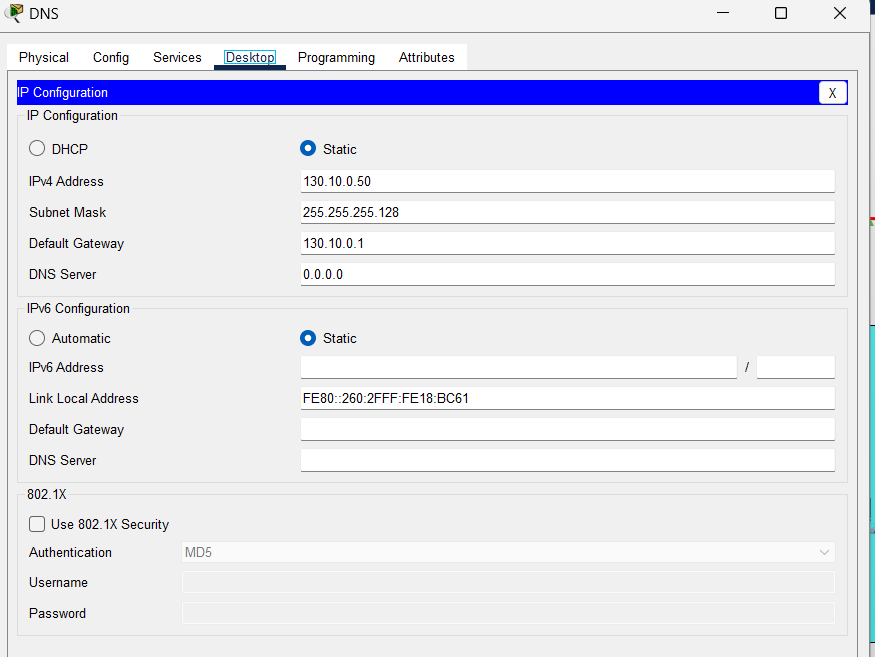
A screenshot of a computer

Description automatically generated

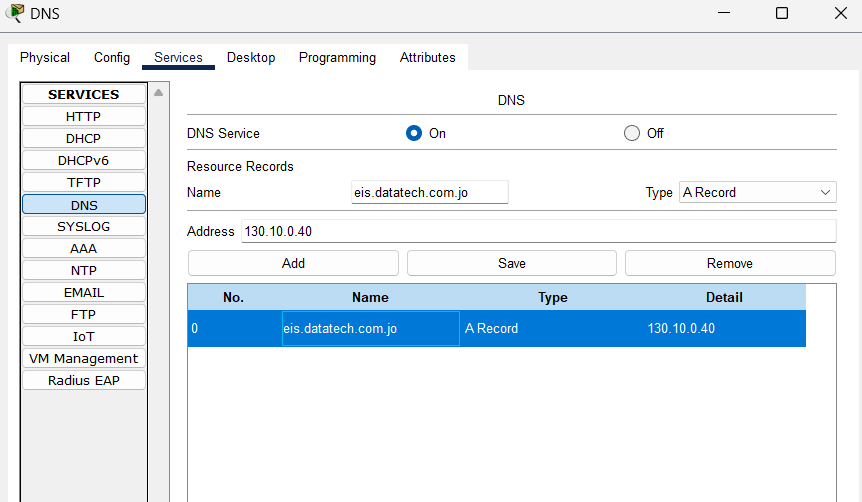
Now the pcs can access the website using the servers ip address.



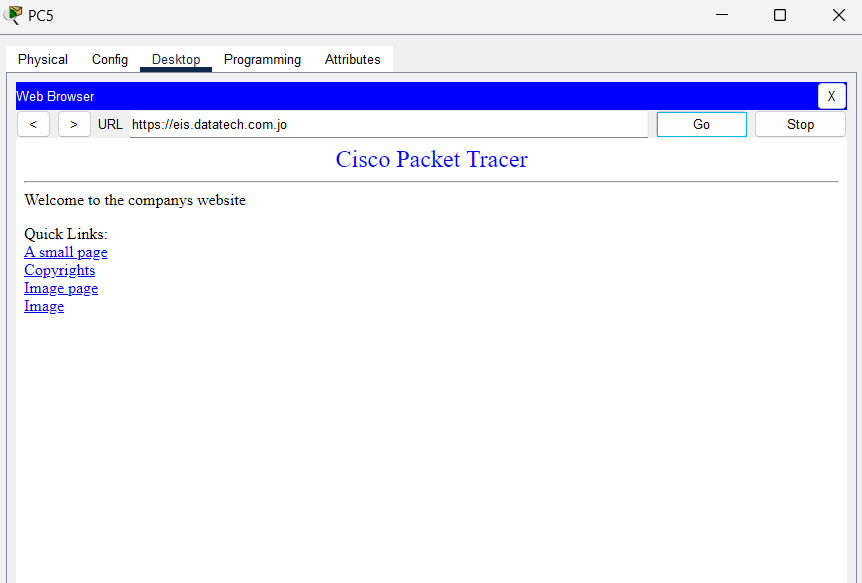
## 4.4 DNS

Now to make the website accessible by the website URL a DNS server should be made as always, I gave an IP address statically and turned it on in the server   


I have added the name of the website and the https servers IP address.

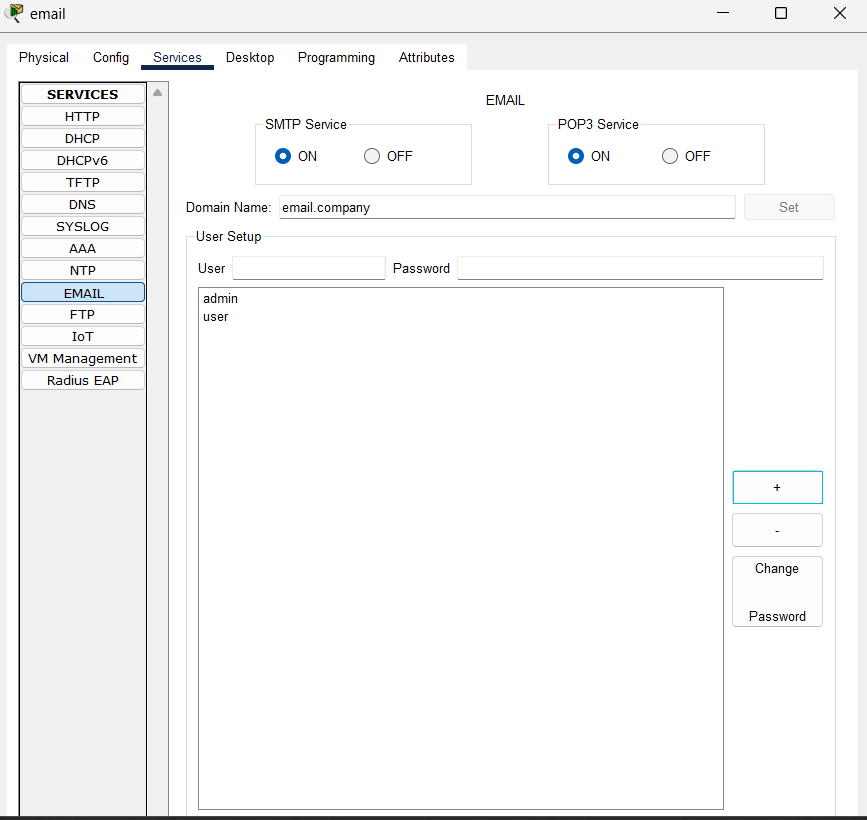


Now I will add the DNS IP address every single server in the network, and I will re give the end devises IP addresses dynamically so they will have the DNS server IP address, now all the devices can use the website name to access it.

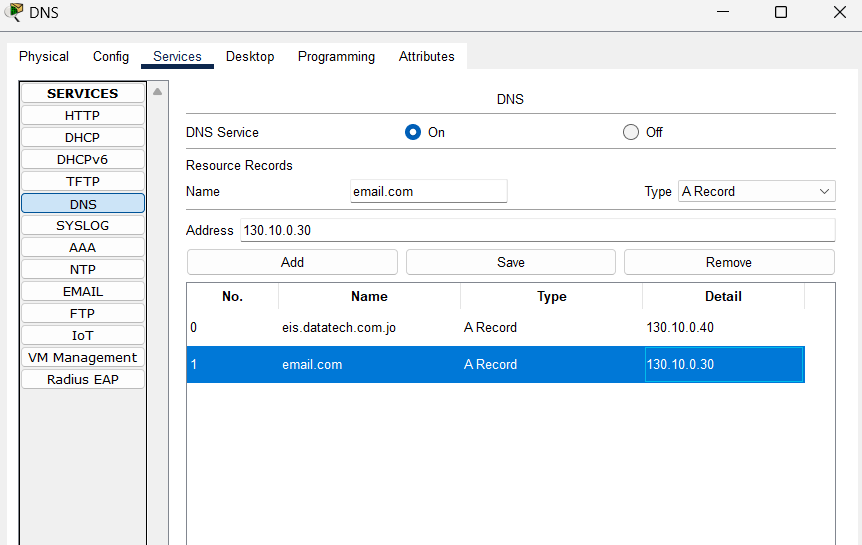


## 4.5 Email

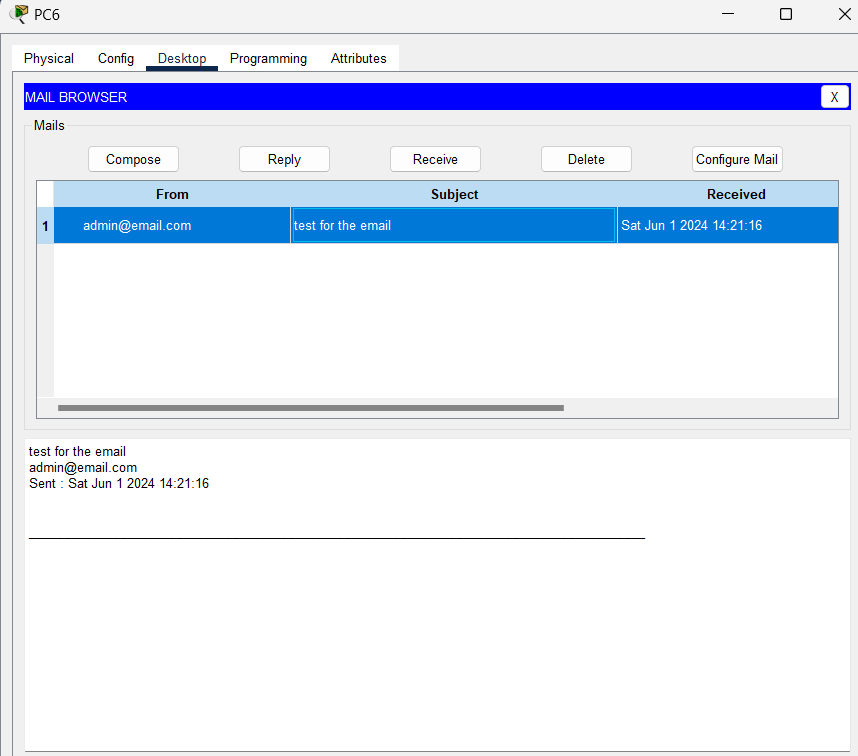
All devices should Be equipped to send and receive emails among each other, fostering prompt and efficient communication based on this a server should have the email service which validate sending and receiving emails between users.



After putting a server for emails, I have added two users as a test and now I will try to send an email. I have added the domain name into the DNS server for easier access.

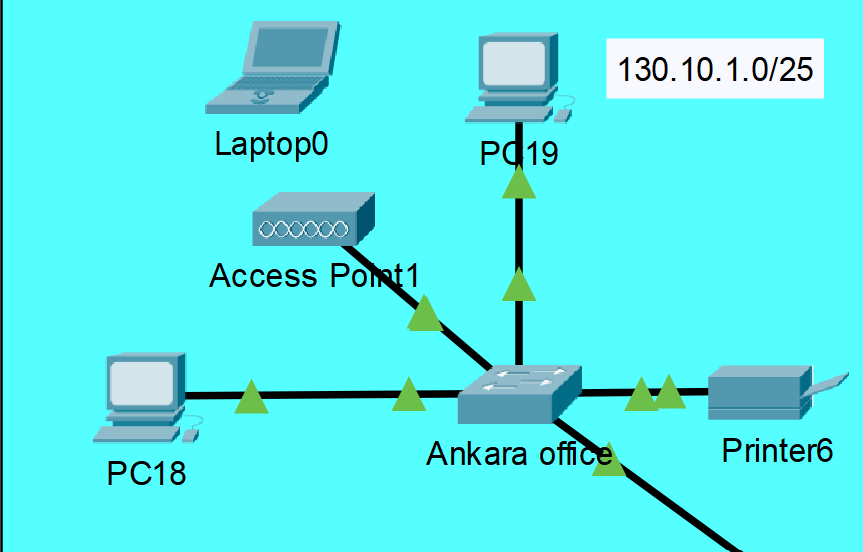


Here are the results:

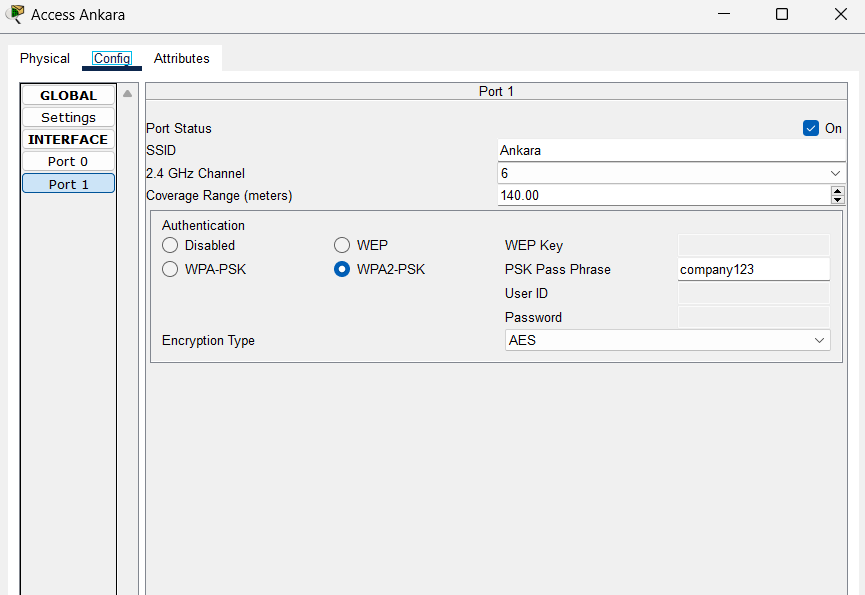


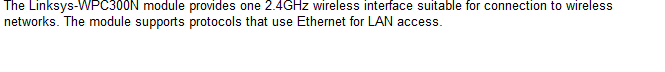
# 5. Adding extra devices

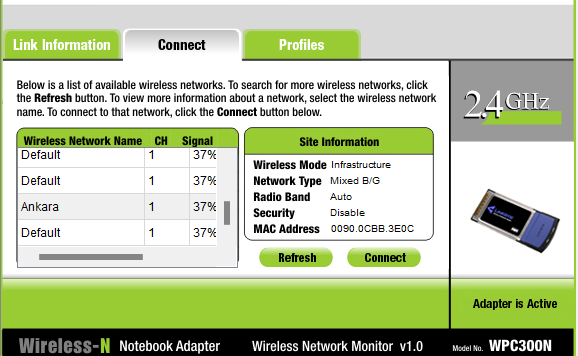
Each DATA-TECH remote office, including Amman Office: Resources: 2 PCs used to access the e-services required using a wired connection, 1 network printer, Wi-Fi access, 1 laptop connected using Wi-Fi access, so now I should add a laptop and a printer with an access point after putting the devices I will give the laptops an ip address dynamically and connect them to the access point

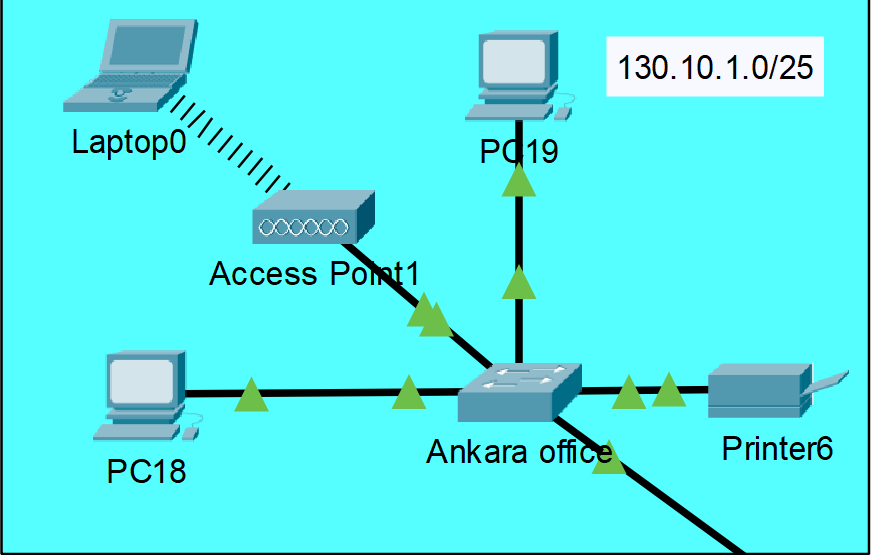
Here is the wiring:  


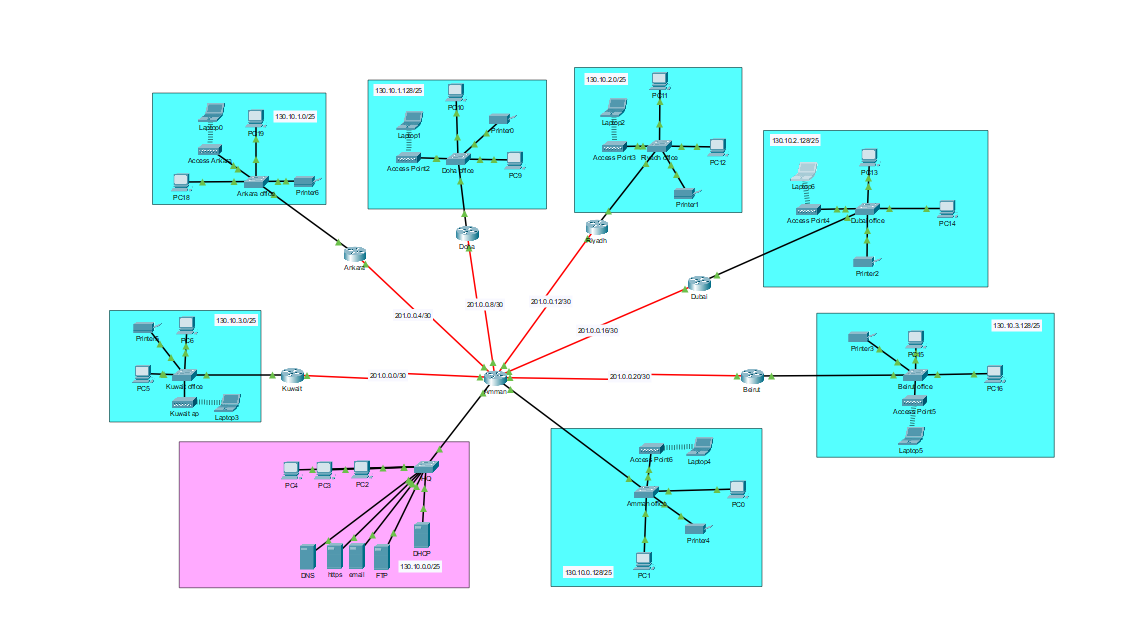
Now I should configure the access point by enabling any authentication method and add a password



Now to connect the laptops with the access point we need and interface   


And we can connect the laptop by using pc wireless and chose the suitable access point   




Same thing for all the LANs  


# 6. Testing

|  |  |  |
| --- | --- | --- |
| What to test | How to test | Expected results |
| Connectivity of each device | The ping command | Replies from the other device |
| DNS | Accessing a website using the web browser by the website’s name /ping devices using their name | Being able to access the website / being able to ping the device |
| EMAIL | Try to send an email to device | The email will be received from the other device |
| HTTPS | Accessing a website using the web browser by its ip address | Being able to access the website |
| FTP | Trying to access or add files | Being able to access them or edit them |
| DHCP | Activate the service in the end devices | Taking right ip address not from APPIPA |
| Firewalls | Scan the company’s devices rapidly | Having safe devices without any viruses or malwares |

Note: all testing results were provided in the configuration of each server

# 7.self-regulation

## 7.1 Topology evaluation

I think that my topology is suitable for the overall asked tasks and features the hub and spoke usage delivered a very good low cost and easy wiring option for such a network since it needed much less cables and time to make the topology is capable of expansion in branches in different countries or more offices in the same country because of the design of the topology it self and the subnetting of available ip address but there are a lot of possible stuff to do if there was more time and budget .

## 7.2 Improvement

Stating from the topology itself it doesn’t provide fault tolerance since all of the routers and connected to the HQ in Amman so if the HQ router goes down or get attacked the whole company will lose the ability of connecting to any other device in other countries so if the company has more budget and time a full mesh topology would deliver a much better network from all perspectives ,now moving to the network security and the lack of filtering of any sent or received data , firewalls should be implemented in the network routers to provide more security and lets not forget how about having all the servers and data in HQ without having cloud backups or backups on other offices or places , and the devices in general don’t have any passwords which can lead to easy sniffing and leak of data

or any unauthorized access to the network’s devices.

# 8. Maintenance Schedule

Now to improve the company’s network and limit and threats in addition to maintaining the stability and preventing any malfunctions or discrepancies from occurring we must set and establish a maintenance schedule for our network, and to do we must consider all the possible shortages. network breaches, and or any complications that may affect the network’s functionality.

|  |  |  |
| --- | --- | --- |
| Task | Description | Frequency |
| Overall network performance | Check if network is functioning properly with no critical alerts and issues. | Daily |
| Hardware Health | Check server components and hardware health | Weekly |
| Server Rooms | Check for cooling and optimal server room conditions | Weekly |
| Disaster Recovery Check | Evaluate the disaster recovery plan and update based on newly found changes | Monthly |
| Contingency Measures | Develop and assess any contingency measures developed to counter discrepancies | Monthly |
| Software Updates | Update all network software with latest versions and patches. | Weekly |
| Update Anti-Virus | Keep anti-virus up to date | Weekly |
| Data Backups | Keep checking for a backup for the data (cloud and hardware backups) in case of any disasters | Daily |

# 9. Scalability Plan

A scalability plan is created to accommodate future and potential growth of the network in terms of size, numbers of users, and number of local areas. All of which need to be accounted for and considered to upgrade the physical and software aspects of the network components. Such as investing in laptops in devices with high capacity and throughput to handle high traffic loads, in addition to increasing the server storage to handle more allocated information, also strategically adding access points would be effective to increase the reach of networked devices, all of these changes can be used to scale a network.

# 10. Logical Topology

Now to discuss the logical topologies utilized in the work and how it was integrated in the network and affected its efficiency which reveals distinct strengths and weaknesses in their logical topologies. Ethernet's logical star topology reduces collisions and is easily scalable, but its central point of failure and higher cabling costs are drawbacks. Wireless networks benefit from a mesh topology's reliability and scalability, though they face complexity and higher costs. Token Ring networks offer collision-free, predictable performance through a logical ring topology, but are slower and less scalable, with single points of failure. IP networks excel with a mesh topology, providing high redundancy and scalability at the expense of increased complexity and management costs. Each topology's suitability depends on specific network needs such as scalability, fault tolerance, cost, and complexity, in our network we integrated the hub and spoke topology by using a specific router compatible with connecting with multiple network interfaces and process of which the routers were connected to the main headquarters router were through connecting each and every individual server to the headquarters server directly without using any neighboring topologies and such.

# 11. Interdependencies

The interdependence that happens between network hardware such as PCs, switches, routers, and servers and the networking software is vital for efficient data communication between the two entities. Clients use network interface cards and operating systems to initiate packet requests, which are sent to switches where encapsulation adds data link layer headers. Switches use certain protocols and functions to manage MAC addresses through MAC sublayer and then forward the packets within the local network. Routers, with their routing software, handle network layer addressing which is level 3 and forward packets between different networks. Servers, equipped with more network interface cards and server operating systems, process these packets, and respond accordingly. As for Firewalls, they happen to inspect and filter packets based on security rules and regulations set and that happens before they reach their destination. Throughout this journey, encapsulation adds headers/trailers at each layer, while decapsulation at each receiving device removes them, ensuring data integrity and security across the network and maintaining compatibility with the data signaling and encoding with the medium’s suitable protocols.