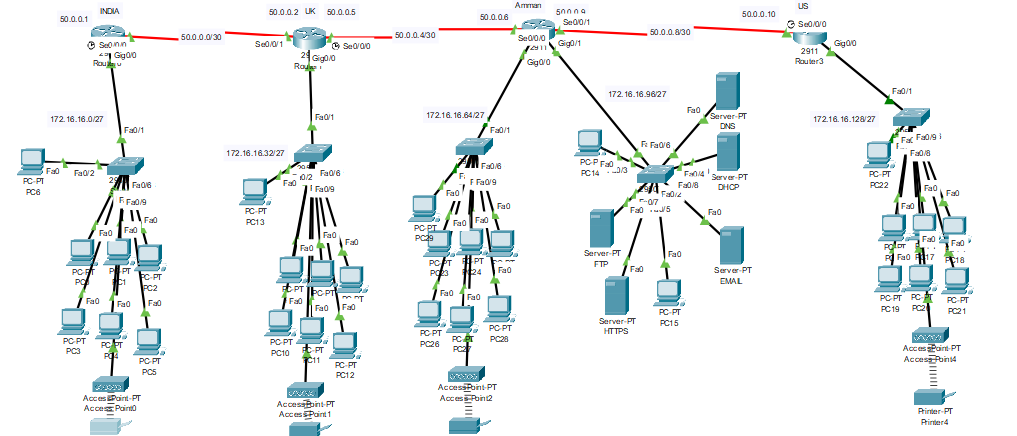
\***the design:**

This is the design that I chose to use:



To design the network I started with four routers, I connected them with serial cables, then on each router I connected a switch using the straight through cable, then on every switch except the HQs switch I connected 7 end devices using the straight through cable and I connected an Access point that I used to connect the printers to, in the HQs switch I connected two pc’s and all of the servers.

\***Network configuration:**

For this network I used 6 types of devices such as: router, server, switch, pc, printer, access point.

\***subnetting:**

To start the subnetting process I had to ask myself some questions such as:

1. how many subnets do I need? And I needed ta least 5 subnets

so I used the rule 2^y (y = the number of bits that you leave from the end for the host part in the mask) so 2^y = 5, if (y)= 2 the number of subnets would be 4 and that is not what we need so (y)has to be 3 to give us more than 5, so the number of subnets that we can make are(8)subnets.

2.how many valid hosts per subnet I need?

And I need to have 7 valid hosts and the network must be able to expand to have 22 more employee per office so the valid host number is 22+7 = 29 so the valid host number has to be ~ 29 host per subnet, so I have to the rule (2^n – 2) (n is the number of the remaining bites of the last part of the mask ) and (n)= 5 so the valid number of hosts is 30 and that is what we need.

So the new mask is:255.255.255.11100000 🡪 255.255.255.224

So this would make the IP add that we are going to use: old:172.16.16.0/24

The new one:172.16.16.0/27

8N.8N.8N.3N5H (H is for host, N is for network)

So following this we have to know the block size of the subnets and for that we have to use the rule (2^n) so 2^5 = 32 so every subnet has 32 hosts.

The IP add that we have to use to make subnets is 172.16.16.0/24

So the subnets that we need are;

172.16.16.0/27

172.16.16.32/27

172.16.16.64/27

172.16.16.96/27

172.16.16.128/27

\*172.16.16.0/27

First valid: 172.16.16.1/27

Last valid: 172.16.16.30/27

Broadcast:172.16.16.31/27

\*172.16.16.32/27

First valid: 172.16.16.33/27

Last valid: 172.16.16.62/27

Broadcast: 172.16.16.63/27

\*172.16.16.64/27

First valid:172.16.16.65/27

Last valid: 172.16.16.94/27

Broadcast: 172.16.16.95/27

\*172.16.16.96/27

First valid: 172.16.16.98/27

Last valid: 172.16.16.126/27

Broadcast: 172.16.16.127/27

\*172.16.16.128/27

First valid: 172.16.16.129/27

Last valid: 172.16.16.158/27

Broadcast: 172.16.16.159/27

Then I had to make subnets for the networks between the routers using the IP:50.0.0.0

And the networks between the routers uses /30 so knowing that I started subnetting.

50.0.0.0/30

255.255.255.11111100

So, using the rule (2^n – 2) the valid hosts I made the subnets.

\*50.0.0.0/30

First valid: 50.0.0.1/30

Second valid: 50.0.0.2/30

\*50.0.0.4/30

First valid: 50.0.0.5/30

Second valid: 50.0.0.6/30

\*50.0.0.8/30

First valid: 50.0.0.9/30

Second valid: 50.0.0.10/30

**\*building the network:**

After I new the subnets that I need I started to build the network

Firstly I started with 4 routers and I connected them with the serial cables, but in order to do that I had to turn off the routers and change the original module with the serial one and then turn on the router and I did that for all the routers, then I connected them.



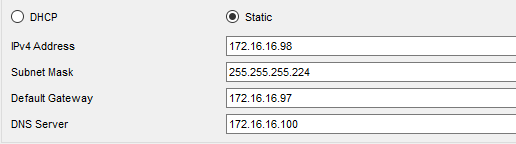
After that on every router I connected a switch except for the Amman router I connected two and I used the straight through cable to do that. Then I connected the 7 PC devices to every switch using the straight through cable except for the HQ Amman office I only connected two of them.

Then I started to configure the OSPF protocol on the routers and to do that I had to open each router, go to the config interface, write router ospf + a random number, then I have to type all the networks that are directly connected to the routers followed by the wild card which is going to be 0.0.0.3 for the normal networks and 0.0.0.31 for the networks between the routers and the n the area number that is 0, and then you have to use the passive interface then the ip add for the networks that does not have another router connected to it.

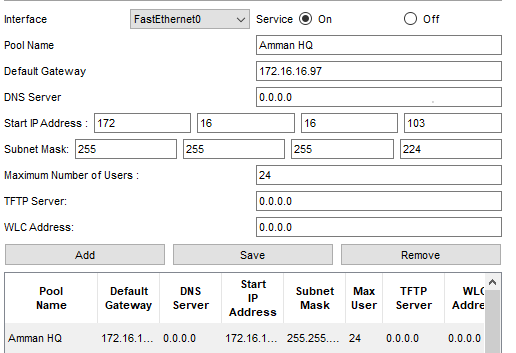


After I do that for all the routers, I started with the DHCP.

First you have to get a server, wire it to Amman’s HQ switch with the straight through cable and then give it an IP address and default gate way,



then you have enter the services tap in the server, turn on the DHCP, give the DHCP the name, default gate way, the start IP address that usually the 6th IP add in the subnet, the subnet mask, the number of users to all the subnets and add them, after that you have to go to each router and go to the config interface and type (rely agent + IP add for the DHCP server) for all the routers, after that you have to change all the IP configuration for the devices to DHCP.



Then I started to make the website for the network.

First I used another server and connected the server to the HQ switch, then I had to give the server the IP add and the default gate way, then you have to go to the services tap, then the http tap and turn off the http and leave the https on.



After that the website is going to be on but you have to go to one of the devices, open the website tap, then you have to type <https://then> the IP add of the http server, but to put the website name instead of the IP add of the http you have to put a DNS server.

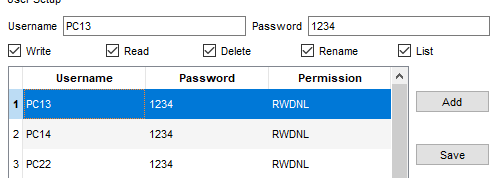


First you have to get a server, connect it the HQ switch then in the server open the services tap, then the DNS tap and put it on, after that you have to put the IP add of the http server and the name of the website that is in this case going to be (projects.jgames.com.jo/).



After that I had to put a service that gives the devices the ability to transfer files between them and for that you have to setup the FTP server.

First you have to get a server, connect it to the HQ switch, open the server on the FTP tap then add the users name and a password for them then give them all the abilities,



after that I add all the users. To use it you have to go to the command prompt in the user device write (ftp + the IP add of the ftp server), then press enter , write the user, the password and then if I need to upload something to the server I write (put) and to download files write (get).

Then I had to configure the email for the network and to do that you first have to get a server, connect it to the switch then give it a static configuration. Then you have to go to the services tap, email tap, then I give the server the email and press set,



then I had to go to the DNS server to set the email and the IP add of the email server,



after that in the email server I have to put all the usernames and the passwords for the devices. Then in each device I go to the email interface and in the user info I type the username and the full email, then in the server info I gave it the IP add of the email server, after that in the logon info I typed the username and the password.

\*how to connect the printer wirelessly: <https://youtu.be/PglzwLp1X34>

\*IP addresses for the servers:

The DHCP: 172.16.16.98/27

The HTTPS: 172.16.16.99/27

The DNS: 172.16.16.100/27

The FTP: 172.16.16.101/27

The EMAIL: 172.16.16.102/27

\***The services:**

DNS: it is used to locate resources on the network, it links the IP address to the uniform resource locator (URL), as used to connect the https website with the IP address of the server that provides the service.

FTP: it is used so the clients can upload and download files on and from the server, you can give the users the ability to upload, download, delete, rename and move files on the server, this service is used in this network to give the clients the ability to upload and to download files on the sever.

SMTP and POP3: SMTP is a set of rules that regulates the travel of email, it is only used to deliver the email, POP3 is responsible for receiving the emails, as soon as you open the emails POP3 downloads them and after that deletes them, this service was used in this network so clients can transfers emails between each other.

HTTP: it is an application protocol used for distributing, collaborative, and hypermedia information system, http is a pull protocol so the clients pull information form the server, http is a request-response protocol, I used this protocol to provide the web service for the network.

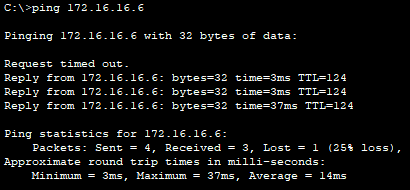
OSPF: it gives the routers the IP addresses of the networks he is not directly connected to.

DHCP: is dynamically assigns IP addresses to the client devices so they can communicate to each other, I used the DHCP to make it easier for me to give the clients the IP addresses.

**\*Testing the network:**

To fully test the network, I had to test the routers, the services, and the protocols.

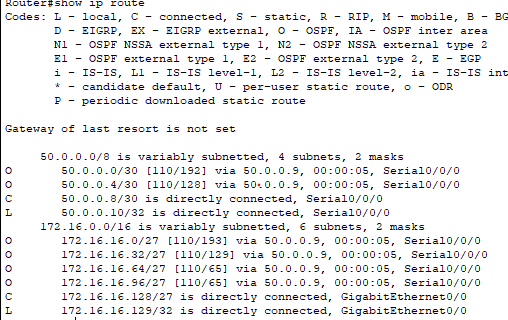
\*The end devices: you have to check it they have the correct ip add and if they can see each other using the ping command.



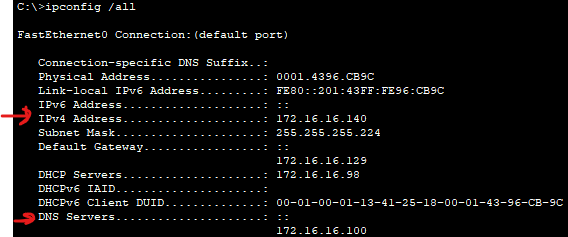
\*The routers: I had to check if the routers knows the networks that he is directly connected to using (show startup config) or by using the ping command.



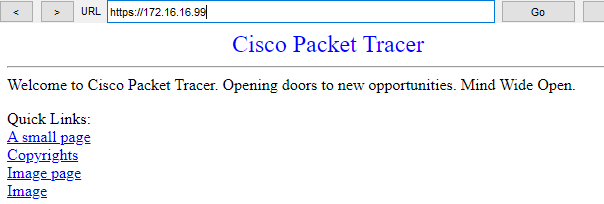
\*The OSPS: to check if the was configured correctly you have to use the (show ip route) command, that shows me all the networks connected to the router and the ones that has an O next to them are the ones that the is not connected directly, but got them from the osps protocol.



\*The DHCP: to test this you have to go to the end devices and in the command prompt type (ip config /all) this will show you the IP add of the device and the IP add of the DHCP server.



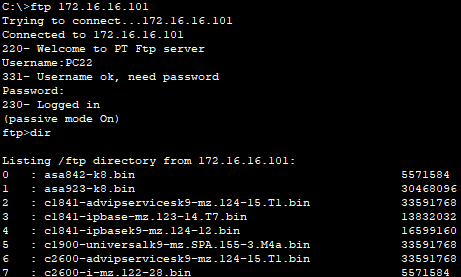
\* The HTTP: to test it you have to go to the end devices and in the HTTP tap type (http:// + the ip add of the http server).



\*The DNS: to test it you have to use the http service but with the name that you gave to the web.



\*The FTP: to test it you have to go to the devices and in the command prompt type ftp + ip add of the server, then enter the user name and password, then you have to upload and download files in the server.



\* The EMAIL: to check it in the end devices you have to go to the email tap, type the email of any of the end device and send them something, and in the receiver device see if the email would show up.





\* The expected results were that everything should work correctly and the tests had matched the expectations.

\***The maintenance schedule:**

Network maintenance is very important to keep the network running and to keep it secure, and to do that you have to upgrade the software and hardware, monitor the network, check the security of the network and to download backup files.

You have to monitor the network everyday to detect any potential problems that might occur, also checking the security of the network has to be done daily because of its importance, downloading the backup files has to be done weekly and software and hardware upgrades has to be done monthly, of course these operations has to be done with out interfering with the times that the network works in and with out interfering with its functions.

<https://ecmanagedit.com/what-network-maintenance/>

\***Potential enhancement:**

There are a lot of devices that can enhance this network such as:

Load balancer: if we had a server that is used a lot during the peak hours of the day, so it keeps failing for the amount of users using it you can install a new sever with the same service and connect them to a load balancer; the load balancer distributes the load on the two of them so that they operate without shutting down.

Proxy: if there is a service that a client needs but in the service is not provided in the network a proxy can scout the internet for a server that provides the service then the proxy send the service a request, then the proxy gets the service and sends it to the client.

Content filtering: is manages the client’s accessibility to the emails, websites. Its goal is to block websites that can distract the clients or to block websites that is dangerous.

Content filtering: <https://www.fortinet.com/resources/cyberglossary/content-filtering#:~:text=Content%20filtering%20is%20a%20process,used%20by%20home%20computer%20users>.

Also the IP subnetting in this network allows it to expand so you can have 8 total subnets and 30 valid IP addresses in each one.

\***Security requirements:**

First there has to be a password to enable the routers so that not everyone can access the routers information.

Fire wall: the fire wall is a network security system that can be either hardware or software, it protects the network from the external internet, the barrier is form according to a set of security rules.

DMZ: if the organization that hast his network wants people that are from the internet to access their servers the severs has to go out of the fire wall protection because if the servers are in the private network you are giving unknown users permission to enter you private network, for that the severs has to go out side the fire wall but to add more protection the organization can install a new fie wall that protects the servers.

VPN: a vpn can extend the private network benefits to a user in a public network as if he was directly connected to the private network.

\***critical evaluation:**

The network that I designed and implemented was very good, all the functions that were working correctly.

I think there are two thing that I didn’t like in my network such as: first, the in the implementation the network wasn’t tidy because I used a small space of the packet tracer work space the devices were very close to each other and it made it hard to read some of the text that has important information.

The other thing is that I used separate servers for each service, this can be beneficial in larger network but in this network there was no need for it, I used a separate server for each service in this network because it is easier for me to maneuver between them.