**Abdullah istanbuli**

**(21110366)**

Part 1

1.network types

WAN: WAN is short for wild area network it’s commonly used to access remote offices or to allow access to data bases or servers that are far away like another cities and countries, it offer fast communication for far areas but it has high cost to setup and low security and its commonly used to connect multiple LAN.

CAN: campus area network is used to connect multiple LANs together in smeller areas, like university campus or business parks or military bases or large schools, it improves communication in different buildings or departments inside a small area to offer low access which increases security and the cost isn’t high.

LAN: local area network it used in small areas like floors or houses, its commonly used to connect inside devices with each other’s or to give access to multiple devices to the internet, it as a low cost to setup and high security because it has limited access.

PAN: personal area network its not common since LANs has a low cost, it used to connect personal devices together like laptop smart phone TVs pods and smart watches, it has low to none cost and very high security since it has 1 or 2 user access.

2.physical network topologies

There are many different topologies some of them are, bus: all devices are connected in single line, tree: all devices are connected to single device in the middle can be hub switch or router with multiple levels of devices (used in formative), ring: the devices are connected in a loop with one direction of data transmitted, mesh: each device is connected to all devices making multiple paths to data transmitted and lastly hybrids: when multiple topologies are used in one network.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | scalability | performance | reliability | cost | maintenance |
| Bus | Limited due to possible data collisions | The larger the network the slower the speed | More likely to failures due to single line of communication | Low due to the simplicity of the network | Easy due to simplicity of the network |
| star | High and easy to add new devices | Good due to centralized control | Highly due to centralized control | Moderate cost due to the need of central device | Easy to maintain due to centralized control |

In the project I would use hybrid network between star mash and tree network in the middle I would make it hybrid between mash and star to offer limited access increase security and low possibility of network failure since the network for banking system and its important to stay online 24/7, and I would make the rest of the network tree to limit the users access due to high privacy clints in a banking system.

3.

1. wi-fi: WIFI provide a wireless connectivity and gives the LAN more flexibility for device placement and eliminates the need for physical cable however the performance can be affected by interferences the signal might become an issue in terms of range and higher risk of congestion to ensure efficiency you most provide proper signal optimization and security measures.

2. Ethernet: ethernet provide high speed reliability it provides low latency making it suitable for demanding applications its commonly used in data canters and LANs to achieve efficient resource usage.

3. point to point (PPP): is a reliable and efficient protocol for PP convictions its provide authentication encryption and error detection PPP is often used to access remote networks while it’s the best choice for point to point connections it might not be the better protocol for large networks

4.

1.HTTPS: this protocol is used for internet browsing securely to have a fully functioning secure connection between the server and the browser with encryption.

2.DHCP: this protocol is used to manage the ip addressing automatically instead of manually to save the time for people to give each device a new ip address.

3.FTP: if you need to update and edit or remove or add content from or to a website you need to use FTP protocol to host the website and insure file transfer effetely

4.DNS: DNS protocol works similar to the way translator do as an alternative to write and memorize the ip addresses of every device and website this protocol let the user access them by writing the name assigned to them.

5.SMTP & POP3: if a user wants to send an email to a an email address ([exp@outlock.com](mailto:exp@outlock.com)) the user email clint uses SMTP to send the email from his device to the email server on the other side POP3 is used by the exp email clint to retrieve the email from the server, the two protocols enable the exchange of email messages across mal servers and clints.

5.

1.switch: the switch operates on layer 2 in the OSI model it connects multiple devices on a LAN and uses MAC address to identify the devices.

2.router: routers operate on layer 3 they connect multiple networks together it uses IP addressing to identify the shortest path to transmit data by using protocols like OSPF or RIP or others.

3.hub: it works on layer 1 it works similar to a switch however its not as intelligent as switch since Broadcast the data to find the right receiver.

4.priter: it operates on layer 7 and 2 it allows access to PCs on the network and they have IP address like other end devices.

5.repeter: it works on layer 1 it works to expand the network signal to farther away devices or to

Make the signal stronger.

6.

1.Data base server: it’s important to have data base server in banking service to store all clint

Personal information and clint balances and loans information’s and more important information.

2.Application server: as mentioned the bank need Esystem to run online banking system that task

Will need an application server to run it.

3. Web server: the bank needs an online server to run an https for the secure internal system

4.File sharing server: the bank employee should be able to share files reports, images and important details

5.mail server: as required we need a server to run an email server to transfer email that can run SMTP and POP3 service.

7. the inter-dependance between hardware devices and networks software is crucial for a functioning network lets divide the packet trip into steps

Step 1 the software sends the packet to the network chip in the pc, then the chip to its part into sending the packet to the network interface that the pc connected to with the gateway ip address.

Step 2 the packet goes into the LAN usually to a HUB or switch in case of the hub it will sent the packet broadcasting through the network into finding the gateway, in case of a switch it looks at the destination MAC address then determine the port that the packet will go through and the software within the switch forward the packet on that information and its responsible to ensure proper MAC address learning.

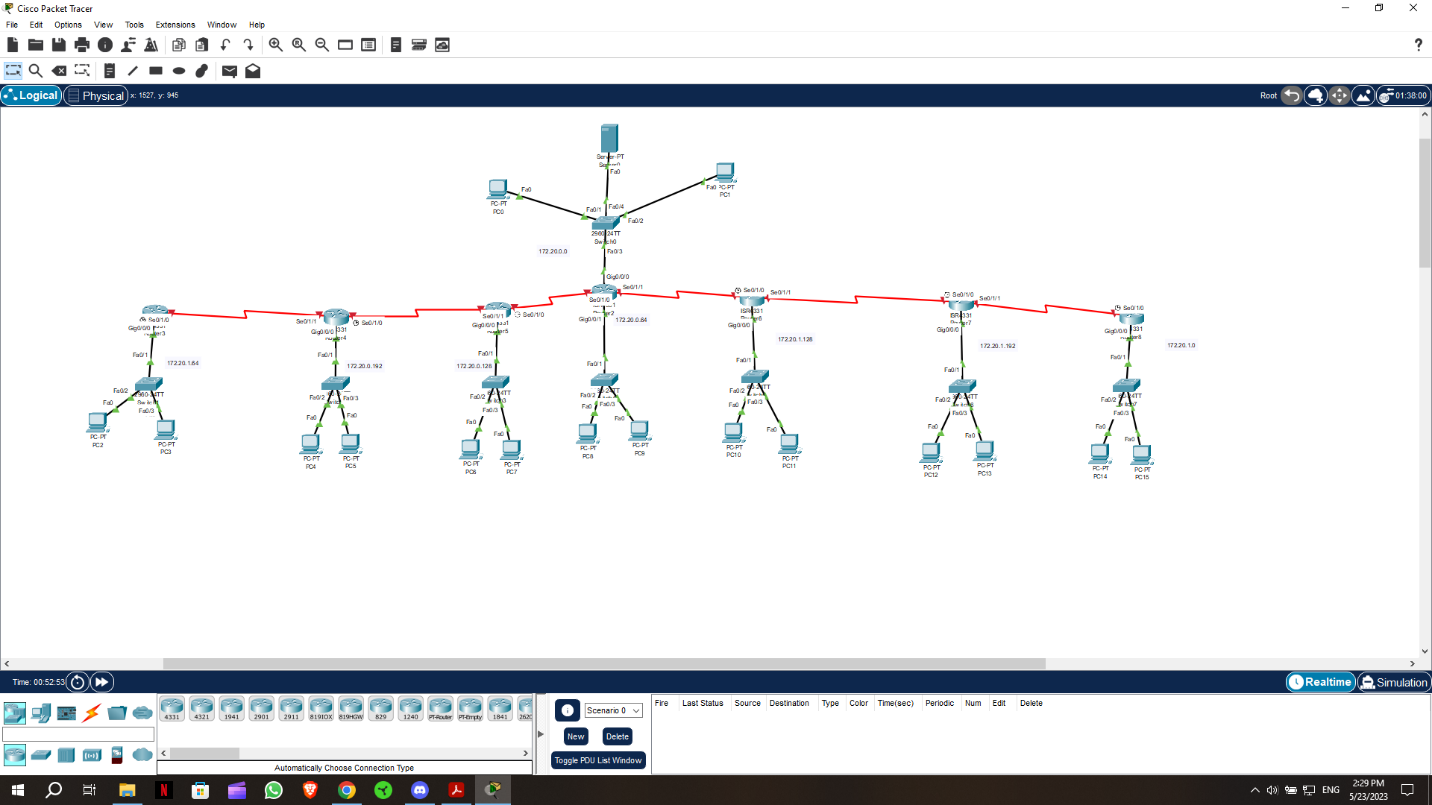
Step 3 if the packet needs to travel outside the LAN, it reaches the router the networks software within the router handles the task of routing table management after filling the information by using OSPF or rip protocols the router knows which route leads to the destination ip address

Step 4 the packet reach the destination network after going thro the WAN similar to previous router the software analyzes the packets destination ip address check the routing table and determent the next device or interface then the router’s hardware handle the packet forwarding process.

Step 5 destination device finally the packet arrives to the destination device the network software receives the packet then proforma tasks such as error checking decapsulation and sending the packet into the appropriate app

Throughout the packet trip the celebration and the dependance between hardware and software is clear and necessary to ensure the network proper job

Part 2



In every LAN except the administrator and server LAN has the same config all the LANs have 2 pcs 1 laptop and 1 printer as end devices pcs and laptops have dynamic (DHSP) ip address all routers have the LAN network connected to them by gig0/0/0 and they all have first available ip and the printer have the second available ip the subnetting goes as follows:

172.20.0.0/16

172.20.N.NNhh hhhh

sm 255.255.255.192/26

s0 id 172.20.0.0-172.20.0.63 as broadcast

s1 id 172.20.0.64-172.20.0.127 as broadcast

s2 id 172.20.0.128-172.20.0.191 as broadcast

s3 id 172.20.0.192-172.20.0.255 as broadcast

s4 id 172.20.1.0-172.20.1.63 as broadcast

s5 id 172.20.1.64-172.20.1.127 as broadcast

s6 id 172.20.1.128-172.20.1.191 as broadcast

s7 id 172.20.1.192-172.20.1.255 as broadcast

for the networks between routers, we need 2 valid ip address with 1 network id and 1 broadcast which is 4 ips per network the submitting goes:

100.0.0.0/30

100.0.0.4

100.0.0.8

100.0.0.12

100.0.0.16

100.0.0.20

100.0.0.24

100.0.0.28

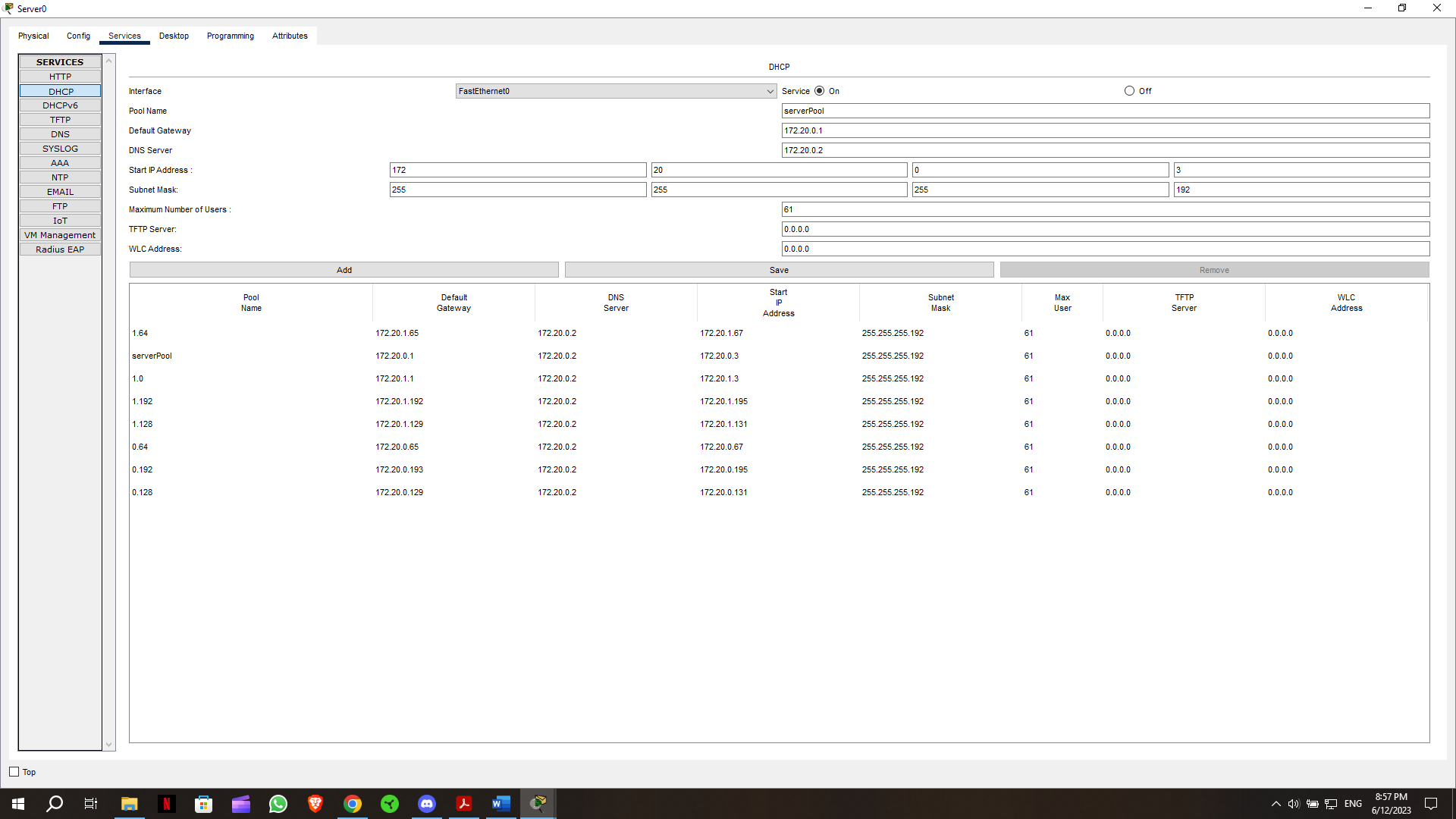
As I separated Amman and admins network with different routers, I needed more subnets

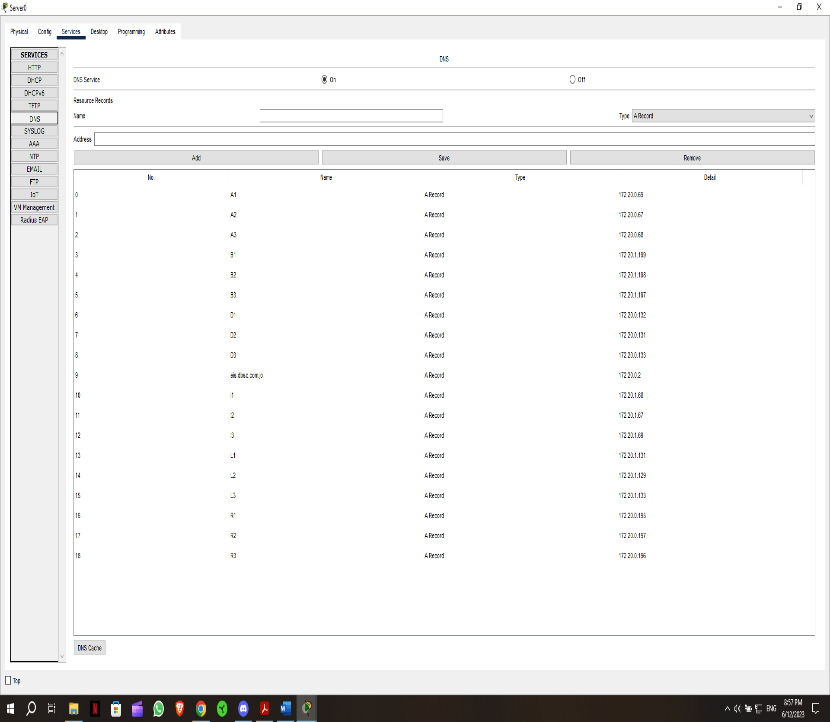
I didn’t config a password for routes I assumed a bank would like it if I didn’t know what passwords they using

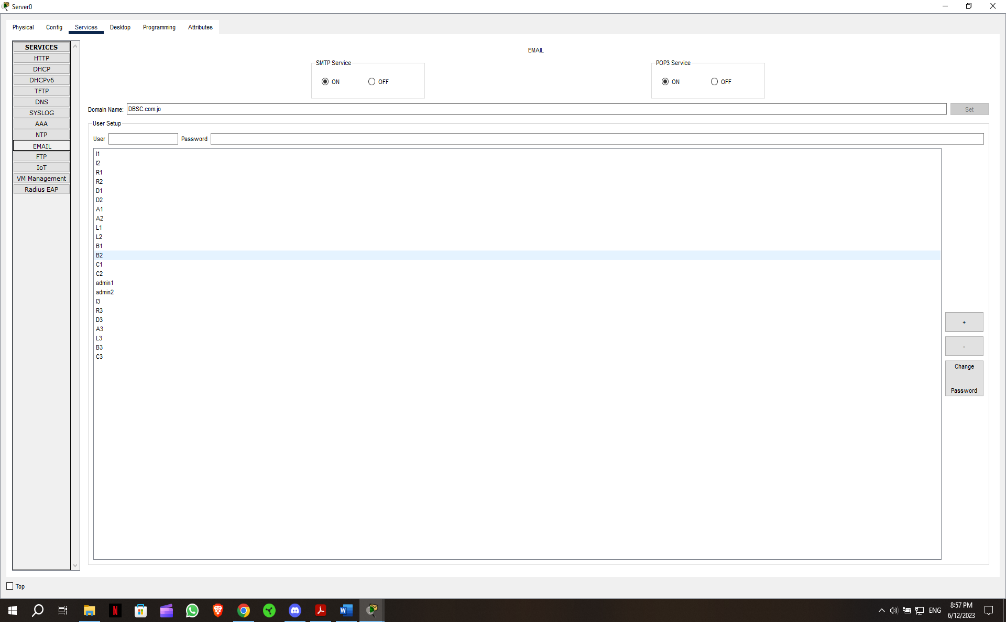
I used ospf protocol to connect the routers together

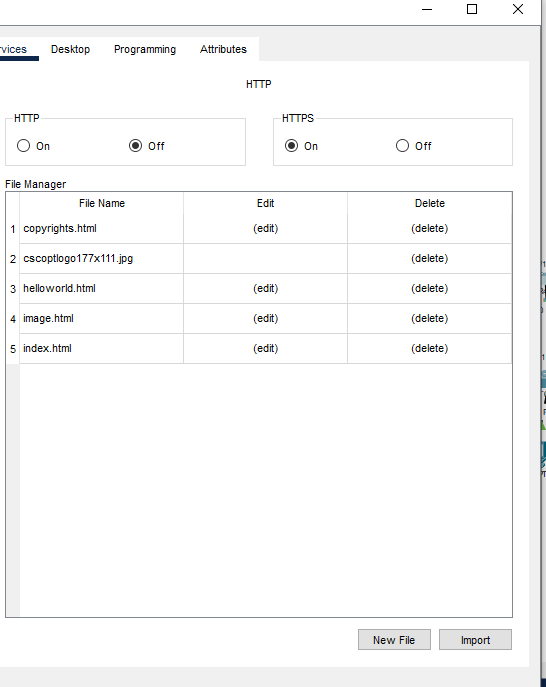
c. I used 1 server for financial reasons because of that there is only one ip address for all services I am including screen shots for all configs

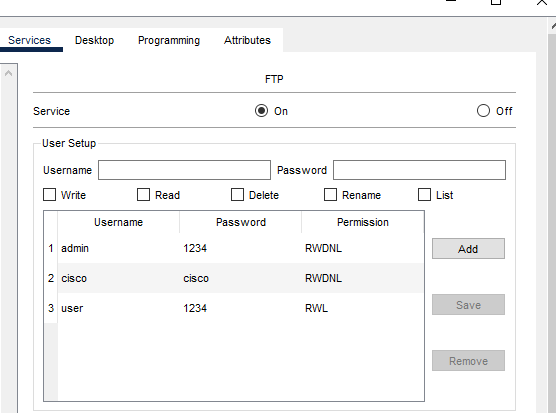
DHCP:



DNS:

email:

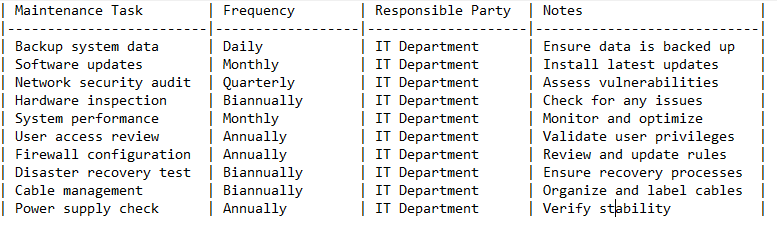
HTTPS



FTP  
All services are made based on the business requirement except DNS which is also required to make full functional website.

2. testing:

The best command to test any network is the ping command if all the work is done you test the farthest 2 divices by pinging on to the other if its successful then then all the connections are running as they should if its not the tester should keep making smaller test until he finds the problem example test 2 pcs from the same LAN then 2 from the other LAN then test the OSPF by pinging the routers with each other etc...

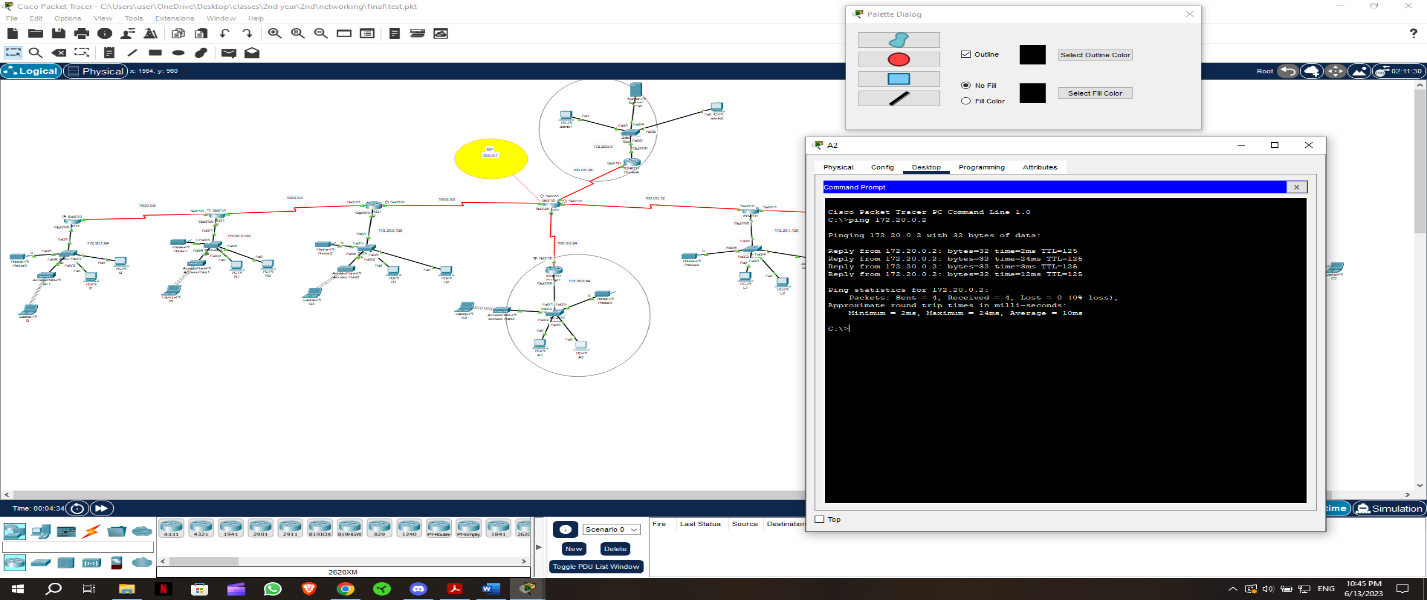
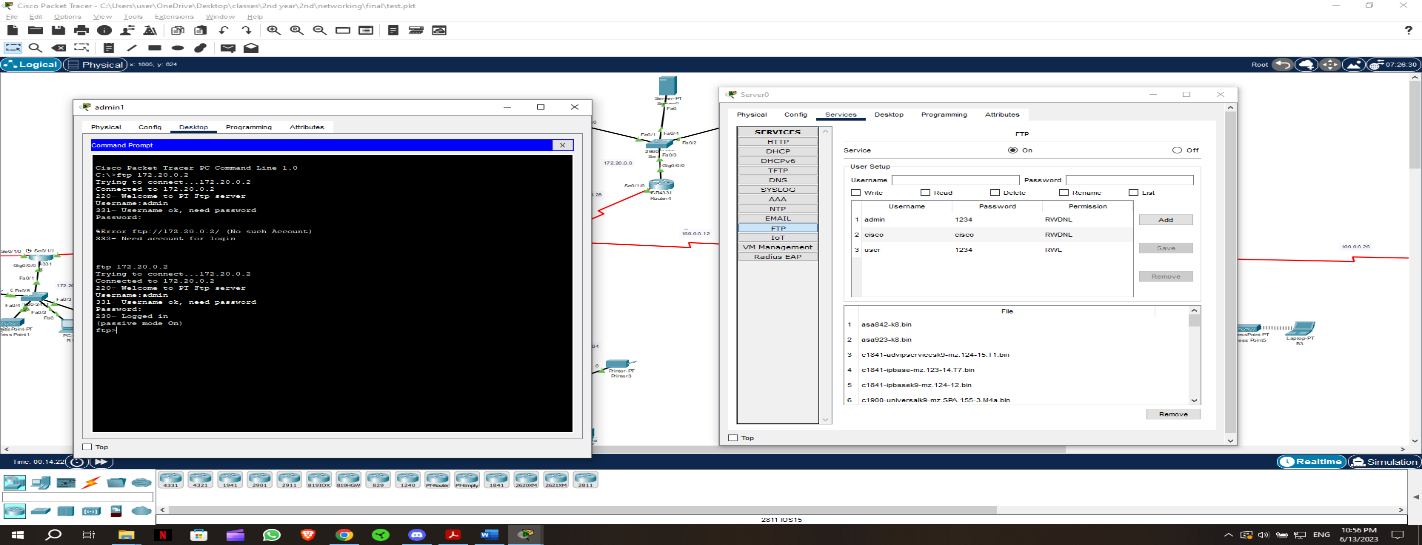
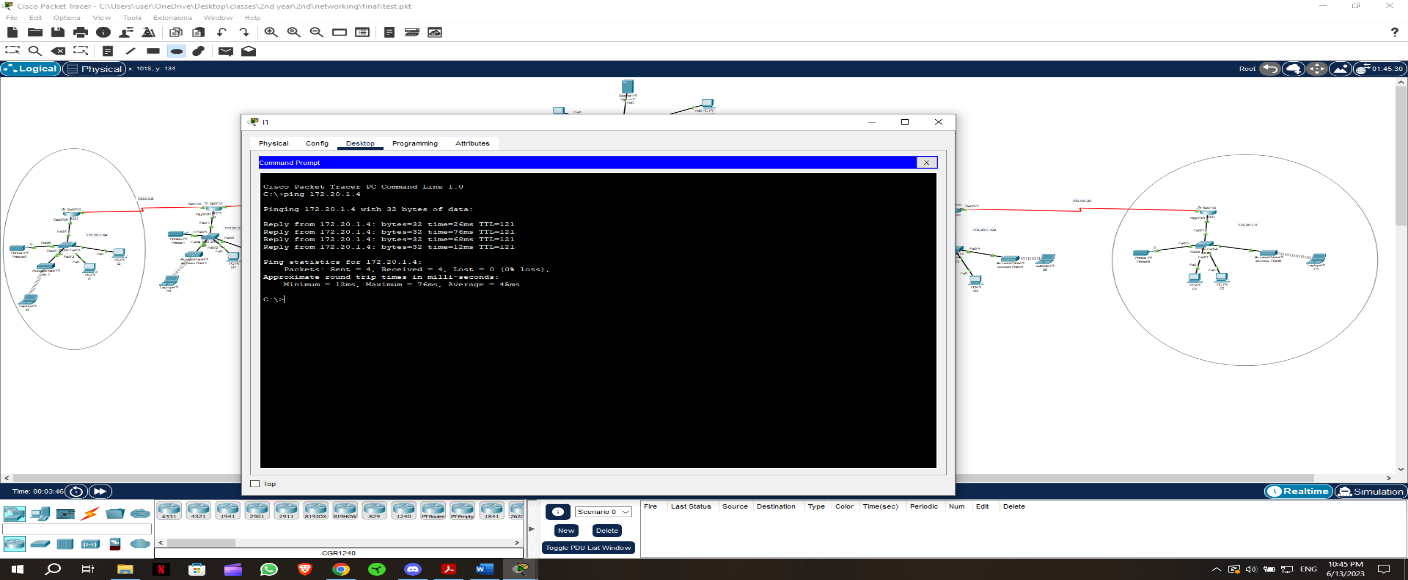
3:maintenance schedule.

Part 3

1 the implemented network is attached with the submission

2 I will perform these tests from the farthest 2 devices to make sure everything is working appropriately

3.



All ip configs are cheeked and everything is working appropriately

4 every network can be enhanced but at the same time every network administrator have to consider their clint budget and the admin cant make the best network there is for all clints then we wouldn’t need admins we are just going to run the same network on all clints but in my network I can recommend connecting the routers as a mesh or star topology to enhance connectivity and make sure that no wire will take down all the network but this will also cost a lot since every router in different country

5. regular upgrades are important for maintaining performance and functionality they ensure that the network stay up to date with the latest technologies, features and patches upgrade often bring improved performance and increased efficiency, upgrades can improve: 1 security 2. Compatibility 3. performance

And the enhancement in the security aspect a. access control b. firewalls c. data encryption

6. there are any aspects for enhancement the most important of them are:

1. design: as I mentioned in part3: 4 the design can be improved at the cost of budget

2. performance: in this aspect there are 2 most important elements which are protocol(software) design (hardware) in terms of the protocol connectivity I used the fastest available protocols Ethernet and OSPF

But there will always be room for improvement you can switch the wires from Ethernet to fiber optic which would be way more costly and you can make the WIFI on 5ghz instead of the 2.4 standard in the packet tracer unfortunately the option isn’t available but I would recommend the 5ghz for the clint since the performance outweigh the cost.

3. security: from my perspective you - add a special firewall server to the network to enhance security and you can deny some sort of accesses to the users to eliminate some risks but that would also risk efficacy.