



Networking
30201110
H/615/1619

Section (5)

Assignment 10
J-Games

Submitted to
Dr. Hebah AlDahoud

Submitted on
June 16th, 2022

Submitted by
Marwan Tareq Shafiq Al Farah

Student ID
21110011

Spring 2021 - 2022

Table of contents

Part 2: Design Efficient Networked Systems	3
The Network	3
The Clear Blueprint of the Overall Network	3
Network Configuration Information	3
Subnetting	3
End Devices' Configuration Information	4
IP Configuration and Valid IP Ranges	4
Router Configuration Information	5
Detailed Information about the Servers to be Installed	6
Services to be Installed	6
Configuration of each Service	7
IP Addresses of the Servers	8
The Test Plan	9
What to be Tested	9
Tools or Commands Used for Testing	9
Expected Results	10
Maintenance Schedule	10
References	11
 Part 3: Implement, Test, and Diagnose Networked Systems	 13
Implementation of the Networked Systems	13
Verification Procedure	13
Record of the Test Results	13
Recommendations for Potential Enhancements and Functionalities to Support Device Growth	16
Recommendations for Potential Enhancements	16
Functionalities to Support Device Growth	18
Critical Reflection	18
References	18

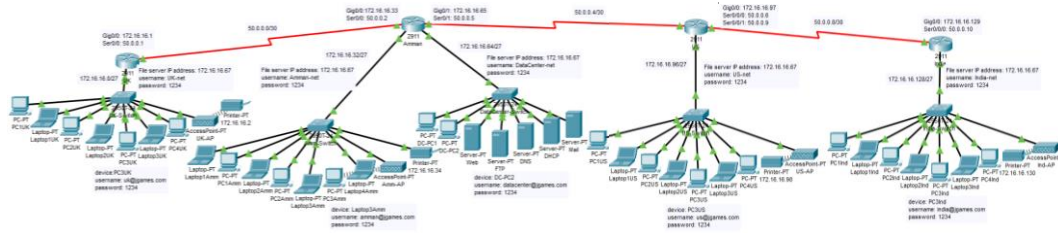
Part 2: Design Efficient Networked Systems

1- The Network:

Firstly, I set up 4 subnets (LANs) in the US, UK, Amman, and India, in which each of them contains 7 PCs or Laptops, 1 Printer, and 1 Access Point. Then I connected all of the devices in each subnet with a switch 2950T-24 using the Copper Straight-Through Cable to form a star network. Furthermore, I connected each switch with its router 2911 using the Copper Straight-Through Cable. After that, I added the HWIC-2T WAN Interface Card to each of the routers, to be able to connect all of the routers using the Serial Cable (Point-to-Point connection), therefore, creating the WAN (Wide Area Network). Finally, I added one last subnet (The Datacenter in HQ) which contains 5 servers and 2 PCs, then I connected these devices to a Switch using the Copper Straight-Through Cable that I directly connected to the HQ Router using the Copper Straight-Through Cable.

The configuration of PCs, Laptops, Servers, Routers, Printers, Access Points, and Services is specified below.

a. The Clear Blueprint of the Overall Network:



b. Network Configuration Information:

1. Subnetting:

To be able to do the network configuration, firstly, we have to determine the subnet mask of the network.

$$2^{\text{subnet identifiers}} \geq \text{number of subnets} \quad \text{subnet identifiers} \in \text{integers}$$

$$2^x \geq 5$$

$$x = 3 = \text{number of subnet identifiers}$$

The original subnet mask = 255.255.255.0 (decimal notation) = /24 (prefix notation)

New subnet mask = 255.255.255.1110 0000 = 255.255.255.224 (decimal notation) = /27 (prefix notation)

$$\text{Block size} = 2^{\text{number of 0s}} = 2^5 = 32$$

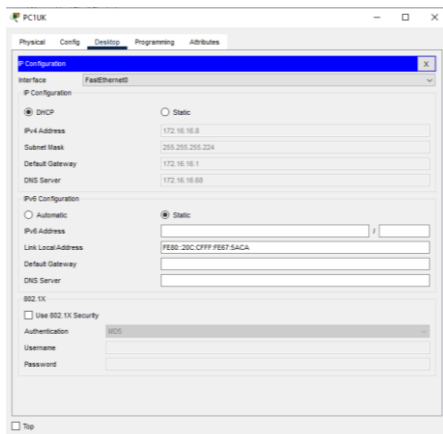
$$\begin{aligned} \text{Number of valid IP addresses} &= \text{Number of hosts per subnet} = \text{Block size} - 2 \\ &= 32 - 2 = 30 \end{aligned}$$

2. End Devices' Configuration Information:

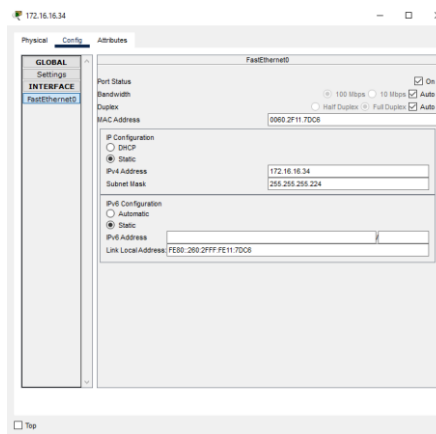
All end devices besides the printers and the servers will be given their IP configuration dynamically using the DHCP service (Dynamic Host Configuration Protocol). Printers and servers will be given their IP configuration statically by using one of 6 reserved IP addresses in each network that will be specified in the next point

3. IP Configuration and Valid IP ranges:

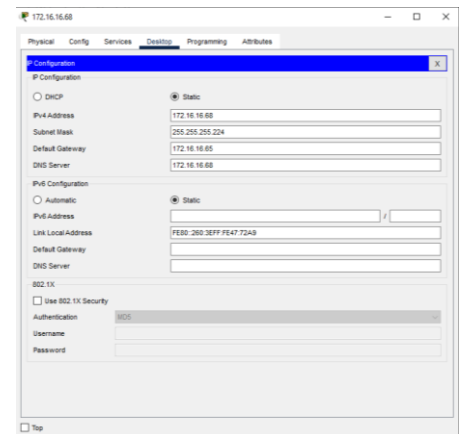
Network	UK	Amman	Data Center	US	India
Network ID	172.16.16.0	172.16.16.32	172.16.16.64	172.16.16.96	172.16.16.128
First Valid IP Address	172.16.16.1	172.16.16.33	172.16.16.65	172.16.16.97	172.16.16.129
Default Gateway					
Reserved IP Addresses	172.16.16.2	172.16.16.34	172.16.16.66	172.16.16.98	172.16.16.130
	—	—	—	—	—
	172.16.16.7	172.16.16.39	172.16.16.71	172.16.16.103	172.16.16.135
Start IP address (DHCP)	172.16.16.8	172.16.16.40	172.16.16.72	172.16.16.104	172.16.16.136
Last Valid IP Address	172.16.16.30	172.16.16.62	172.16.16.94	172.16.16.126	172.16.16.158
Broadcast IP Address	172.16.16.31	172.16.16.63	172.16.16.95	172.16.16.127	172.16.16.159
DNS server	172.16.16.68				
Subnet Mask	255.255.255.224				



Example of the PCs' and Laptops' IP configuration



Example of the Printers' IP configuration



Example of the Servers' IP configuration

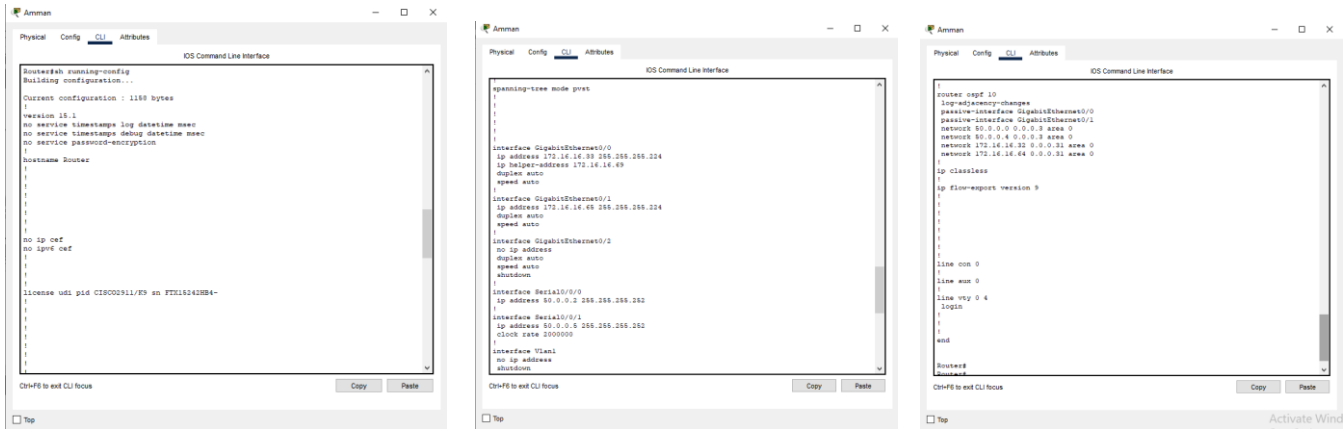
4. Router Configuration Information:

For the networks that connect the routers, we use the subnet mask 255.255.255.252 (decimal notation), /30 (prefix notation), because it gives us a block size of 4, with only 2 valid IPs that can be used, and that is what is needed with the network that is between the routers.

$$\text{Block size} = 2^{\text{host identifiers}} = 2^2 = 4$$

$$\text{Valid IPs} = 2^{\text{host identifiers}} - 2 = 2^2 - 2 = 4 - 2 = 2$$

Network between Routers	UK - Amman	Amman - US	US-India
Network ID	50.0.0.0	50.0.0.4	50.0.0.8
First Valid IP Address	50.0.0.1	50.0.0.5	50.0.0.9
Last Valid IP Address	50.0.0.2	50.0.0.6	50.0.0.10
Broadcast IP Address	50.0.0.3	50.0.0.7	50.0.0.11
Subnet Mask	255.255.255.252		



Example of the Routers' configuration

Firstly the routers' configuration starts by giving each interface their IP configuration by going into the CLI (Command Line Interface), and going from the User Mode to the Privilege Mode by using the “enable” command, then going from the Privilege Mode to the Global Configuration Mode by using the “configure terminal” command, then going from the Global Configuration Mode to the Interface Mode by using the “Interface” command followed by the name of the interface (such as GigabitEthernet0/0). After we have reached the Interface Mode, we use the “ip address” command followed by the IP address that you want to give to that interface along with its subnet mask. We also use the “no shutdown” command in the Interface Mode to enable that interface. Finally, we repeat the same process for the rest of the interfaces that we want to give their IP configuration.

I used the OSPF routing protocol (Open Shortest Path First) as opposed to the RIP routing protocol (Routing Information Protocol), mainly because the 4 branches of J-Games span out through different continents, therefore, they will most likely need more than 16 routers to connect between the 2 ends of the network, and RIP supports a maximum of 16 routers, therefore, OSPF was the valid option for this case. I also

didn't use the static routing protocol because using it is a full-time job for the network administrator, and it requires a lot of configuration and a single human error could cause the network to not function properly. I used the OSPF routing protocol on the routers, for them to be able to exchange their routing table, to allow all subnets to be visible to each other, and therefore, to communicate with each other. I started by entering the "router ospf" command followed by the Process ID (a number between 1 and 65535), in the Global Configuration Mode to go to the Router Mode. Then, I entered the command "network" followed by the network ID of a network that is directly connected to the router followed by the Wild Card Mask (which can be calculated by converting each 0 into a 1 and each 1 into a 0 in the subnet mask) and then the area number "area 0". This process is repeated for each network that is directly connected to the router. After that, if there is an interface in the router that is not directly connected to another router, we use the "passive-interface" command followed by the name of that interface (such as GigabitEthernet0/0) so that the router doesn't consume the network's bandwidth by sending its routing tables to end devices (such as PCs and Laptops). Finally, we repeat this process for all the routers in the network.

I also used the "ip helper-address" command followed by the IP address of the DHCP server, in the Interface Mode of the interface that tries to broadcast the discover DHCP message, to allow the message to be directed toward the DHCP server, for the PCs or Laptops to be able to be given their IP configuration dynamically.

After all the configuration on the routers was done, I returned to the Privilege Mode and inserted the command "wr" to ensure that all of my configurations on the routers were saved.

c. Detailed Information about the Servers to be Installed:

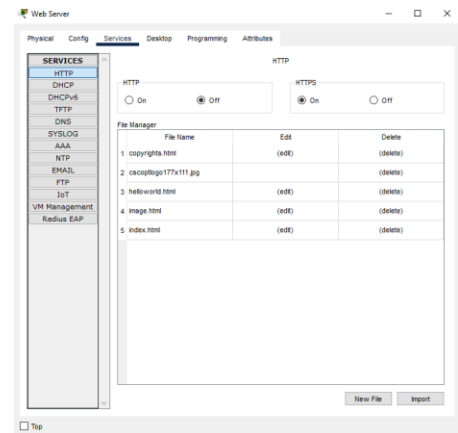
i. Services to be Installed:

1. Web Service on the Web Server using the HTTPS Protocol. In the business requirements of the network, it was specified that the employees have to have access to the company's internal system to be able to share projects, tasks, and data through a secure website.
2. DNS Service on the DNS Server using the DNS Protocol. In the business requirements of the network, it was specified that the employees should be able to access the company's internal system by using FQDN (Fully Qualified Domain Name) (<https://projects.jgames.com.jo/>).
3. File Service on the File Server using the FTP Protocol. In the business requirements of the network, it was specified that employees should be able to share and transfer files among all remote offices.
4. Mail Service on the Mail Server using the SMTP/POP3 Protocols. In the business requirements of the network, it was specified that the employees should be able to send and receive emails from each other.
5. DHCP Service on the DHCP Server using the DHCP Protocol. This service will be installed on the DHCP server, firstly, to avoid human error in the process of the IP configuration of PCs and Laptops. Secondly, the process of

statically inserting the IP configuration of every PC and Laptop can be a very tedious job and can get overwhelming very quickly, in comparison to dynamically giving it its IP configuration.

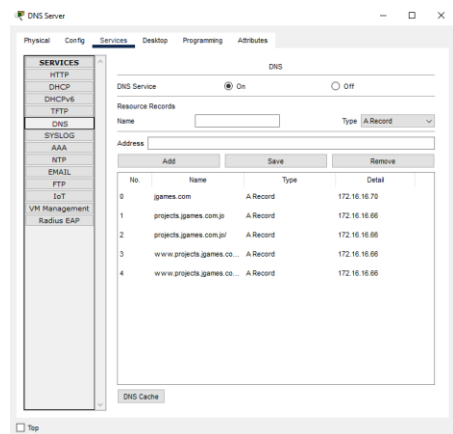
ii. Configuration of Each Service:

1. **Web Service:** I will go to Services in the Web Server, then select HTTP. I will turn the HTTP (Hypertext Transfer Protocol) protocol “Off” and make sure that the HTTPS (Hypertext Transfer Protocol Secure) protocol is turned “On” to ensure a secure connection between the server and the host.



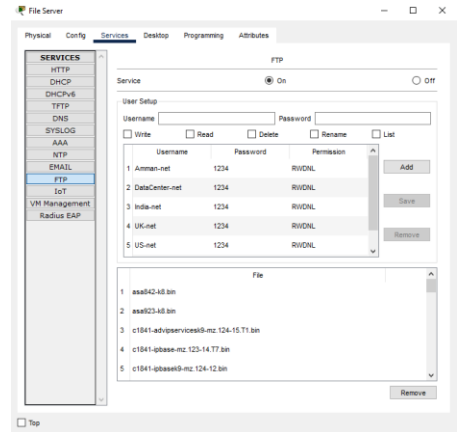
Web Service Configuration

2. **DNS Service:** I will go to Services in the DNS Server, then select DNS (Domain Name System). I will make sure that the DNS Service is turned “On”. Then I will insert the domain name of the website in the “Name” slot, and the IP address of the Web Server in the “Address” slot, then I will press “Add” and repeated this process for all the names that I want to give for my website. I will also add the domain name of the email addresses in the DNS server as I put the name as “jgames.com” and the address of the Mail Server. Finally, I will enter the IP address of the DNS Server in the IP configuration of all end devices, statically and dynamically.



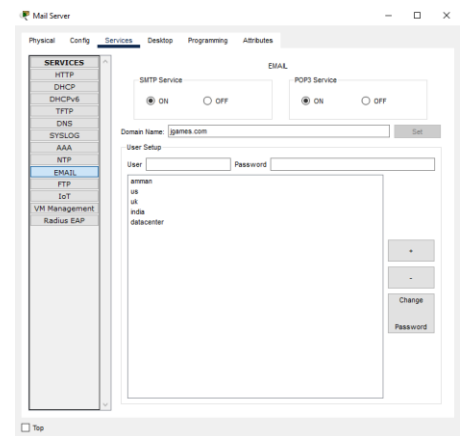
DNS Service Configuration

3. **File Service:** I will go to Services in the File Server, then select FTP (File Transfer Protocol). I will make sure that the FTP Service is turned “On”. Then I will insert the username and password of the user that I want to create and give the user all 5 permissions (Read, Write, Rename, List, and Delete), and then press “Add” to create that user. I will repeat that process for each user that I want to create.



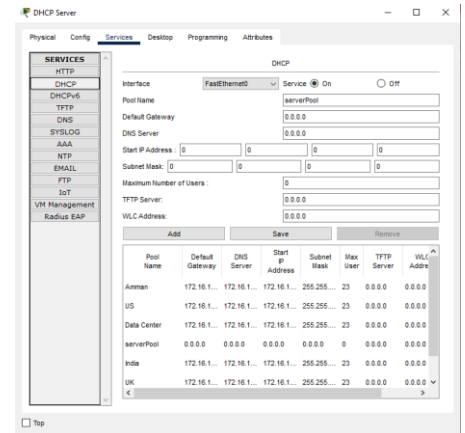
File Service Configuration

4. **Mail Service:** I will go to Services in the Mail Server, then select EMAIL. I will make sure that the SMTP (Simple Mail Transfer Protocol) and POP3 (Post Office Protocol 3) protocols are turned “On” to ensure that all the emails can be sent using SMTP and received using POP3 successfully. Firstly, I will insert the domain name of the email “jgames.com” and then press “Set”. Then I will insert the username (the name before the ‘@’ in the email address) and password of the user that I want to create, and then I will press “+” to create that user. I will repeat that process for each user that I created. Finally, I will press on email on the PCs and Laptops that will have the Mail Service on them and I will configure their mail, by inserting the User Information, Logon Information, and Server Information (the IP addresses of the incoming and outgoing Mail Server).



Mail Service Configuration

5. **DHCP Service:** I will go to Services in the DHCP Server, then select DHCP. I will make sure that the DHCP service is turned “On”. After that, I will enter the Pool Name, its default gateway, and the IP address of the DNS server. Then I will also enter the “Start IP address” after reserving 6 IP addresses for any devices that need to use the static IP configuration. After that, I calculated the maximum number of users by subtracting the last octet of the broadcast IP address from the last octet of the start IP address. Furthermore, I pressed “Add”, which added the network to the DHCP Server. After that, I used the IP helper-address command on the routers as I have mentioned before to enable devices in other subnets to use the DHCP service as well. Finally, when you press on DHCP in the IP configuration of one of the PCs or Laptops, it should gain its IP configuration dynamically using DHCP, not APIPA.



DHCP Service Configuration

- iii. **IP Addresses of the Servers:**
1. **Web Server:** 172.16.16.66/27
 2. **DNS Server:** 172.16.16.68/27
 3. **File Server:** 172.16.16.67/27
 4. **Mail Server:** 172.16.16.70/27
 5. **DHCP Server:** 172.16.16.69/27
- 2- **The Test Plan:**
- a. **What to be Tested:**
1. Test the connectivity between all the subnets and test the functionality of the OSPF routing protocol.
 2. Test the functionality of the Web service that is using the HTTPS protocol on the Web Server.
 3. Test the functionality of the DNS service that is using the DNS protocol on the DNS Server.
 4. Test the functionality of the File service that is using the FTP protocol on the File Server.
 5. Test the functionality of the Mail service that is using the SMTP/POP3 protocol on the Mail Server.
 6. Test the functionality of the DHCP service that is using the DHCP protocol on the DHCP Server.
 7. Test the functionality of the wireless connection using the Access Point device.
- b. **Tools or Commands Used for Testing:**
1. By inserting on the command prompt of one of the end devices (PCs, Laptops, or Servers) the command “ping” followed by the IP addresses of an end device from

a different subnet, then repeating this process throughout all the subnets to check the connectivity between all of them.

2. By inserting on the URL of the Web Browser of one of the end devices (PCs, Laptops, or Servers) “https://” followed by the IP address of the Web server (172.16.16.66).
3. By inserting on the URL of the Web Browser of one of the end devices (PCs, Laptops, or Servers) “https://” followed by one of the domain names of the website.
4. By inserting on the command prompt of one of the end devices (PCs, Laptops, or Servers) the command “ftp” followed by the IP address of the File Server (172.16.16.67), then by entering the username and password of the user, and then using the “put” command followed by the name of the file and its extension that will be transferred, then repeating the process on another end device which is located on another subnet but using the “get” command instead of “put” and then using the “dir” command on the command prompt.
5. By pressing on the email of one of the end devices (PCs or Laptops) that has their email configured and then pressing compose and then inserting the email address, subject, and content of the email and then pressing “Send”, and then going to the email of the end device that has its mail configured to the same email address that had the email sent to, and then pressing “Receive”.
6. By pressing DHCP on the IP configuration of one end device (PCs or Laptops) in each subnet.
7. By switching out the Ethernet port with a Wireless port on one of the end devices (PCs or Printers), then choose in Authentication “WPA2-PSK”, and then enter the SSID of the Access Point and its PSK Pass Phrase.

c. Expected results:

1. To get a 100% reply from the destination host.
2. For the website to appear on the web browser.
3. For the website to appear on the web browser.
4. For the file to be transferred to and from the File Server successfully, and for the file to appear on the device that received it when the “dir” command is put in the command prompt.
5. For the email to be sent and received successfully.
6. For the “DHCP request successful” message to appear, and for the end device to have the correct IP configuration.
7. For the connection to be established successfully, by having Wi-Fi signals connect between the end device and the Access Point.

3- Maintenance Schedule:

A network maintenance plan is a plan that consists of all the tasks and systems that are put in place to ensure that all key components of the network are monitored regularly for any potential problems. A good maintenance plan should be able to predict problems and

take the required steps to address them before they even occur. (World Wide Services, 2018; M Global Services, 2019; eTech7, 2020)

Since the network consists of hardware like servers, printers, laptops, scanners, etc., and software like the OS, computer programs, etc., hardware and software installation are an essential part of any network maintenance plan to ensure that the devices and programs you have are ready to use without any problems. (World Wide Services, 2018; M Global Services, 2019; eTech7, 2020)

Network Maintenance Schedule: (World Wide Services, 2018; Jacobs, 2021; Supertechman, 2021)

	Daily	Weekly	Monthly	Quarterly	Annually
Keep track of performance benchmarks, such as WAN connection speed and its average usage, and the latency of ping to reach a remote office.	✓				
Data backups on a local or network level	✓				
Checking that all services on the servers are working properly	✓				
Backups should be tested and ensure that you can properly restore a virtual machine from zero.			✓		
Check the network's security by checking for any infected devices, and checking the licenses, dashboard, and logs.		✓			
Check the software on your switches and routers and any other devices in the network, and make sure the data and time are still correct.				✓	
All service accounts' passwords should be checked and reset.					✓

References:

eTech7 (2020) *What Is a Network Maintenance Plan and Does Your Business Need It?*, eTech7. Available at: <https://blog.etech7.com/what-is-a-network-maintenance-plan>

Jacobs, D. (2021) *Key Tasks in a Network Maintenance Checklist, The Importance of Regular Network Maintenance*. Available at: <https://www.techtartget.com/searchnetworking/tip/Key-tasks-in-a-network-maintenance-checklist>

M Global Services (2019) *What is Network Maintenance? / M Global Services, M Global Services*. Available at: <https://mglobalservices.com/knowledge-center/blog/what-is-network-maintenance>

Supertechman (2021) *Server and Network Maintenance Checklist*. Available at:
<https://supertechman.com.au/server-and-network-maintenance-checklist/>

World Wide Services (2018) *What Is Network Maintenance? / Network Maintenance Plans & Tips*, World Wide Services. Available at: <https://worldwideservices.net/network-maintenance-guide-upkeep/>

Part 3: Implement, Test, and Diagnose Networked Systems

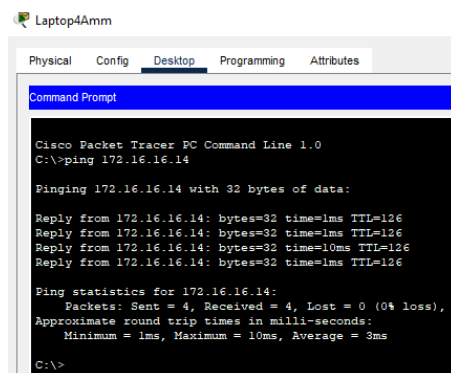
1. Implementation of the Networked System: on the Cisco Packet Tracer 8.1.1 file.

2. Verification Procedure:

- a. **ping:** it is used for checking the accessibility of the devices on the network, and to check for the connectivity between all subnets by following the steps that are mentioned in Part 2 (section 2.b.1). (Cisco, 2010)
- b. **ftp:** it is used for transferring files over the network and it is used to check the functionality of the FTP Service by following the steps that are mentioned in Part 2 (section 2.b.4).
- c. **Extended ping:** it is used to check for host reachability and network connectivity in a more advanced way. When a ping is sent from a router, the source IP address is the IP address of the interface that the message came out of, therefore, with extended ping you can change the source IP address of your message to an IP address of another interface of the router. You can also use extended ping to change the number of sent packets, change the datagram size, the time of the timeout of the ping message, and many other options by inserting the command “ping” on the CLI of a router in the Privilege Mode. (Cisco, 2010)
- d. **nslookup:** it is a command that is used to get the IP address of the DNS Server of the device, and the IP address of the Web Server of one of the domain names of the websites that the DNS Server has by inserting the command “nslookup” on the CMD of a device.
- e. **telnet:** telnet is a Layer 7 protocol that allows users to access and manage devices remotely by telnetting their IP address or their hostname by following a series of configuration steps on the CLI of the switch and the CMD of a PC or Laptop. (Computer Networking Tips, 2020)
- f. **Packet Sniffer:** it is used to monitor the traffic in a network by monitoring either the incoming or the outgoing packets from/to a subnet by connecting the Sniffer between the switch and the router. (Kaspersky, 2019)
- g. **tracert:** it is used to determine the route that a packet takes to reach its destination by inserting the command “tracert” followed by the destination IP address on the CLI of the router in the Privilege Mode. (CCNA, 2019)

3. Record of the Test Results:

- a. **ping:** it matches the expected result as 100% of the sent packets were received without any loss of data.



```
Laptop4Amm
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.16.16.14

Pinging 172.16.16.14 with 32 bytes of data:

Reply from 172.16.16.14: bytes=32 time=1ms TTL=126
Reply from 172.16.16.14: bytes=32 time=1ms TTL=126
Reply from 172.16.16.14: bytes=32 time=10ms TTL=126
Reply from 172.16.16.14: bytes=32 time=1ms TTL=126

Ping statistics for 172.16.16.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 10ms, Average = 3ms

C:\>
```

Ping

- b. **ftp:** it matched the expected result because the file was transferred successfully to and from the server and the file appeared on the device that received it when the “dir” command was put on that device’s CMD.

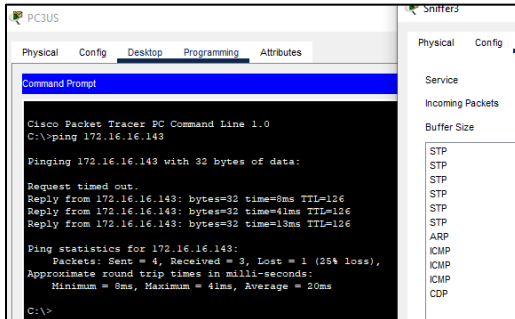
- c. **Extended ping:** it matches the expected result as 100% of the sent packets were received without any loss of data.

- d. **nslookup command:** it matched the expected result as it gave us the correct IP addresses of the DNS Server and Web Server.

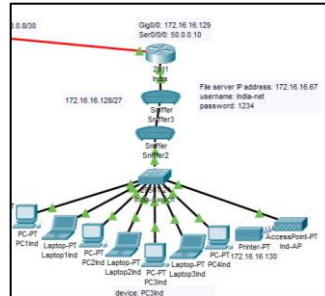
- e. **telnet:** it matched the expected result as the user was able to access and manage the switch remotely on a Laptop.

telnet

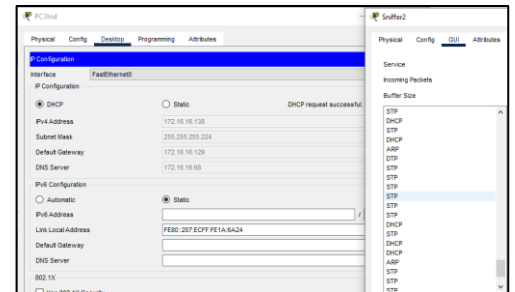
- f. **Packet Sniffer:** it matched the expected results as the packet sniffer (for the traffic that is coming into the LAN) detected 3 ICMP (ping) messages, and the packet sniffer (for the traffic that is coming out of the LAN), detected the DHCP messages when a device turned “On” its DHCP IP configuration.



Packet Sniffer
(For the traffic that is coming into the LAN)

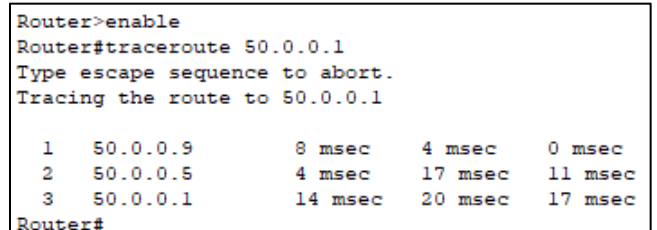


Packet Sniffers
(As a test in the Cisco Packet Tracer File)



Packet Sniffer
(For the traffic that is coming out of the LAN)

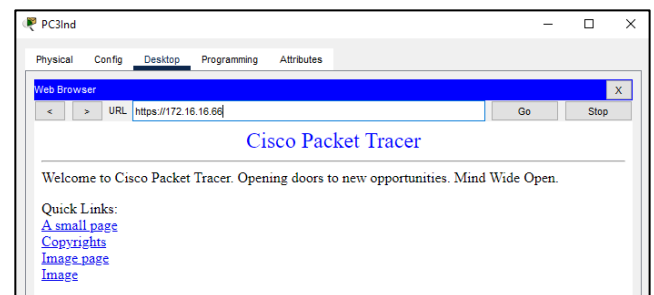
- g. **traceroute:** it matched the expected result as it gave us the correct route that the packet took to reach its destination.



traceroute

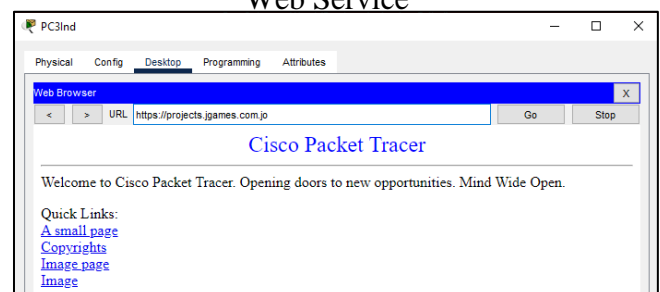
The rest of the services that need to be tested:

- h. **Web Service:** it matched the expected result because the website page appeared.



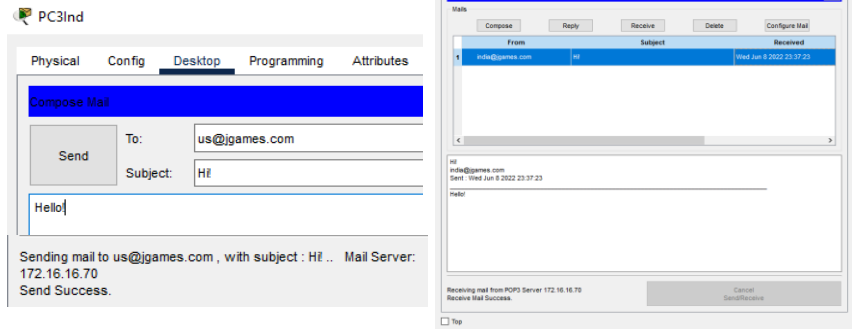
Web Service

- i. **DNS Service:** it matched the expected result because the website page appeared.



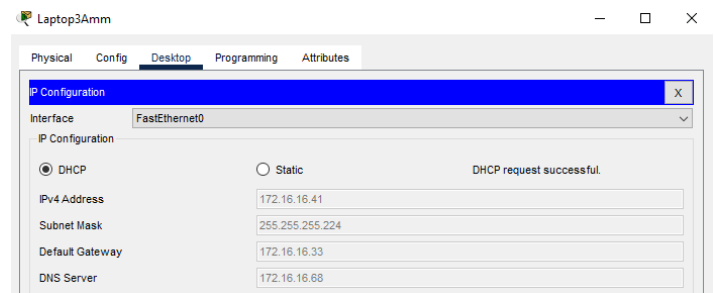
DNS Service

- j. **Mail Service:** it matches the expected result because the email was sent and received successfully.



Mail Service

- k. **DHCP Service:** it matches the expected result because the “DHCP request successful” message appeared and the correct IP configuration was given for the device.



DHCP Service

4. & 5. Recommendations for potential enhancements and functionalities to support device growth:

a. Recommendations for potential enhancements:

1. **Create a separate network for guests:** if you routinely welcome a big number of guests that want Internet connectivity, you may run into issues of your network slowing down, because having a few guests using your network isn't a big deal, however, when you have up to a hundred visitors at any given time, network slowdowns are very certain to occur, therefore, you can offer them to log in to a guest network rather than the main network. (Model, 2018; LiveAction, 2019)
2. **Reconfigure the hardware on your network:** if any new devices are added to your network or when any devices in the network get updated, you have to make sure that the devices are properly configured, and if necessary reconfigure these devices to match the network's requirements, to ensure that the devices can communicate and interact with each other properly, and to avoid any difficulties in routing or any increased latency. (Hein, 2019)
3. **Monitor and eliminate bottlenecks:** bottlenecks are among the most common issues that networks face regularly because even if one device is

functioning slower than the rest it can cause a ripple effect that will affect the network's latency greatly across different areas of the network. This is the reason that most corporations run their network backups late at night when almost no one is using the network, therefore, not consuming the network's bandwidth when employees are working. A network monitoring tool will look for any traffic in your network and it will notify you if it identifies a device or area of a network that is performing slowly to be able to solve the issue as soon as possible. (Model, 2018; Hein, 2019)

4. **Update and Upgrade your network regularly:** for a network to function properly and with maximum efficiency, all of the software and firmware must be updated or upgraded when new versions are released. There are many other reasons behind the importance of updating and upgrading your network. First and foremost, after a certain period, the expense of maintaining your network with outdated technology outweighs the cost of modernizing it, therefore, it will help us get more cost-effective equipment. Also, for the network administrator, the employees, and the consumers, new equipment improves their experience on the network drastically. Network updates and upgrades also help in improving your network's security, because with each update new security measures are put into place to protect the users more and more from any cyber-attacks or malware. New updates and upgrades will also provide you with new features that will help your business thrive and stand out which will help you keep up with your competitors. Last but not least, by regularly updating or upgrading your network, you are lessening your tech debt and making it easier for you to reach the latest technology generation with minimal costs. (Model, 2018; LiveAction, 2019; Intelligent Technical Solutions, 2022)
5. **Regular security checkups:** a reliable and effective network security system is critical for safeguarding the data of the company. No matter the size of the company, network security and regular security checkups is one of the most crucial factors to take into account while working over any type of network. Thanks to network security all workstations are protected from any malicious software. By splitting down information into several components, encrypting these parts, and transmitting them across distinct pathways, the safety of the shared information is ensured. Network security also ensures, through its security requirements, that when any vulnerabilities appear in the network they will be solved immediately by continuously monitoring the network for any suspicious activities that could compromise it. (ECPI, 2022)
6. **Adding backup servers:** if the budget allows for backup servers to be purchased, I would like to buy backup servers for the network to ensure that the network and all services will keep on functioning even if a server is down.

b. Functionalities to support device growth and the addition of communication devices:

1. **Subnetting:** it can help you divide your original network into many smaller subnets. For example, by subnetting the original network 172.16.16.0/24, we have created 8 different subnets each with the subnet mask of 255.255.255.224, and only 5 networks have been used, therefore, 3 subnets are kept for further expansion of the network. Also, each subnet was designed to withstand 22 employees, while only 7 employees are working currently in every branch.
2. **Adding additional servers:** the growth of the network will put more strain on the servers, therefore, there would be a bigger chance that one of them will crash, but if the load is distributed on more than one server, the chances of the server breaking down is much smaller.
3. **Load Balancers:** it is a device that distributes network traffic across multiple servers to boost application capacity and reliability, increase the network's bandwidth, and lower the network's latency. They boost application performance by relieving servers of their load by distributing it between other servers.
4. **Consult an MSP:** to deploy an all-in-one network management solution to set up a scalable network, and to have a single network administration tool not a patchwork of several different parts which will make any future device growth much easier and smoother. (XBASE Technologies, 2018)

6. Critical Reflection:

I believe I did a good job on this project because I was able to fully implement all of the business requirements that were specified in the assignment brief, in the Cisco Packet Tracer Simulator. I believe I have thoroughly detailed every step I took to plan, implement, and test my network, perfectly, in the report since I am confident that I fully comprehend each and every one of them. The report also included a maintenance schedule, recommendations for potential enhancements, and functionalities to support device growth and the addition of communication devices, which I didn't fully comprehend at first, but after conducting extensive research, I believe I have reached a deep understanding of each of these topics and have adequately covered them in the report, but I hope to be able to improve my technical knowledge about them in further courses. Finally, I would like to improve and enhance my network more in the future by making the network more secure and be able to implement all of my recommendations of potential enhancements for the network to become as efficient and as effective as possible.

References:

CCNA (2019) *Traceroute Command*, CCNA. Available at: <https://study-ccna.com/traceroute-command/>

Cisco (2010) *Using the Extended ping and Extended traceroute Commands The ping Command*, Cisco. Available at: http://www.cisco.com/image/gif/paws/13730/ext_ping_trace.pdf

Computer Networking Tips (2020) *Configuring Telnet on a switch and a router in Packet Tracer*, Computer Networking Tips. Available at: <https://computernetworking747640215.wordpress.com/2018/07/05/configuring-telnet-on-a-switch-and-a-router-in-packet-tracer/>

ECPI (2022) *Importance of Network Security: Safety in the Digital World*, East Coast Polytechnic Institute. Available at: <https://www.ecpi.edu/blog/importance-of-network-security-safety-in-the-digital-world#:~:text=A good network security system,shared data is kept secure.>

Hein, D. (2019) *7 Ways to Improve Your Company's Network Performance*, Solutions Review. Available at: <https://solutionsreview.com/network-monitoring/7-ways-to-improve-your-companys-network-performance/>

Intelligent Technical Solutions (2022) *Why Should You Upgrade Your Network This 2022? (5 Crucial Advantages)*, Intelligent Technical Solutions. Available at: <https://www.itsasap.com/blog/upgrade-network-advantages>

Kaspersky (2019) *What is a Packet Sniffer?*, Company Website. Available at: <https://usa.kaspersky.com/resource-center/definitions/what-is-a-packet-sniffer>

LiveAction (2019) *5 Ways to Improve Network Performance*, LiveAction. Available at: <https://www.liveaction.com/resources/blog/5-ways-to-improve-network-performance/>

Model, I. (2018) *8 Tips to Improve Network Performance in Your Office*, Managed IT. Available at: <https://brightlineit.com/8-tips-to-improve-network-performance-in-your-office/>

XBASE Technologies (2018) *How can I make my network scalable?*, XBASE Technologies. Available at: <https://www.xbase.com/2020/01/how-can-i-make-my-network-scalable/>