

**Network Final Project.**

**Jordan National Railway (JNR)**

**Submitted By: Hamza Osama AL-Risheq.**

**Submitted To: Dr. Sami Al-Mashaqbeh**

**Summer 2021 – 2022**

**Table of contents:**

Introduction………………………………………………………………………………………………………………(page 3)

Task 1:

Task 1, Part1, Types of networks based on the size of the network……………………………(page 3 – page 5)

Task 1, Part2, Physical network topology……………………………………………………………………(page 6 – page 10)

Task 1, Part3, Logical topology protocol……………………………………….….…………………………(page 10 – page 12)

Task 1, Part4, Protocols………………………….…………………………………….….…………………………(page 12 – page 15)

Task 1, Part5, Network devices…………………………………………………….….…………………………(page 16 – page 18)

Task 1, Part6, Servers…………….…………………………………………………….….…………………………(page 19 – page 20)

Task 1, Part7, inter-dependences of the hardware with relevant networking software(page 20 – page 22)

Task 2:

Task 2, Part1, Part a, clear blueprint of your overall network ……………………………………(page 23 – page 24)

Task 2, Part1, Part b, Network configuration information for each device …..……………(page 24 – page 49)

Task 2, Part1, Part c, Detailed information about the servers to be installed.……………(page 50 – page 55)

Task 2, Part1, how to connect the printer wired and wirelessly.…………………….…………(page 56)

Task 2, Part2, Produce a detailed test plan……………………………...…………………….…………( page 57 – page 58)

Task 2, Part3, Maintenance schedule……………………………...…………………….…………………( page 58 – page 60)

Task 3:

Task 3, Part3, Record the test results for each installed service………………………………. (page 61 – page 64)

Task 3, Part4, Recommend potential enhancements and investigate………..……………. (page 65)

Task 3, Part5, Discuss the significance of upgrades and security requirements ………..(page 65)

Task 3, Part3, Critical reflection to evaluate own work……………………………………………. (page 66)

The declaration form and signature………………………………………………………………………….(page 67)

**Introduction:**

I have been employed as an assistant for the JNR train tracks in Jordan, I have been asked to create a network that covers 7 places in Jorden and one central data point. With all the parts of any network. Also, I am going to design everything and add 5 services to the network which are DHCP, HTTPS, DNS, FTP, and Email.

And the project I have been asked to do were separated into 3 tasks and every task was separated into many parts.

**Task 1:**

**Part 1.1:**

Types of networks: to know about types of networks first we should what is a network. Networks are defined as the connection of at least two computer systems, either by a cable or a wireless connection. There are many types of networks, these are the network types that depend on the network size.

Types Of Networks (based on size): starting from the smallest one to the hugest one:

1. Personal Area Network:

|  |  |  |  |
| --- | --- | --- | --- |
| Definition: | Usages: | Benefits: | Disadvantages: |
| The smallest type of network that are based on size. It connects personal device to create a network. PANs connect the devices on a very short distance which is less than 10 meters. It connects the devices wirelessly and have a range of protection that is 30 meters. | We use it to connect personal devices. For example, connecting the wireless headphones with laptop by using the Bluetooth. | 1- easy to control and protect the networks because it’s a very small area network.  2- you can connect many of the devices to one single device at the same time. | 1- The area coverage is very short. (Range limits).  2- It might establish a bad connection to other networks at the same radio bands. |

2- Local Area Network:

|  |  |  |  |
| --- | --- | --- | --- |
| Definition: | Usages: | Benefits: | Disadvantages: |
| The second smallest type of network that are based on size. It is a collection of devices (two or more devices) connected in one area by using mediums like twisted pair or coax. Its bigger than the PAN but smaller than the CAN, MAN and the WAN. | 1- We can share computer system resources like hard disks or printers, which help us to save more money because we use the same printer and so on.  2- we can use it to connect more than devices (two or more) together to share the data. Like using it in our home. | 1- Simple to manage the data from one place which makes the data more secured.  2- It is flexible and easy to grow.  3- Easy to secure the network.  4- Easy to troubleshoot the problems. | 1- The admin having access to everyone inside the network which means less privacy.  2- A virus can be spread more easily inside the network.  3- limited number of systems can only be connected. |

3- Campus Area Network (MAN):

|  |  |  |  |
| --- | --- | --- | --- |
| Definition: | Usages: | Benefits: | Disadvantages: |
| It’s a network that links many LAN networks to create the CAN network which is larger than the LAN network but smaller than the MAN and the WAN.  Also, it covers a limited area. | it is very helpful to campuses like colleges, universities, corporate organizations.  For example, when we want to create a network between the buildings inside the university, we use the CAN network. (CAN networks are used to help us connect between buildings that are in the same geographical area). | 1- The data transfer rate between systems is faster than the MAN and the WAN.  2- Economical.  3- easy and fast to share the data.  4- having options to connect many buildings wirelessly with the headquarter building. | 1- it’s expensive to have a maintenance for the network.  2- There is a limit for the network. |

4- Wide Area Network (WAN):

|  |  |  |  |
| --- | --- | --- | --- |
| Definition: | Usages: | Benefits: | Disadvantages: |
| It’s the hugest type of networks that based on the size. It is not tied to a single location.  It’s used to share the information and communicate between the devices around the world through the WAN network.  The WAN offers services for the devices to connect to wireless. | This type of network is used when we want to make a network around the world.  The internet is considered the largest WAN in the world. | 1- Easy to communicate and share data.  2- contains every type of devices.  3- High bandwidth.  4- Easy to transfer data from country to country (between huge distances). | 1- it’s too expensive to setup and create the network.  2- Very hard to secure the network.  3- Very expensive to have maintenance for the network.  4- it is slow compared to other networks.  5- it’s very complex and complicated. |

**Part 2:**

Physical Network Topology:

It’s the shape of the network that is made from different connectors usually to represent physical networks like cables, and the nodes usually represent the physical network devices (like switches or routers and so on). And there are a lot of types of physical network topologies such as star topology, ring topology, bus topology, Hierarchical topology, hybrid topology, and mesh topology.

The importance of Physical Topologies:

The layout of a network has a direct impact on the network’s functionality. Selecting the right topology can improve performance and data efficiency, optimize the allocation of resources, and reduce operational costs. Software-created network topology diagrams are important references for diagnosing network connectivity problems, investigating network slowdowns, and generally troubleshooting issues. One of the primary uses of network topologies is to define the configuration of various telecommunication networks, including computer networks, command and control radio networks, and industrial field buses.

Explanation of these types of topologies:

1-Ring Topology:

|  |  |  |
| --- | --- | --- |
| Definition: | Advantages: | Disadvantages: |
| In this shape, the devices connect with two neighboring devices, and they form a circle structure.  In this structure the data travels from one device to another until it reaches the desired destination. Because of the ring structure there isn’t an administrator. | 1- Data flows in one direction which reduces the chance of packet collisions.  2- Easy to manage.  3- The speed of data is very high.  4- no collisions. | 1- Difficult to troubleshoot the ring.  2- Expensive.  3- If one workstation shuts down, it affects whole network or if a node goes down entire network goes down. |

2-Extended Star Topology:

|  |  |  |
| --- | --- | --- |
| Definition: | Advantages: | Disadvantages: |
| In this structure all the devices connect with central devices (central connection point).  When a device wants to send data or communicate with other device in the network it must send the info to the central device through to the other side (destination). | 1- If one of the devices in the network or a cable fails (stops working) the network will still work. “This doesn’t include the central point because if the central point shuts down all of the networks will stop working”.  2- Every device will connect with one port with central point so that means cheaper cost  3- Easy to troubleshoot the problems and the disconnection inside the network. | 1- If the central device falls that means the network will stop working.  2- Needs extra hardware  3- If the central device gets hacked that means all the network has been hacked. |

3- Bus Topology:

|  |  |  |
| --- | --- | --- |
| Definition: | Advantages: | Disadvantages: |
| In this structure all the devices connect with one cable and the devices connect with main medium. The node checks the destination address (MAC/IP address) to know where to go.  If the address does not match with the node, the node does nothing more. But if the address of nodes matches the address contained within data, they process on knowledge. | 1- It is easy to connect or remove devices in this network without affecting other devices.  2- If any devices fall down the network will stay working.  3- Not expensive comparing to other topologies.  4- It is the easiest network topology to connect devices. | 1- If the main medium falls, that means all the network will stop working.  2- It’s not the good choice for huge networks.  3- Troubleshooting every single device individual very hard.  4- Very slow topology. |

4- Hierarchical Topology:

|  |  |  |
| --- | --- | --- |
| Definition: | Advantages: | Disadvantages: |
| In this structure all the devices connected make a tree form, them being the branches. And this type of topology is made from combining star and bus topologies. | 1- This type of topology is very secured.  2- Point-to-point wiring for individual device.  3- Easy to troubleshoot the problems.  4- Easy to maintenance the problems and the faults. | 1- Very difficult to make the configuration for it.  2- If a device in first level goes down all the devices in the other level under the first one will go down to.  3- Comparing to other topologies, the tree topology is slow, because there are too many nodes in the topology.  4- Needs too many mediums (cables) comparing to star and ring topology. |

5- Mesh Topology:

|  |  |  |
| --- | --- | --- |
| Definition: | Advantages: | Disadvantages: |
| In this type, the devices are completely connected with other device in the same network and there are two types of the Mesh, full mesh and partial mesh topology. | 1- If one of the devices or mediums is down the network will stay working.  2- Very hard to maintain.  3- used in large networks.  4- reliable network.  5- Easy to be modified on it. | 1- Very expensive.  2- Very complex.  3- Installation and configuration is difficult.  4- Very hard to extensible the network. |

6- Hybrid Topology:

|  |  |  |
| --- | --- | --- |
| Definition: | Advantages: | Disadvantages: |
| In this type of topology is made up from combinations of different topologies made from star topology and bus topology so on. | 1- It’s very flexible.  2- troubleshooting the problems is not hard.  3- created to use it in large networks.  4- reliable network.  5- Easy to be modified on it. | 1- Very expensive.  2- Very complex.  3- Installation and configuration is difficult. |

Comparison between Hybrid Topology and Hierarchical Topology:

This comparison will be on the cost, several PCs, the difficulty of configuring the network, the extensible, usages, the difficulty of the maintenance, and the difficulty of the troubleshooting and the security.

|  |  |  |
| --- | --- | --- |
| ////////////////////////////////////////////// | Hybrid Topology: | Hierarchical Topology: |
| Cost: | Expensive. | Expensive. |
| Number of PC’s: | You can add as much you want devices, and the size of network is larger than the tree topology. | Smaller than the hybrid topology but logically can add as much devices as needed. |
| The difficulty of configuration the network: | Hard to setup and configure the network because it’s a combination of topologies. | Easy compared to the hybrid topology. |
| The extensible: | Easy to extensible the network. | Easy to extensible the network. |
| Usages: | Used in WAN’s and MAN’s networks. | Used in WAN’s and MAN’s networks. |
| Difficulty of the maintenance: | Very hard to do maintenance to the network compared to the Tree topology. | Easier than the hybrid Topology. |
| Difficulty of the troubleshooting and the security: | Harder than the Tree topology to troubleshoot the problems.  It’s a secured network but it’s harder to control and protect. | Easier to troubleshoot the problems.  Its a secured network and it’s easy to control and protect. |

In the project that I have been asked to create a network for (JNR). I chose to use the hybrid topology and extended star topology. Because the hybrid topology covers a huge area, so we can cover all the Jordanian cities by using the hybrid topology. And I used the extended star topology for the Lan’s. Because all the devices will connect with one port in the switch and it’s easy to troubleshoot the problems. Also, because if one of the devices (except the level one device) falls down the network will stay working.

Diagram

Description automatically generatedA group of computer monitors

Description automatically generated with low confidence

Bus Topology. Hierarchical Topology.

Diagram, polygon

Description automatically generatedDiagram

Description automatically generated

Ring Topology. Mesh Topology.

Diagram

Description automatically generatedDiagram

Description automatically generated

Extended Star Topology. Hybrid Topology.

**Part 3:**

Logical topology protocol:

There are many types of logical topology protocols such as HDCL, Ethernet, and PPP.

High-level Data Link Control (HDLC):

It is a collection of data link layer communication protocols used to send data between network points or nodes. A frame is sent via the network to the destination, where its successful arrival is verified. It is a bit-oriented protocol that may be used for point-to-point and multipoint communications. Ethernet topology 802.3:

is a communication standard in networks used for transferring large amounts of data with a speed ranging from 10 Mbps to 100 Mbps.

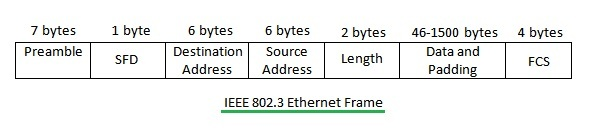
Ethernet lies in the lower layers of the Open Systems Interconnection (OSI) model. It facilitates the operation of physical and data link layers. The OSI model, which is composed of seven layers, illustrates how various communication protocols work together.

The Ethernet protocol uses a star topology or linear bus which is the foundation of the IEEE 802.3 standard. Also, Ethernet separates the Data Link layer into two different layers called the Logical Link Control layer & the Medium Access Control layer. The main reason to use Ethernet widely is, simple to understand, maintain, and implement, provides flexibility, and permits less cost network implementation. And the ethernet contains frame is a data packet on Layer 2 of the OSI model. A frame is “the unit of transmission in a link layer protocol and consists of a link-layer header followed by a packet.” Examples are Ethernet frames (maximum 1500 byte plus overhead).

A data packet on an Ethernet link is called an Ethernet frame. A frame begins with a preamble and with a starts frame delimiter. Following this, each Ethernet frame continues with an Ethernet header featuring destination and source MAC addresses. The middle section of the frame is payload data including any headers for other protocols (Internet Protocol) carried in the frame. The frame ends with a 32-bit cyclic redundancy check which is used to detect any corruption of data in transit.

Ethernet is a layer 1,2 most widely used LAN technology defined in IEEE 802.2 and 802.3 standards and supports data bandwidths of 10, 100, and 1000 Mbps.

Ethernet Frame:



Preamble:

It’s a part of the Ethernet frame it contains 0’s and 1’s the size of the Preamble is 7 bites. The preamble is the starting point for the frame. Its working gives the sender and the receiver to establish bit synchronization.

Destination Address:

The size of the destination address is 6-Byte, which contains the MAC address of the device for which the data is destined.

Source Address:

The size of the source address is 6-Byte, which contains the MAC address of the source device. The source address of the devices is always Unicast (individual address). The least significant bit of the first byte is always 0.

Length:

The size of the length is 2-Byte, which indicates the length of the entire Ethernet frame.

Data:

This is the place where actual data is inserted, also known as Payload. Both IP header and data will be inserted here if Internet Protocol is used over Ethernet. The maximum data present maybe if 1500 Bytes. In case data length is less than the minimum length i.e., 46 bytes, then padding 0’s is added to meet the minimum possible length.

Cyclic Redundancy Check (CRC):

The size of the CRC is 4 Bytes. This 4bytes contain a 32-bit hash code of data, which is generated over the Destination Address, Source Address, Length, and Data field. If the checksum computed by destination is not the same as the sent checksum value, the data received is corrupted.

Point to Point Protocol (PPP):

It is a data link layer protocol. It is used to encapsulate the layer 3 protocols and all the information available in the payload to be transmitted across the serial links. It is mainly used for communication between two devices.

It can be used over many types of physical networks such as serial cables, phone lines, and fiber optic links such as SONET. As the data link layer protocol is used to identify from where the transmission starts and ends. Also, there is no mac address or source address they replaced with tribble FFF.

**Part 4:**

Protocols:

Protocols are sets of rules that are used to show the way the devices communicate within a network.

The protocols that are used in the project: are DNS, DHCP, SMTP & POP3(EMAIL), FTP, SMB, and HTTPS. There are a lot of other protocols but the ones I chose were the best.

1- Domain Network System (DNS):

Definition: it’s a protocol that is used to turn the domain names into IP addresses, DNS servers make it possible for people to input normal words into their browsers, such as facebook.com, without having to write the IP address for every website every time. the DNS protocol works on the application layer. and works on port 53.

For more information:

When we enter a browser like a google and enter the name or URL of a website in the search engine. The browser will pass the name to the resolver.

The resolver will send the name to the DNS server.

The server will look up for IP address that belongs to this name.

After the server finds the IP address, it will be sent to the client.

2- Telnet protocol:

Telnet protocol is one of the oldest protocols. It was invented in 1969. This protocol provides two-way interactive communication compatibility for devices on the internet and local area networks. In 1969, the protocol helped the universities and the professors to log in to a university mainframe from any terminal in a building of large mainframe computers. This remote login saved researchers hours of walking each semester. This protocol works on port 23.

3-Dynamic Host Configuration Protocol (DHCP):

It’s a protocol that allows the (DHCP server) to dynamically distribute IP addressing and configuration information to clients. Normally the DHCP server provides the client with at least this basic information: 1-IP Address. 2-Subnet Mask. 3- Default gateway. 4-Domain name. 5- DNS server. It works on the application layer. Works on ports 67, and 68.

More Explanation:

A- DHCP discovers message:

this is the first message created between the client and the server. It is created by a client to check if there is a DHCP server network. The client will send a broadcast message to all the devices in the network to check if there is a DHCP server.

B- DHCP offer message:

The DHCP server will respond to client messages and will offer unused IP addresses and other TCP configuration information. This message is broadcasted by the server. If there is more than one DHCP server present in the network, then the client host will accept the first DHCP message it receives.

C-DHCP request message:

After the server offers the unused IP address and sends it to the client (device), the device responds to the DHCP server with a DHCP request packet to accept the offer.

D- Acknowledge message:

the server sends an acknowledge message to confirm that the device has that specific IP address and to define the amount of time that the device can use the address before getting a new one. If the server decides that the device cannot have the IP address, it will send a NACK (Not Acknowledge) message to the client.

4-Simple Mail Transfer Protocol (SMTP-Email):

It is an email protocol used for sending email messages from one email account to another via the internet or the mediums. Email protocols are sets of rules that let email clients and accounts easily exchange information, and SMTP is one of the most common ones alongside POP and IMAP. Also, it’s the only dedicated protocol for sending emails. Most email clients—including Outlook, Apple Mail, Gmail, and Yahoo Mail—rely on SMTP to send messages from a sender to a recipient. And there are two types of SMTP protocols, the first one is the End-To-End model, and the Store-and-forward model. Also, the SMTP protocols work on the Application layer. It works on port 25.

More Explanation: to be understandable let’s imagine that hamza@gmial.com sent a message to Sami@hotmail.com.

A-When hamza opens the website or the application then he clicked on compose to send a message, He writes a recipient email in the body of the message then he clicks on send.

B-Then the message will be downloaded on the SMTP server that belongs to Gmail to send again Hotmail server. The SMTP protocol covers and governs the communication between the two servers.

C-Then when the Hotmail after the handshaking between the two servers. The Gmail server will upload the message to the Hotmail server.

D-The Hotmail server by using the headers on the data that came from the Gmail server will search for the patient to send to him which he is Sami in this case.

E-When the server finds Sami’s IP address and uploads the data (message) to Sami’s mail then the server will close the communication between the two servers (the end of the protocol).

5-File Transfer Protocol (FTP):

It’s a protocol that helps to transfer files from a device (PC) to another device (PC), providing access to files or data or directories which are on other devices (PC) in the network. (it is used to push and pull files from the server). It works on ports 20 and 21.

It helps to transfer files from one computer to another by providing access to directories or folders on remote computers and allows software, data, and text file to be transferred between different kinds of computers. The end-user in the connection is known as the local host and the server which provides data is known as the remote host.

Extra explanation:

A- When one of the devices wants to share or get files from another device in the same network, the first device (sender) will ask the FTP server to establish a connection between the two devices, so they can communicate with each other.

B-When the FTP connection is established, there are two types of communication channels that are also established and are known as the command channel and the data channel. Those two commands help to push and pull the files (data).

C- After the two devices are connected, they must enter the user ID and password. If the user is registered with the server, then the user can access the files.

6-Hypertext Transfer Protocol Secure (HTTPS):

HTTPS is a secure type of HTTP. HTTP is a communication protocol used to connect to Web servers on the Internet or a local network (intranet). The primary function of HTTP is to establish a connection with the server and send HTML pages back to the user's browser. It is also used to download data from the server either to the browser or to any requesting applications that use HTTP. The HTTPS works on the application layer.

For more information:

A- When we want to browse the web, we open a browser like Google or Tour. Then the user inputs the app, or the website needed.

B-After entering the name of the website, the HTTPS server should get the IP address for it from the DNS server.

C- Once the browser identifies the IP address of the computer hosting the requested URL, it sends an HTTPS request.

D- Then the URL of the website will be sent to the HTTPS server to find the data that belongs to that IP address that the user entered it.

E- When the server finds the data, it will be sent to the user, if everything goes right, the website will be opened exactly as it should be.

7-Server Message Block (SMB):

It is a network protocol used by Windows-based computers that allow systems within the same network to share files. It allows computers (devices) connected to the same network or domain to access files from another local device.

SMB was originally developed for Windows, but it can be used by other platforms, including Unix and Mac OS X, using a software implementation called Samba.

**Part 5:**

There are many devices used in the structure of the network, and each device has a different use that benefits the network. such as routers, switches, PCs, servers, access points, printers, firewalls, hubs, and mediums.

Routers:

Routers are a layer 3 (Network layer) device used to forward packets from one network to another (to connect networks). It forwards the packet through one of its ports based on the destination IP address and the entry in the routing table. By using a routing table, it finds an optimized path between the source and destination network. And of course, there are many commands are used to configure the router, to know them we separate user EXEC mode, privileged EXEC mode, global configuration mode, and interface configuration mode. Examples used in the privileged mode like hostname and banner MOTD are used to write opening messages when someone opens the router. Example on commands is used on the interface mode as IP addresses for the router and no shutdown command to use. There are many types of routers that are based on connecting with other devices, Wireless routers, and Wired routers. And routers are based on a specific function that the router can do, such as Core router, Edge router, and Virtual router. The routers work on half duplexes.

Switches:

Switches are a better (updated) version from the HUBs. Its works on connecting all the devices, including computers, printers, and servers, in a small business network. The difference between the hub and the switch is when the hub takes the message from the device equine cast and sends it as a broadcast but when the switch takes the message, it takes the sent broadcast which means it is not secure. Switches work on the second layer (Datalink). And there are many types of switches, Modular switches vs. fixed-configuration switches, Modular switches, Modular switches, Modular switches, Smart switches, and Managed switches. And the switches work on full duplex

PC’s:

PCs are the main device in the network because people made the networks to share data and services, and to communicate.

A simple definition of PC: typical PCs include a system unit, monitor, keyboard, and mouse. Most PCs today also have a network or Internet connection, as well as ports for connecting peripheral devices, such as digital cameras, printers, scanners, speakers, external hard drives, and other components. All these services are used to make our lives easier and help us do our tasks faster and easier. And the PCs work on the application layer (layer 7). And the PCs work on full duplex.

Servers:

The servers will be explained later in the report, Servers work on layer 7 (application layer).

Access Point:

It is a type of hardware, such as a wireless router, that acts as a connection portal for other devices in the network. An access point connects wireless-enabled devices to a network. Also, it is about an access point as a standalone device that serves as a link between routers and local area networks (LANs) to enable device connections.

It would have various access points positioned on every floor or office corner to project a Wi-Fi connection to nearby devices. So, the network users get to enjoy a Wi-Fi connection wherever they move around in the building, and they can connect to the network by using the access point. Their systems would essentially just need to switch between access points to keep the link. The access point works on layer 2 (Data link layer).

Printer:

It is an output device that prints paper documents. It takes the electronic data stored on a computer or other device and generates a hard copy. There are a lot of types of printers like 3D printers AIO (all-in-one) printer, Dot matrix printer, Inkjet printer, Laser printer, and LED printer. Works on layer.

Fire Wall:

It is a network security device that monitors incoming and outgoing network traffic and permits, or blocks data packets based on a set of security rules. Its purpose is to establish a barrier between your internal network and incoming traffic from external sources (such as the internet) to block malicious traffic like viruses and hackers. Also, these types of the firewall as the (NGFW) next-generation firewall, proxy firewall, network address translation firewall (NAT), and Stateful multilayer inspection firewalls (SMLI). The last version of the firewall now works on layer 7, and the old version works on layer 4.

HUB:

It’s a network device that connects the devices in the network as computers, laptops, and servers. It works by getting the data and sending it by broadcasting it to all the devices that are connected to the HUB because of that it is called the dumb device. Also, the problem that HUBs have is they detect basic network errors, such as collisions, but having all information broadcasted to multiple ports is a security risk. In the past, HUBs were popular devices but now they are replaced with switches. And the HUB works on layer 1 (physical layer).

Mediums:

Medium is the cable that connects the device in the network like the medium connect between the router or the PCs or between the switches and the routers. And the mediums are layer 1 devices (physical layer). (The cables are not devices, but they are necessary equipment for the networks) Also, there are many types of mediums:

1. Coaxial Cable.
2. Twisted Pair Cable:
3. UTP (Unshielded Twisted Pair).
4. FTP (Foil Twisted Pair).

3. Fiber.

A close-up of a bracelet

Description automatically generated with low confidenceA close-up of a pen

Description automatically generated with low confidence

A picture containing pen

Description automatically generated Fiber cable. UTP cable.

A picture containing cosmetic

Description automatically generated

STP cable. Co-axil cable.

There are many types of the UTP cable based on the Band Width (BW) as Cat 3, Cat 5, Cat 5E, and Cat 6.

And the devices are used in the project are the routers, switches, PC’s, servers.

**Part 6:**

In this part of the assignment, I will talk about the servers and the types of servers, cost, performance optimization, infrastructure needs, usages, and hardware specification selection.

Definition of servers:

It is a machine or a computer program that provides data or functionality (service) for other machines (devices) or programs. We call the other devices or programs ‘clients.’ They are called servers because they serve the clients (they provide functionality). To be more specific the serves are terms that provide data for the clients. Also, their many types of servers but I'll separate them into two types, the first type is based on the functionalities that servers serve. Such as Web servers, FTP servers, Email servers, Real-Time Communication Servers, and so on. The second type of operating system works on serving such as widow’s servers, Linux servers, z/OS Unix System Services, Android servers, MacOS servers, and so on.

For example: When someone in the network opens a website, he\she will write the URL for the website the PC will ask for the website from the website's servers (HTTPS). For more information about the types of servers based on the functionality go back to part 1.3.

Now I will talk about 3 servers based on the operating system the Windows server, Linux server, and macOS server. Then I will do a comparison between the Windows server and the Linux server:

Windows server:

It is a group of operating systems designed by Microsoft that supports enterprise-level management, data storage, applications, and communications. Previous versions of Windows Server have focused on stability, security, networking, and various improvements to the file system. Also have included improvements to deployment technologies, as well as increased hardware support.

Linux server:

It is a family of UNIX-like operating systems that have all the features of UNIX. It is open source, facilitating multi-user, free-to-use, multi-process, multi-thread operations. However, Linux servers require more technical knowledge - from installation to maintenance and bug fixing. So, to know more about Linux we should look at the difference between Unix and Linux. Unix is a multi-tasking, multi-user operating system but is not free to use and is not open source. It was developed in 1969 by the Ken Thompson team at AT&T Bell Labs. It is widely used on servers and workstations.

MacOs server:

It is a server edition of Mac OS X developed by Apple Inc. It is based on the BSD-Unix derived operating system Apple Computer that acquired from NeXT to form the basis of AppleShare services provided server applications such as file and printer sharing and user management.

In the network that I am going to create, I prefer to choose Linux red hat operating system because of its open-source nature, customization, free-to-use, using commands for working, and easier of windows to control everything. Also, it's easy for security people to secure the network, and easier for programmers to create needed codes.

|  |  |
| --- | --- |
| The cost for licenses | For free. |
| Hardware specification selection | Needs CPU, RAM, storage. |
| Performance optimization | Easy to upgrade the server and the software. |
| infrastructure needs | Needs a room for the server. Also, needs a cooling conditioner and some thermometers and humidity. |
| Services | Linux allows users to select the packages for apps that they want to install in order to build the ideal environment.  Also, users can inspect and edit the operating system code. |

**Part 7:**

To know the inter-dependences of the hardware with relevant networking software. We should define the hardware and the software.

Hardware:

The context of technology refers to the physical elements (touchable elements) that make the computer or electronic system and everything else involved physically touchable. This includes the monitor, hard drive, memory, screen, CPU, and so on. Hardware works together to create the physical part of the PC (DEVICE).

Software:

It is a set of non-physical technology (set of instructions) programs used to control the physical part, used to operate a computer, and execute specific tasks. We can say software tells a computer how to function. (Set of computer programs that control all the parts in the pc).

Now we can answer how the hardware interdependencies with relevant networking software.

Hardware and software are mutually dependent on each other. Both must work together to make a computer produce a useful output. The software cannot be utilized without supporting hardware. Hardware without a set of programs to operate upon cannot be utilized and is useless. To get a particular job done on the computer, relevant software should be loaded into the hardware. (We can say that software is something inside the hardware).

Furthermore, if no hardware devices are supported, the software cannot be utilized, and if no instructions are provided, the hardware cannot be used and is rendered worthless.

To do a certain task on the computer, the appropriate software package must be installed into the hardware.

For example: If we want to use the mouse which is a physical part, we connect it to the computer, but we need software to start working together.

Another example:

We can say that the relationship between hardware and software is the same as the human body; hardware is the outer part of the body that represents the bones and the skin, and software is the inner part of the body that represents the organs. The organs give functions to the outer body to do, so both need each other to work.

Now we can understand the workstation:

First, what is the workstation?

A workstation is a computer that functions independently of the network. It handles its files and processing. Users' principal network interface and the resource on which they rely the most to get their jobs done.

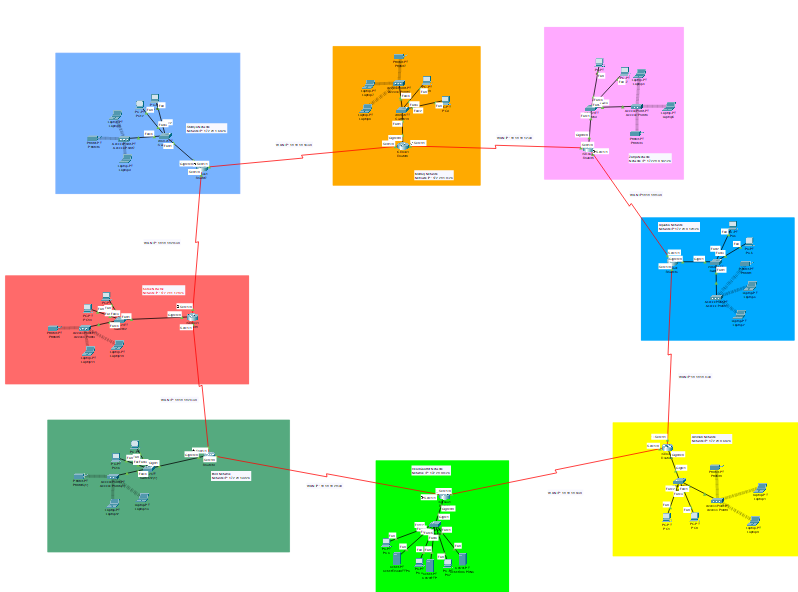
To know how the inter-dependences of the hardware with relevant networking software in the workstation. We should use an example:

Let’s say that we have a small network containing 2 routers and we want to send a packet from router one to router 2. And of course, both routers are working on layer 3.

The packet will be Encapsulate in the router and the router will give the data a header that contains the source IP address and the destination IP address (in our example router one will be the source and router 2 will be the destination) then will send the data to the right path will take the. Router two will check if the data is for him the router will take it and will be encapsulated then send it to the next destination IP address and router 2, will be the source IP address if it's not for the router will send it to the next router if there is another or will drop if there are not any other routers. That is how a router works

**Task 2:**

**Part 1.a:**

As I showed a good understanding of different aspects. My second task was to implement a packet tracer simulation of how I will connect the train tracks between the cities of Jordan, I started with a picture of all the networks that I made:

This is the biggest WAN network in the project, and it contains 8 LANs networks, starting with the headquarter then Amman remote office then Aqaba remote office then Zarqa remote office then Mafraq remote office then Shidiya remote office last but not least Karak remote office last one is Irbid remote office. The physical topology is the hybrid topology for the biggest WAN but for the WAN which is between the routers I used Ring topology with HDLC logical topology protocol for LAN’s I used extend Star topology with Ethernet logical topology protocol.

The protocol that I used between the small WAN (for example between Amman remote office and Karak remote office) is OSPF with a 0.0.0.63 wild card for the LANs. And 0.0.0.6 wild card for the WAN’s networks. And of course, all the IPs in the network work on IP address version 4.

Why OSPF (Open shortest path first)?

Because OSPF has fast convergence and has the option for tuning more metric values, you can divide your network into different OSPF areas. OSPF also supports equal-cost multipath load balancing and neighbor authentication. And because OSPF finds the shortest path among the different areas using the Dijkstra algorithm. Also, we can expand the network whenever we want. (No maximum network or devices). And because the OSPF protocol minimizes the overhead and OSPF supports interface-based plaintext and md5 authentication so, that means good security.

All network has one website that works on HTTPS which is https://eis.jnr.com.jo/. (Any website that will be added in the future will work on HTTPS because HTTP is not working in this network.).

Also, the domain name for the network is eis.jnr.com.jo

In the end, I just want to mention that the default root in the network is in the Head Quarter network

**Part 1.b:**

**The subnetting for the IP’s:**

LAN’s Networks:

172.28.0.0/16

255.255.0.0

2^n=64

N=6

172.28.00000000.00|000000

Subnet mask: 255.255.255.192

Wild card: 0.0.0.63

|  |  |  |  |
| --- | --- | --- | --- |
| N.W | F.H | L.H | B.C |
| 172.28.0.0 \26 | 172.28.0.1 \26 | 172.28.0.62 \26 | 172.28.0.63\26 |

172.28.00000000.01|000000

255.255.255.192

0.0.0.63

|  |  |  |  |
| --- | --- | --- | --- |
| N.W | F.H | L.H | B.C |
| 172.28.0.64\26 | 172.28.0.65 \26 | 172.28.0.126 \26 | 172.28.0.127\26 |

172.28.00000000.10|000000

255.255.255.192

0.0.0.63

|  |  |  |  |
| --- | --- | --- | --- |
| N.W | F.H | L.H | B.C |
| 172.28.0.128\26 | 172.28.0.129 \26 | 172.28.0.190 \26 | 172.28.0.191\26 |

172.28.00000000.11|000000

255.255.255.192

0.0.0.63

|  |  |  |  |
| --- | --- | --- | --- |
| N.W | F.H | L.H | B.C |
| 172.28.0.192\26 | 172.28.0.193 \26 | 172.28.0.254 \26 | 172.28.0.255\26 |

172.28.00000001.00|000000

255.255.255.192

0.0.0.63

|  |  |  |  |
| --- | --- | --- | --- |
| N.W | F.H | L.H | B.C |
| 172.28.1.0\26 | 172.28.1.1 \26 | 172.28.1.62 \26 | 172.28.1.63\26 |

172.28.00000001.01|000000

255.255.255.192

0.0.0.63

|  |  |  |  |
| --- | --- | --- | --- |
| N.W | F.H | L.H | B.C |
| 172.28.1.64\26 | 172.28.1.65\26 | 172.28.1.190\26 | 172.28.1.191\26 |

172.28.00000001.10|000000

255.255.255.192

0.0.0.63

|  |  |  |  |
| --- | --- | --- | --- |
| N.W | F.H | L.H | B.C |
| 172.28.1.128\26 | 172.28.1.129\26 | 172.28.1.126\26 | 172.28.1.127\26 |

172.28.00000001.11|000000

255.255.255.192

0.0.0.63

|  |  |  |  |
| --- | --- | --- | --- |
| N.W | F.H | L.H | B.C |
| 172.28.1.192\26 | 172.28.1.193\26 | 172.28.0.254\26 | 172.28.1.255\26 |

WAN’s Networks:

18.18.18.0/24

255.255.255.0

2^n=2 n=2

Wild card: 0.0.0.3

SM: 255.255.255.252

18.18.18.000000|00/30 = 18.18.18.0

18.18.18.000001|00/30 = 18.18.18.4

18.18.18.000010|00/30 = 18.18.18.8

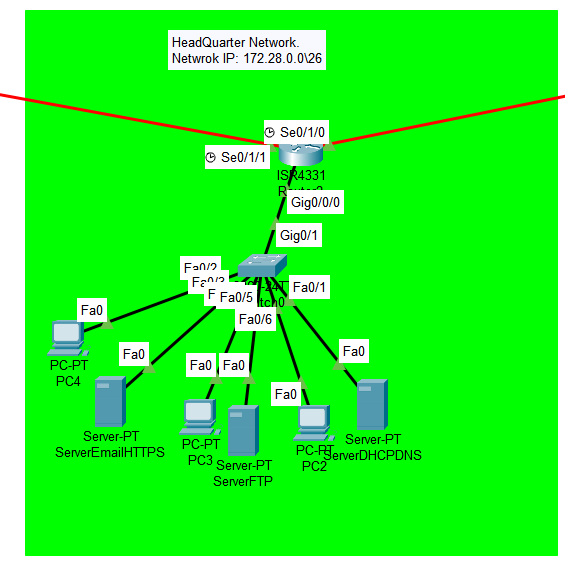
18.18.18.000011|00/30 = 18.18.18.12

18.18.18.000100|00/30 18.18.18.16

18.18.18.000101|00/30 18.18.18.20

18.18.18.000110|00/30 18.18.18.24

18.18.18.000111|00/30=18.18.18.28

The Headquarter network: The IP address for the network is 172.28.0.0\26 and the default gateway for the network is 172.28.0.1\26

It’s the central data in our project it contains 3 servers the first server for DNS and DHCP, second for FTP, and the third one for the Email and the HTTPS. I put DNS and DHCP together because both needs each other. FTP alone in a server because the data needs a huge space for it. HTTPS and Email together because both do not need a huge space as the FTP. The DNS DHCP server IP is 172.28.0.2\26 with 255.255.255.192 SM, the FTP server IP address is 172.28.0.3 with 255.255.255.192 SM, and the Email HTTPS server is 172.28.0.4\26 with 255.255.255.192 SM. All the servers work on static IP address.

Also, the network contains 3 administrators (3 PC’s) those 3 administrators can write, read, list, delete, and rename in the FTP server. And the network has one switch and one router. The router has IP address on gigabit Ethernet which is have 172.28.0.1\26 IP address with 255.255.255.192 SM. Also, the router has 2 serials the first one is se0/1/0 with 18.18.18.1\30 IP address and with 255.255.255.252 SM. The second serial is se0/1/1 with 18.18.18.30\30 IP address with 255.255.255.252 SM. The physical topology used in this network is extend Star topology with ethernet topology for the logical topology protocol.

All the administrators work on DHCP, the first (PC2) administrator has 172.28.0.6\26 IP address with 255.255.255.192 SM, second administrator (PC3) has 172.28.0.9\26 IP address with 255.255.255.192 SM, and the third administrator (PC4) has 172.28.0.7\26 IP address with 255.255.255.192 SM.

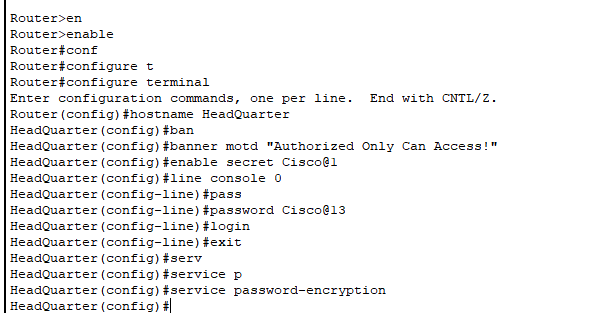
The FTP username and password for the first administrator (PC2) is PC2 for the username and Cisco@22 for the password. The FTP username and password for the second administrator (PC3) is PC2 for the username and Cisco@33 for the password. The FTP username and password for the third administrator (PC4) is PC2 for the username and Cisco@44 for the password. For all the 3 administrators can write, read, rename, list, and delete from the FTP server.

The email address and username for the first administrator (PC2) is [pc2@eis.jnr.com.jo](mailto:pc2@eis.jnr.com.jo) for the email address and pc@2 for the password. The email address and username for the second administrator (PC3) is [pc3@eis.jnr.com.jo](mailto:pc3@eis.jnr.com.jo) for the email address and pc@3 for the password. The email address and username for the third administrator (PC4) is [pc4@eis.jnr.com.jo](mailto:pc4@eis.jnr.com.jo) for the email address and pc@4 for the password.

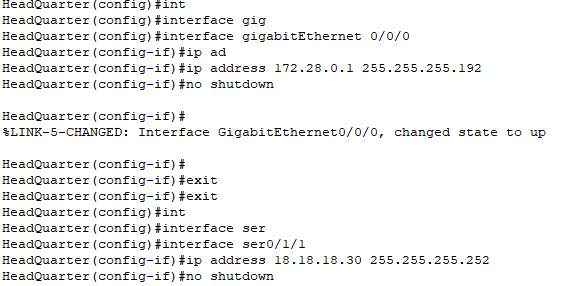
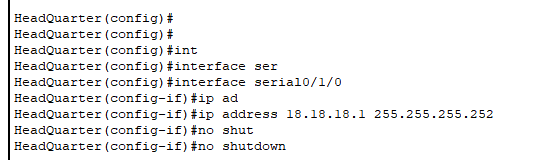
|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | PC2 | PC3 | PC4 | DNS,DHCP server | FTP server | Email, HTTPS server |
| IP address: | 172.28.0.6\26 | 172.28.0.9\26 | 172.28.0.7\26 | 172.28.0.2\26 | 172.28.0.3\26 | 172.28.0.4\26 |
| Subnet Mask: | 255.255.255.192 | 255.255.255.192 | 255.255.255.192 | 255.255.255.192 | 255.255.255.192 | 255.255.255.192 |
| DHCP or Static: | DHCP | DHCP | DHCP | Static | Static | Static |
| FTP user: | Pc2 | Pc3 | Pc4 | ---------------------- | ---------------------- | ---------------------- |
| FTP pass: | Cisco@22 | Cisco@33 | Cisco@44 | ---------------------- | ---------------------- | ---------------------- |
| Email user: | Pc2@eis.jnr.com.jo | Pc3@eis.jnr.com.jo | Pc4@eis.jnr.com.jo | ---------------------- | ---------------------- | ---------------------- |
| Email pass: | pc@2 | pc@3 | Pc@4 | ---------------------- | ---------------------- | ---------------------- |

Configuration for the router: First of all I have to mention that there is line console 0 password which is Cisco@13 and it is encrypted with service password-encryption. Also, there is a enable secret which is Cisco@1. The hostname for the route is HeadQuarter and there is a Banner which is “Authorized Only Can Access!”.

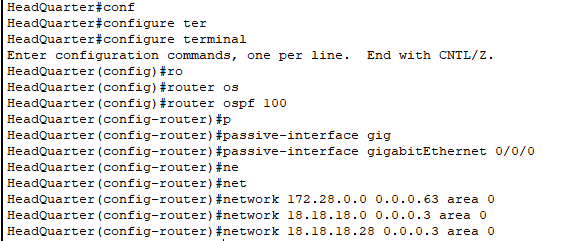
The configuration for these things:



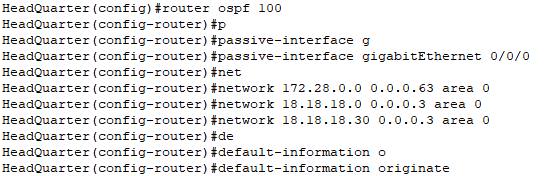
The configuration for the serials and the gigabit Ethernet:

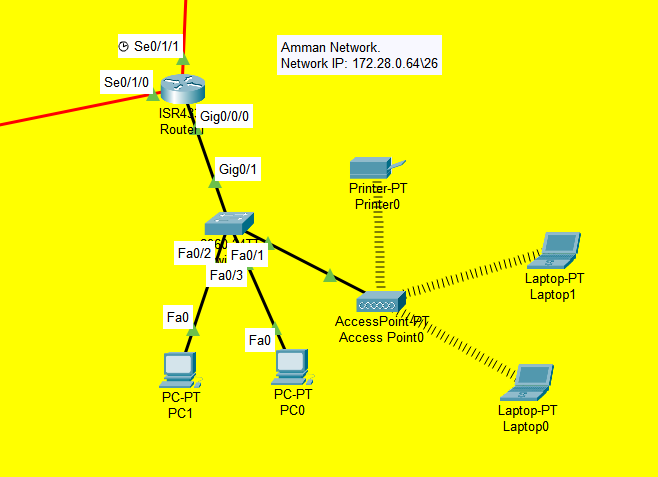
 

The configuration for the OSPF:



The default root configuration:





Amman Network: The IP address for the network is 172.28.0.64\26 and the default gateway for the network is 172.28.0.65\26.

This is the first remote office I create it was in Amman. The physical topology used in the network is extended star and the logical topology protocol is ethernet.

It’s included 2 PC and one of these PC’s is a manger in Amman office. Also, there are 2 laptops connected wireless and one printer connected wireless. And there is one switch and one router connected with a switch in gigabit Ethernet with 172.28.0.65\26 IP address and 255.255.255.192 subnet mask. And 2 serials are connected in the router se0/1/1 with 18.18.18.5\30 IP address and 255.255.255.252 subnet mask, se0/1/0 with 18.18.18.2\30 and 255.255.255.252 subnet mask.

The PC’s IP’s, for the first one (PC0) is 172.28.0.68\26 and 255.255.255.192 subnet mask, for the second one and the manger (PC1) is 172.28.0.65\26 and 255.255.255.192 subnet mask. PC1 can write read and list in the FTP server but PC0 can write and read only.

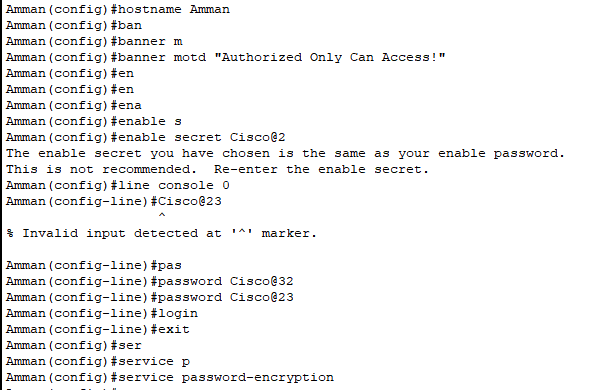
Also, there is access point to connect the laptops and printer wirelessly. The IP address for laptop0 is 172.28.0.71\26 and 255.255.255.192 subnet mask, laptop1 IP address is 172.28.0.70\26 and 255.255.255.192 subnet mask. The IP address for the printer is 172.28.0.66\26.

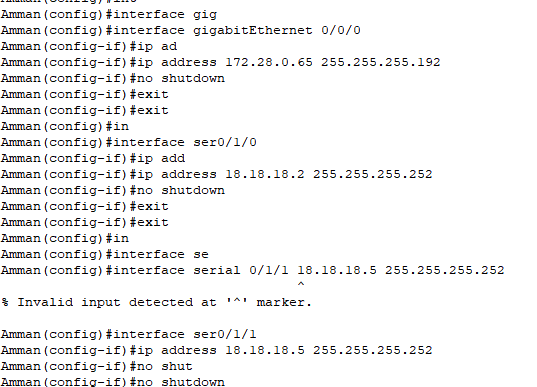
The username for the Access point is AmmanAccessPoint and the password is Cisco@231

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | PC0 | PC1 | Lapto0 | Laptop1 | Printer |
| IP address: | 172.28.0.68\26 | 172.28.0.65\26 | 172.28.0.71\26 | 172.28.0.70\26 | 172.28.0.66\26 |
| Subnet Mask: | 255.255.255.192 | 255.255.255.192 | 255.255.255.192 | 255.255.255.192 | 255.255.255.192 |
| DHCP or Static: | DHCP | DHCP | DHCP | DHCP | Static |
| FTP user: | Pc0 | Pc1 | Laptop0 | Laptop1 | ---------------------- |
| FTP pass: | Cisco@ | Cisco@1 | Cisco@ | Cisco@ | ---------------------- |
| Email user: | Pc0@eis.jnr.com.jo | Pc1@eis.jnr.com.jo | Laptop0@eis.jnr.com.jo | Laptop1@eis.jnr.com.jo | ---------------------- |
| Email pass: | pc@0 | pc@1 | laptop@0 | laptop@1 | ---------------------- |

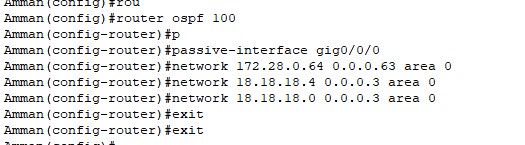
Configuration for the router: First of all, I have to mention that there is line console 0 password which is Cisco@23 and it is encrypted with service password-encryption. Also, there is a enable secret which is Cisco@2. The hostname for the route is Amman and there is a Banner which is “Authorized Only Can Access!”.

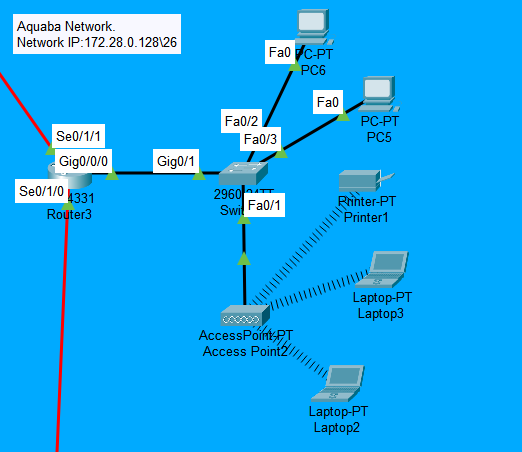
The configuration for the line console 0 password, enable password, hostname, and banner:



The configuration for the serials and the gigabit Ethernet:

The configuration for the OSPF:





Aquaba Network: The IP address for the network is 172.28.0.128\26 and the default gateway for the network is 172.28.0.129\26.

The physical topology used in the network is extended star and the logical topology protocol is ethernet.

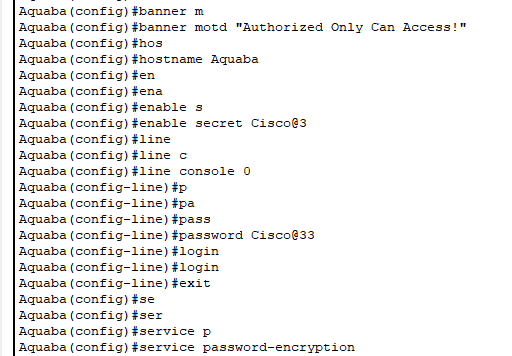
It’s included 2 PC and one of these PC’s is a manger in Aquaba office. Also, there are 2 laptops connected wireless and one printer connected wireless. And there is one switch and one router connected with a switch in gigabit Ethernet with 172.28.0.129\26 IP address and 255.255.255.192 subnet mask. And 2 serials are connected in the router se0/1/1 with 18.18.18.9\30 IP address and 255.255.255.252 subnet mask, se0/1/0 with 18.18.18.6\30 and 255.255.255.252 subnet mask.

The PC’s IP’s, for the first one (PC5) is 172.28.0.132\26 and 255.255.255.192 subnet mask, for the second one and the manger (PC6) is 172.28.0.131\26 and 255.255.255.192 subnet mask.

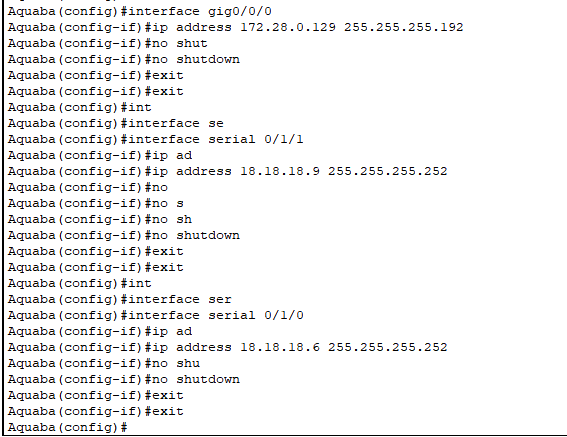
Also, there is access point to connect the laptops and printer wirelessly. The IP address for laptop2 is 172.28.0.133\26 and 255.255.255.192 subnet mask, laptop3 IP address is 172.28.0.134\26 and 255.255.255.192 subnet mask. The IP address for the printer is 172.28.0.130\26. The username for the Access point is AquabaAccessPoint and the password is Cisco@331

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | PC5 | PC6 | Laptop2 | Laptop3 | Printer |
| IP address: | 172.28.0.132\26 | 172.28.0.131\26 | 172.28.0.133\26 | 172.28.0.134\26 | 172.28.0.130\26 |
| Subnet Mask: | 255.255.255.192 | 255.255.255.192 | 255.255.255.192 | 255.255.255.192 | 255.255.255.192 |
| DHCP or Static: | DHCP | DHCP | DHCP | DHCP | Static |
| FTP user: | Pc5 | Pc6 | Laptop2 | Laptop3 | ---------------------- |
| FTP pass: | Cisco@5 | Cisco@ | Cisco@ | Cisco@ | ---------------------- |
| Email user: | Pc5@eis.jnr.com.jo | Pc6@eis.jnr.com.jo | Laptop2@eis.jnr.com.jo | Laptop3@eis.jnr.com.jo | ---------------------- |
| Email pass: | pc@5 | pc@6 | laptop@2 | laptop@3 | ---------------------- |

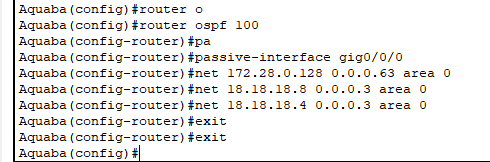
Configuration for the router: First of all, I have to mention that there is line console 0 password which is Cisco@33 and it is encrypted with service password-encryption. Also, there is a enable secret which is Cisco@3. The hostname for the route is Aquaba and there is a Banner which is “Authorized Only Can Access!”.

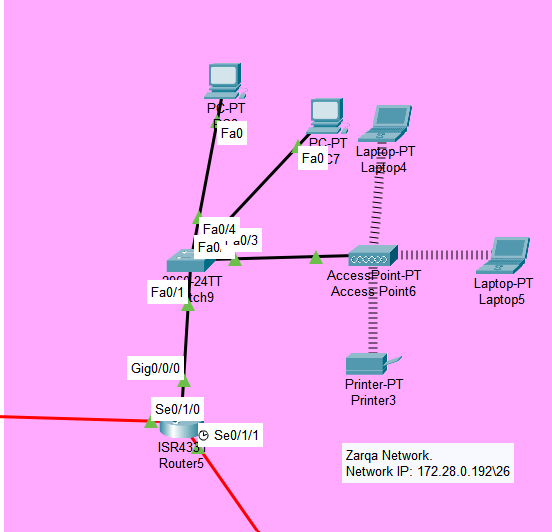
The configuration for the line console 0 password, enable password, hostname, and banner: 

The configuration for the serials and the gigabit Ethernet:



The configuration for the OSPF:





Zarqa Network: The IP address for the network is 172.28.0.192\26 and the default gateway for the network is 172.28.0.193\26.

The physical topology used in the network is extended star and the logical topology protocol is ethernet.

It’s included 2 PC and one of these PC’s is a manger in Zarqa office. Also, there are 2 laptops connected wireless and one printer connected wireless. And there is one switch and one router connected with a switch in gigabit Ethernet with 172.28.0.193\26 IP address and 255.255.255.192 subnet mask. And 2 serials are connected in the router se0/1/1 with 18.18.18.10\30 IP address and 255.255.255.252 subnet mask, se0/1/0 with 18.18.18.13\30 and 255.255.255.252 subnet mask.

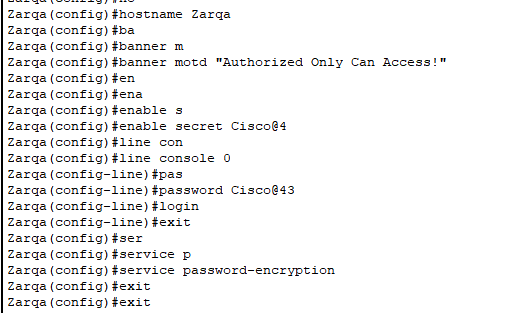
The PC’s IP’s, for the first one and the manger (PC7) is 172.28.0.195\26 and 255.255.255.192 subnet mask, for the second one (PC8) is 172.28.0.196\26 and 255.255.255.192 subnet mask.

Also, there is access point to connect the laptops and printer wirelessly. The IP address for laptop4 is 172.28.0.198\26 and 255.255.255.192 subnet mask, laptop5 IP address is 172.28.0.197\26 and 255.255.255.192 subnet mask. The IP address for the printer is 172.28.0.194\26. The username for the Access point is ZarqaAccessPoint and the password is Cisco@431

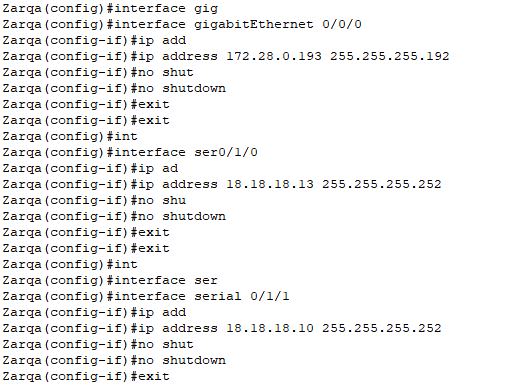
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | PC7 | PC8 | Laptop4 | Laptop5 | Printer |
| IP address: | 172.28.0.195\26 | 172.28.0.196\26 | 172.28.0.198\26 | 172.28.0.197\26 | 172.28.0.194\26 |
| Subnet Mask: | 255.255.255.192 | 255.255.255.192 | 255.255.255.192 | 255.255.255.192 | 255.255.255.192 |
| DHCP or Static: | DHCP | DHCP | DHCP | DHCP | Static |
| FTP user: | Pc7 | Pc6 | Laptop4 | Laptop5 | ---------------------- |
| FTP pass: | Cisco@7 | Cisco@ | Cisco@ | Cisco@ | ---------------------- |
| Email user: | Pc7@eis.jnr.com.jo | Pc8@eis.jnr.com.jo | Laptop4@eis.jnr.com.jo | Laptop5@eis.jnr.com.jo | ---------------------- |
| Email pass: | pc@7 | pc@8 | laptop@4 | laptop@5 | ---------------------- |

Configuration for the router: First of all, I have to mention that there is line console 0 password which is Cisco@43 and it is encrypted with service password-encryption. Also, there is a enable secret which is Cisco@4. The hostname for the route is Zarqa and there is a Banner which is “Authorized Only Can Access!”.

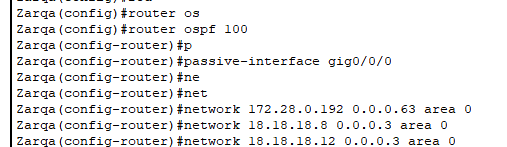
The configuration for the line console 0 password, enable password, hostname, and banner:



The configuration for the serials and the gigabit Ethernet:



The configuration for the OSPF:



A picture containing map

Description automatically generated

Mafraq Network: The IP address for the network is 172.28.1.0\26 and the default gateway for the network is 172.28.1.1\26.

The physical topology used in the network is extended star and the logical topology protocol is ethernet.

It’s included 2 PC and one of these PC’s is a manger in Maraq office. Also, there are 2 laptops connected wireless and one printer connected wirelessly to. And there is one switch and one router connected with a switch in gigabit Ethernet with 172.28.1.1\26 IP address and 255.255.255.192 subnet mask. And 2 serials are connected in the router se0/1/1 with 18.18.18.14\30 IP address and 255.255.255.252 subnet mask, se0/1/0 with 18.18.18.17\30 and 255.255.255.252 subnet mask.

The PC’s IP’s, for the first one and the manger (PC9) is 172.28.1.4\26 and 255.255.255.192 subnet mask, for the second one (PC10) is 172.28.1.7\26 and 255.255.255.192 subnet mask.

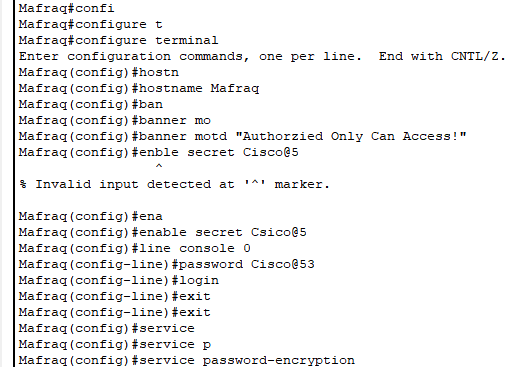
Also, there is access point to connect the laptops and printer wirelessly. The IP address for laptop6 is 172.28.1.6\26 and 255.255.255.192 subnet mask, laptop7 IP address is 172.28.1.5\26 and 255.255.255.192 subnet mask. The IP address for the printer is 172.28.1.2\26.

The username for the Access point is MafraqAccessPoint and the password is Cisco@531

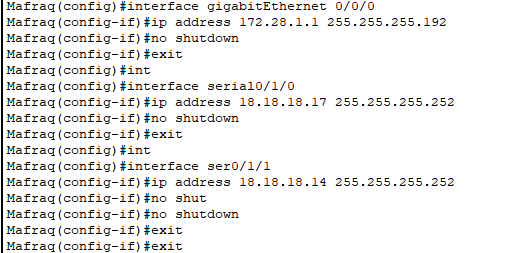
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | PC9 | PC10 | Laptop6 | Laptop7 | Printer |
| IP address: | 172.28.1.4\26 | 172.28.1.7\26 | 172.28.1.6\26 | 172.28.1.5\26 | 172.28.1.2\26 |
| Subnet Mask: | 255.255.255.192 | 255.255.255.192 | 255.255.255.192 | 255.255.255.192 | 255.255.255.192 |
| DHCP or Static: | DHCP | DHCP | DHCP | DHCP | Static |
| FTP user: | Pc9 | Pc10 | Laptop6 | Laptop7 | ---------------------- |
| FTP pass: | Cisco@9 | Cisco@ | Cisco@ | Cisco@ | ---------------------- |
| Email user: | Pc9@eis.jnr.com.jo | Pc10@eis.jnr.com.jo | Laptop6@eis.jnr.com.jo | Laptop7@eis.jnr.com.jo | ---------------------- |
| Email pass: | pc@9 | pc@10 | laptop@6 | laptop@7 | ---------------------- |

Configuration for the router: First of all, I have to mention that there is line console 0 password which is Cisco@53 and it is encrypted with service password-encryption. Also, there is a enable secret which is Cisco@5. The hostname for the route is Mafraq and there is a Banner which is “Authorized Only Can Access!”.

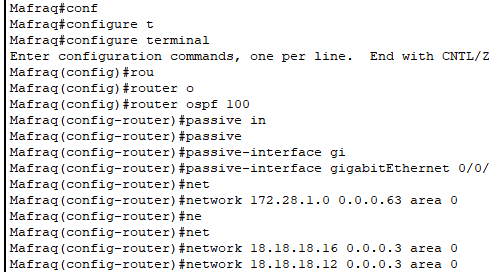
The configuration for the line console 0 password, enable password, hostname, and banner:



The configuration for the serials and the gigabit Ethernet:



The configuration for the OSPF:



Diagram

Description automatically generated

Shidiya Network: The IP address for the network is 172.28.1.64\26 and the default gateway for the network is 172.28.1.65\26.

The physical topology used in the network is extended star and the logical topology protocol is ethernet.

It’s included 2 PC and one of these PC’s is a manger in Shidiya office. Also, there are 2 laptops connected wireless and one printer connected wirelessly to. And there is one switch and one router connected with a switch in gigabit Ethernet with 172.28.1.65\26 IP address and 255.255.255.192 subnet mask. And 2 serials are connected in the router se0/1/1 with 18.18.18.18\30 IP address and 255.255.255.252 subnet mask, se0/1/0 with 18.18.18.21\30 and 255.255.255.252 subnet mask.

The PC’s IP’s, for the first one and the manger (PC11) is 172.28.1.67\26 and 255.255.255.192 subnet mask, for the second one (PC12) is 172.28.1.68\26 and 255.255.255.192 subnet mask.

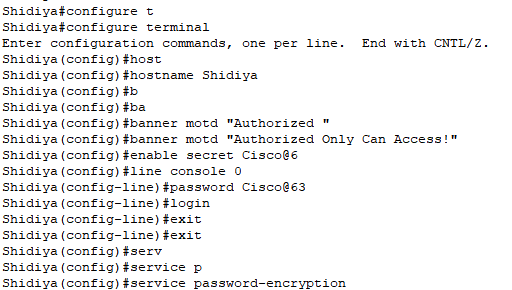
Also, there is access point to connect the laptops and printer wirelessly. The IP address for laptop8 is 172.28.1.70\26 and 255.255.255.192 subnet mask, laptop9 IP address is 172.28.1.69\26 and 255.255.255.192 subnet mask. The IP address for the printer is 172.28.1.2\26.

The username for the Access point is ShidiyaAccessPoint and the password is Cisco@631

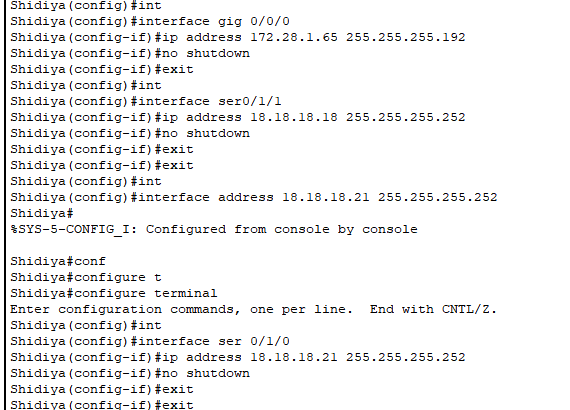
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | PC11 | PC12 | Laptop8 | Laptop9 | Printer |
| IP address: | 172.28.1.67\26 | 172.28.1.68\26 | 172.28.1.70\26 | 172.28.1.69\26 | 172.28.1.66\26 |
| Subnet Mask: | 255.255.255.192 | 255.255.255.192 | 255.255.255.192 | 255.255.255.192 | 255.255.255.192 |
| DHCP or Static: | DHCP | DHCP | DHCP | DHCP | Static |
| FTP user: | Pc11 | Pc12 | Laptop6 | Laptop9 | ---------------------- |
| FTP pass: | Cisco@11 | Cisco@ | Cisco@ | Cisco@ | ---------------------- |
| Email user: | Pc11@eis.jnr.com.jo | Pc12@eis.jnr.com.jo | Laptop8@eis.jnr.com.jo | Laptop9@eis.jnr.com.jo | ---------------------- |
| Email pass: | pc@11 | pc@12 | laptop@8 | laptop@9 | ---------------------- |

Configuration for the router: First of all, I have to mention that there is line console 0 password which is Cisco@63 and it is encrypted with service password-encryption. Also, there is a enable secret which is Cisco@6. The hostname for the route is Mafraq and there is a Banner which is “Authorized Only Can Access!”.

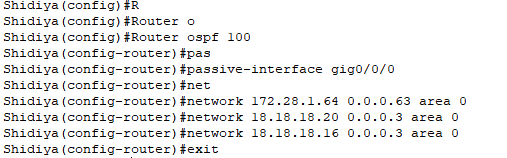
The configuration for the line console 0 password, enable password, hostname, and banner:



The configuration for the serials and the gigabit Ethernet:



The configuration for the OSPF:



Diagram

Description automatically generated

Karak Network: The IP address for the network is 172.28.1.128\26 and the default gateway for the network is 172.28.1.129\26.

The physical topology used in the network is extended star and the logical topology protocol is ethernet.

It’s included 2 PC and one of these PC’s is a manger in Karak office. Also, there are 2 laptops connected wireless and one printer connected wirelessly to. And there is one switch and one router connected with a switch in gigabit Ethernet with 172.28.1.129\26 IP address and 255.255.255.192 subnet mask. And 2 serials are connected in the router se0/1/1 with 18.18.18.25\30 IP address and 255.255.255.252 subnet mask, se0/1/0 with 18.18.18.22\30 and 255.255.255.252 subnet mask.

The PC’s IP’s, for the first one and the manger (PC13) is 172.28.1.131\26 and 255.255.255.192 subnet mask, for the second one (PC14) is 172.28.1.134\26 and 255.255.255.192 subnet mask.

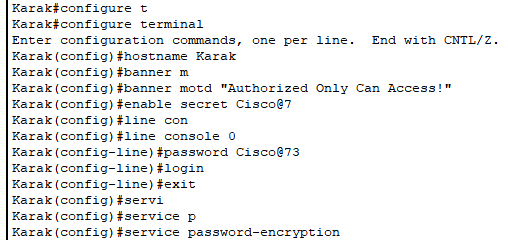
Also, there is access point to connect the laptops and printer wirelessly. The IP address for laptop10 is 172.28.1.132\26 and 255.255.255.192 subnet mask, laptop11 IP address is 172.28.1.134\26 and 255.255.255.192 subnet mask. The IP address for the printer is 172.28.1.130\26.

The username for the Access point is KarakAccessPoint and the password is Cisco@731

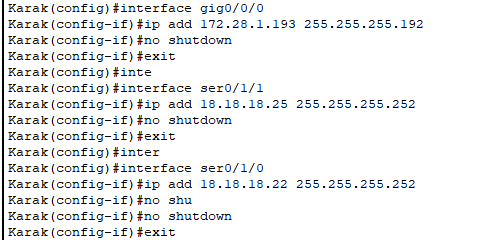
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | PC13 | PC14 | Laptop10 | Laptop11 | Printer |
| IP address: | 172.28.1.131\26 | 172.28.1.134\26 | 172.28.1.132\26 | 172.28.1.134\26 | 172.28.1.130\26 |
| Subnet Mask: | 255.255.255.192 | 255.255.255.192 | 255.255.255.192 | 255.255.255.192 | 255.255.255.192 |
| DHCP or Static: | DHCP | DHCP | DHCP | DHCP | Static |
| FTP user: | Pc13 | Pc14 | Laptop10 | Laptop11 | ---------------------- |
| FTP pass: | Cisco@13 | Cisco@ | Cisco@ | Cisco@ | ---------------------- |
| Email user: | Pc13@eis.jnr.com.jo | Pc14@eis.jnr.com.jo | Laptop10@eis.jnr.com.jo | Laptop11@eis.jnr.com.jo | ---------------------- |
| Email pass: | pc@13 | pc@14 | laptop@10 | laptop@11 | ---------------------- |

Configuration for the router: First of all, I have to mention that there is line console 0 password which is Cisco@73 and it is encrypted with service password-encryption. Also, there is a enable secret which is Cisco@7. The hostname for the route is Mafraq and there is a Banner which is “Authorized Only Can Access!”.

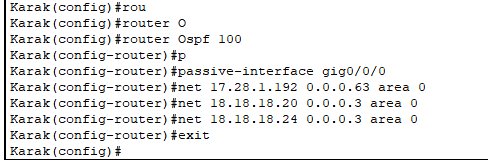
The configuration for the line console 0 password, enable password, hostname, and banner:

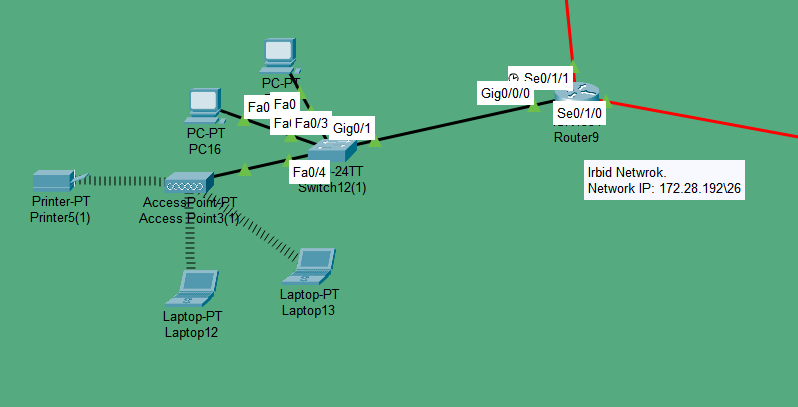


The configuration for the serials and the gigabit Ethernet:



The configuration for the OSPF:





Irbid Network: The IP address for the network is 172.28.1.192\26 and the default gateway for the network is 172.28.1.193\26.

The physical topology used in the network is extended star and the logical topology protocol is ethernet.

It’s included 2 PC and one of these PC’s is a manger in Irbid office. Also, there are 2 laptops connected wireless and one printer connected wirelessly to. And there is one switch and one router connected with a switch in gigabit Ethernet with 172.28.1.193\26 IP address and 255.255.255.192 subnet mask. And 2 serials are connected in the router se0/1/1 with 18.18.18.26\30 IP address and 255.255.255.252 subnet mask, se0/1/0 with 18.18.18.29\30 and 255.255.255.252 subnet mask.

The PC’s IP’s, for the first one and the manger (PC15) is 172.28.1.195\26 and 255.255.255.192 subnet mask, for the second one (PC16) is 172.28.1.196\26 and 255.255.255.192 subnet mask.

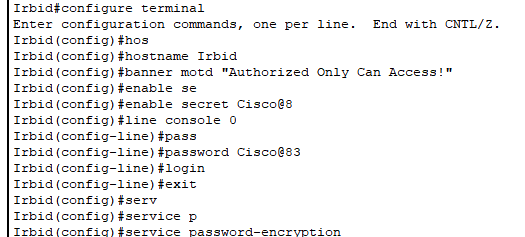
Also, there is access point to connect the laptops and printer wirelessly. The IP address for laptop12 is 172.28.1.197\26 and 255.255.255.192 subnet mask, laptop13 IP address is 172.28.1.198\26 and 255.255.255.192 subnet mask. The IP address for the printer is 172.28.1.194\26.

The username for the Access point is IrbidAccessPoint and the password is Cisco@831

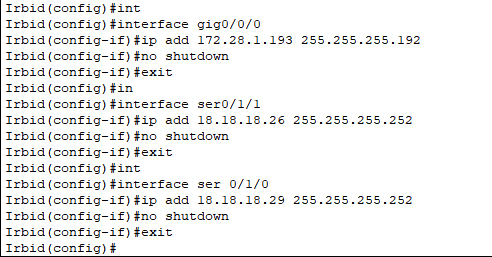
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | PC15 | PC16 | Laptop12 | Laptop13 | Printer |
| IP address: | 172.28.1.195\26 | 172.28.1.196\26 | 172.28.1.197\26 | 172.28.1.198\26 | 172.28.1.194\26 |
| Subnet Mask: | 255.255.255.192 | 255.255.255.192 | 255.255.255.192 | 255.255.255.192 | 255.255.255.192 |
| DHCP or Static: | DHCP | DHCP | DHCP | DHCP | Static |
| FTP user: | Pc15 | Pc16 | Laptop12 | Laptop13 | ---------------------- |
| FTP pass: | Cisco@15 | Cisco@ | Cisco@ | Cisco@ | ---------------------- |
| Email user: | Pc15@eis.jnr.com.jo | Pc16@eis.jnr.com.jo | Laptop12@eis.jnr.com.jo | Laptop13@eis.jnr.com.jo | ---------------------- |
| Email pass: | pc@15 | pc@16 | laptop@12 | laptop@13 | ---------------------- |

Configuration for the router: First of all, I have to mention that there is line console 0 password which is Cisco@83 and it is encrypted with service password-encryption. Also, there is a enable secret which is Cisco@8. The hostname for the route is Mafraq and there is a Banner which is “Authorized Only Can Access!”.

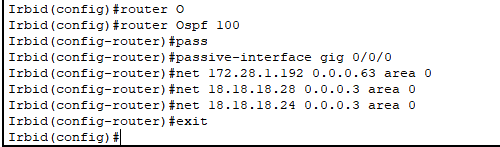
The configuration for the line console 0 password, enable password, hostname, and banner:



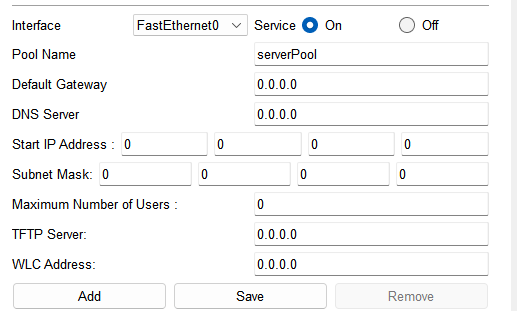
The configuration for the serials and the gigabit Ethernet:



The configuration for the OSPF:



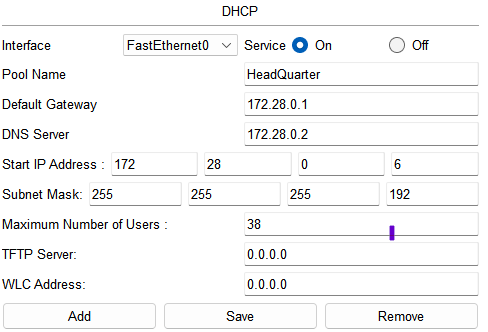
The configuration for DHCP server:



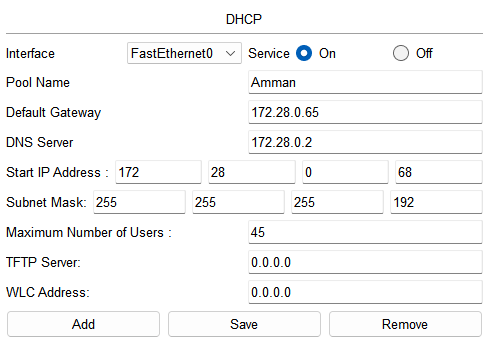
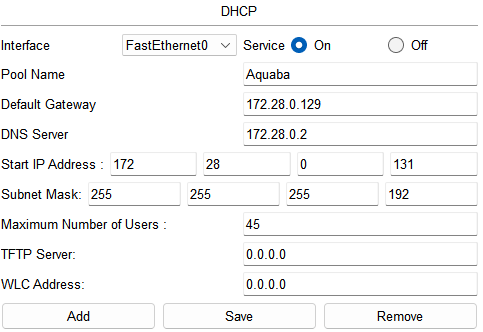
1-First of all we should add server pool with 0 start IP, 0 subnet mask, 0 default gateway, 0 DNS server, and 0 maximum number of users. The IP address for DHCP server is 172.28.0.2\26

2- Then add the networks we have in the WAN.

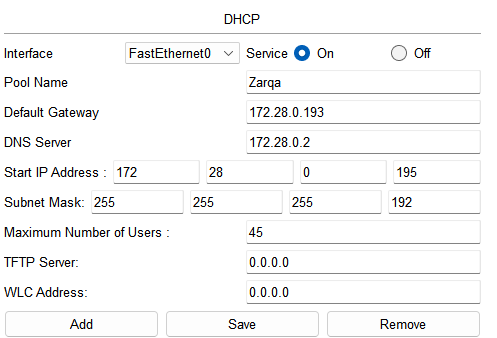
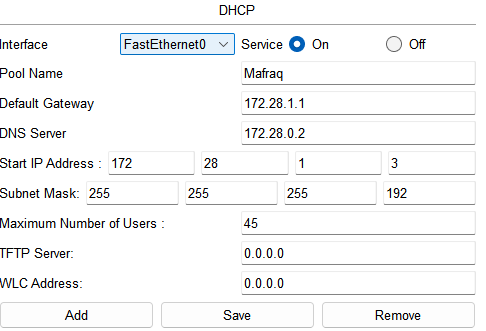
3- we start with headquarter then Amman remote office and so on.



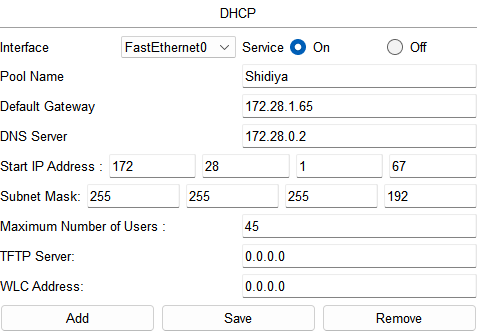
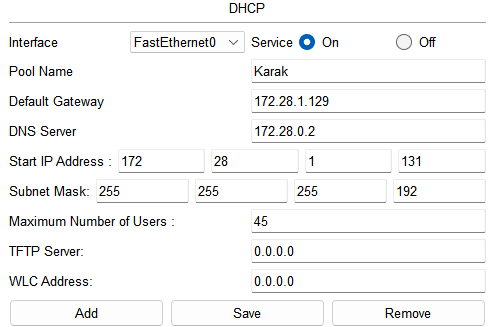
Headquarter DHCP configuration.

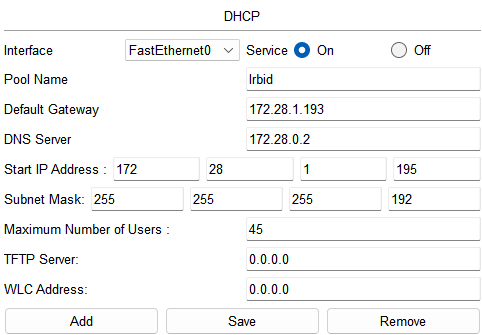
Amman remote office DHCP configuration. Aqaba remote office DHCP configuration.

Zarqa remote office DHCP configuration. Mafraq remote office DHCP configuration.

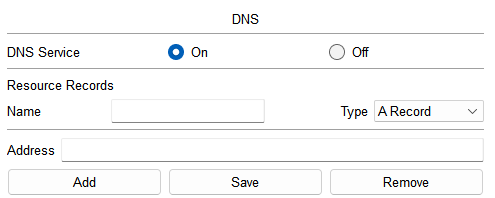
 

Shidiya remote office DHCP configuration. Karak remote office DHCP configuration.



Irbid remote office DHCP configuration.

DNS ser configuration:



we should add every device in the netwrok except the printers and the IP addresses for the PC’s. The IP address for the DNS server is 172.28.0.2\26

Graphical user interface, text, application

Description automatically generated Graphical user interface, text, application, email

Description automatically generated

And so on for all the devices in the netwrok.

FTP server configuration:

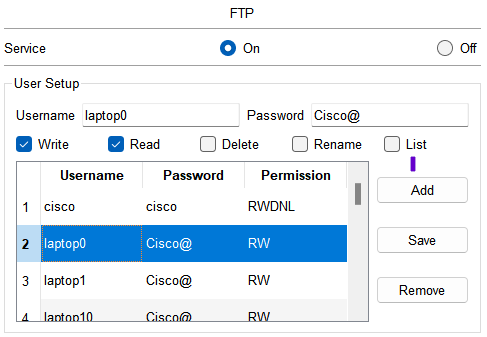
Graphical user interface, text, application

Description automatically generated

We should add the all device in the netwrok except the printers also we should deterimine the permisions for every device so for the addministrators have full access to the FTP server. For the manger in the remote offices have read, write, and list permisions. The IP address for the FTP server is 172.28.0.3\26

We should enter the username for the devices which is the devices names and create a password for the user.

Graphical user interface, text, application, email

Description automatically generated

Adding laptop0 to the FTP server. Adding PC4 to the FTP server.

And so on for all the devices in the netwrok except the printers.

HTTPS server configuration:

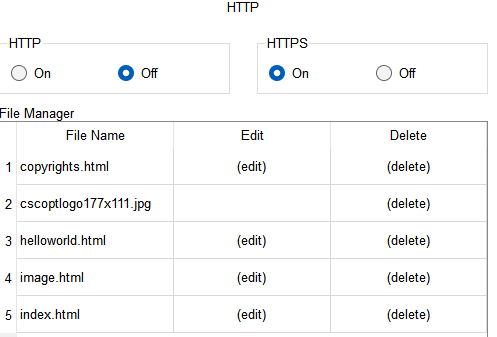
To add a webite in the HTTPS server we should add the webits in the DNS server.

The IP address for the HTTPS server is 172.28.0.4\26

Graphical user interface, application

Description automatically generated

Added the webiste which is eis.jnr.com.jo in the DNS server.



Then we have to turn off the HTTP because we need the webite to be seucred.

Configuration for the Email server:

Graphical user interface, application

Description automatically generated

We should add a domain name and its common to all the devices in this network and of course we have to turn on the STMP protocol to send the mail and POP3 to recive the mail. The IP address for the Email server is 172.28.0.4\26

Graphical user interface, application

Description automatically generatedThen we should add the username and it’s the devices name the we have to create the password for the email.

Graphical user interface, application

Description automatically generated

These are created email for lapotp1 and pc9 and I did the same for all the deiveces.

How to connect the Printer wirelessly:

Graphical user interface, application

Description automatically generated

We should turn off the print by clicking on this then we should replce this

With this because we want to connect it wirelessly if we want to connect it dirctly we should leave this thing as it’s.

How to connect the printer wired?

**Part 2:**

|  |  |  |
| --- | --- | --- |
| What to be tested: | Tools or commands used fro testing: | Expected results: |
| The connectivity between all the network. | We should enter the command in (CMD) and then write Ping with the IP address that we want to check | The first check gives at least 3 packets to be received.  If it’s the second time 4 packets should be received. |
| DHCP | Go to the desktop then IP configuration for all the devices that use the DHCP service to get an IP address | I expect all the PCs have their IP addresses, subnet masks, and default gateways by the DHCP service by checking the IP configuration for every device. |
| E-mail | Go to the desktop of any device then go to Email and send an email message to any device in the network. | I expect the email to be sent successfully. This means the SMTP email protocol is working correctly and if the other device receives the message that means the POP3 email protocol is working perfectly. The same thing should happen when replying to the email |
| DNS | Go to Desktop from any device then Web browser and enter the website URL | I expect the DNS server to be working properly so PCs can type a domain name to link to the website and PCs |
| HTTPS | We should go to the desktop then open the Web browser and write the URL for the website  https://eis.jnr.com.jo/ | I expect the website to open normally which means HTTPS works properly. |
| FTP | Go to CMD then write FTP with the FTP server’s IP address | I expect the device to be asked to enter the username and the password if they are both right. The client will enter the FTP server. |

**Part 3:**

Maintenance schedule for the network:

Because the JNR network is a big and an important company it should work all the time without any problem. To reach this goal we should do daily, weekly, monthly, and yearly maintenance on different remote offices.

So, after implementing the networks in the packet tracer simulator, the project has been scheduled to be built and finished by 2023. Therefore, the maintenance program will start by the start of 2024, having the first maintenance to take place on 1/1/2024.

Maintenance schedule:

For everyday maintenance we should check the network security, the connectivity between the LAN and WAN networks, and the network’s efficiency.

Network security: we should check the security every day, so we must make sure that there are no unknown devices connected to your clients’ networks because These devices can be as innocent as a WIFI-enabled toy, but because they contain mini web servers that can be hijacked by malicious attackers, they need to be found and placed in a secure place on the network.

Network efficiency: we should troubleshoot the network to check if there are any problem in the network. Monitoring availability as speed and latency between the device’s networks.

weekly maintenance we should check the connection between the Head quarter and other networks, and we should check if the devices are working normally.

Monthly maintenance we should check the FTP server and clear it from the unnecessary data, and check that there are no unknown files in the server. Also, we should check the hardware and software configuration.

Yearly maintenance overall checking and maintenance (we should check all the hardware’s and software’s equipment’s that form the network). And we should upgrade our network security.

Head Quarter maintenance schedule for everyday:

|  |  |
| --- | --- |
| 1/1/2024 | All the remote offices include the Head quarter should check on the network security (that there are no unknown clients), the connectivity between the Lan’s and WANs, and network efficiency. Also, the head quarter should check the server’s room specially the AC because any heat increase will affect hardly in the efficiency.  Also, the maintenance team should check the connectivity for the server. (DHCP, DNS, Email, FTP, and HTTPS) then we should check the connectivity for the administrators’ devices then the routers and the switches. |
| 1/2/2024 | All the remote offices include the Head quarter should check on the network security (that there are no unknown clients), the connectivity between the Lan’s and WANs, and network efficiency. Also, the head quarter should check the server’s room specially the AC because any heat increase will affect hardly in the efficiency.  Also, the maintenance team should check the connectivity for the server. (DHCP, DNS, Email, FTP, and HTTPS) then we should check the connectivity for the administrators’ devices then the routers and the switches. |

And so on for every day.

Head Quarter maintenance schedule for every week:

|  |  |
| --- | --- |
| 1/7/2024 | We should check the connection between the HQ and the other networks. Also, we should check that all the devices are working normally, and we should check that the connective between the networks working normally. |
| 1/14/2024 | We should check the connection between the HQ and the other networks. Also, we should check that all the devices are working normally, and we should check that the connective between the networks working normally. |

And so on for every end of a week.

Head Quarter maintenance schedule for every end of the month:

|  |  |
| --- | --- |
| 1/30/2024 | we should check the FTP server and clear it from the unnecessary data, and check that there are no unknown files in the server. Also, we should check the hardware and software configuration. And we should that all the devices inside the network are working normally specially the servers |
| 2/30/2024 | we should check the FTP server and clear it from the unnecessary data, and check that there are no unknown files in the server. Also, we should check the hardware and software configuration. And we should that all the devices inside the network are working normally specially the servers |

And so on for every end of a month.

Head Quarter maintenance schedule for every end of the year:

|  |  |
| --- | --- |
| 12/30/2024 | overall checking and maintenance (we should check all the hardware’s and software’s equipment’s that form the network). And we should upgrade our network security. And we should look for planes that upgrade our network. Also, we have to improve the performance by seeing the weaknesses and improve it. |
| 12/30/2025 | overall checking and maintenance (we should check all the hardware’s and software’s equipment’s that form the network). And we should upgrade our network security. And we should look for planes that upgrade our network. Also, we have to improve the performance by seeing the weaknesses and improve it. |

And so on for every end of year.

Maintenance schedule for all the remote offices:

Maintenance daily schedule for all the remote offices:

|  |  |
| --- | --- |
| 1/1/2024 | We should check that the network is secure and there are no unknown clients, we should check that all the devices connect normally with HQ. |
| 1/2/2024 | We should check that the network is secure and there are no unknown clients, we should check that all the devices connect normally with HQ. Also, we must check that all the device working rightly. (the efficiency). |

And so on for every day.

Maintenance weekly schedule for all the remote offices:

|  |  |
| --- | --- |
| 1/7/2024 | We must check that all the device working rightly. (The efficiency). And that there are no problems in connection. |
| 1/14/2024 | We must check that all the device working rightly. (The efficiency). And that there are no problems in connection. |

And so on for every end of a week.

Maintenance monthly schedule for all the remote offices:

|  |  |
| --- | --- |
| 1/30/2024 | We should check the hardware and the software configuration, and all the emails that sent and received. |
| 2/30/2024 | We should check the hardware and the software configuration, and all the emails that sent and received. |

And so on for every end of a month.

Maintenance yearly schedule for all the remote offices:

|  |  |
| --- | --- |
| 12/30/2024 | We should check everything in the network, and we should upgrade the security system. |
| 12/30/2025 | We should check everything in the network, and we should upgrade the security system. |

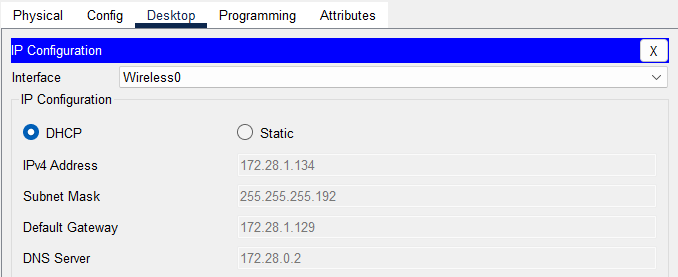
And so on for every end of year.

**Task 3:**

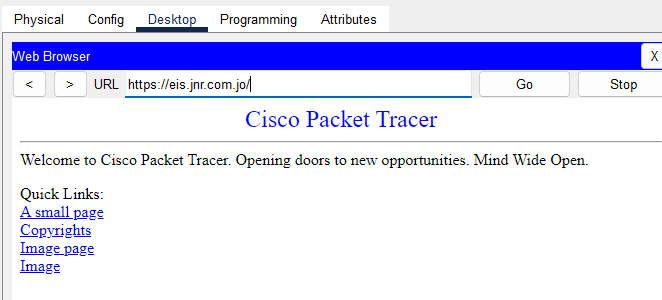
**Part 3:**

The expected result of checking the connection between the clients and between a device and servers:

First, we should check that the DHCP server working normally by going to all the devices that taking there IP address from the DHCP server and check if they have IP addresses:

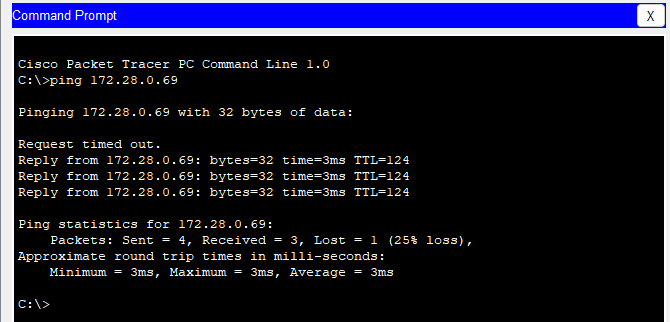


Second, we should check that the DNS working to check it we should check the website if it’s working normally that’s mean the DNS server working normally:



Now we have to check the connection between 2 devices (2 pc):

Between 2 clients the expected results to get at least 3 replies:

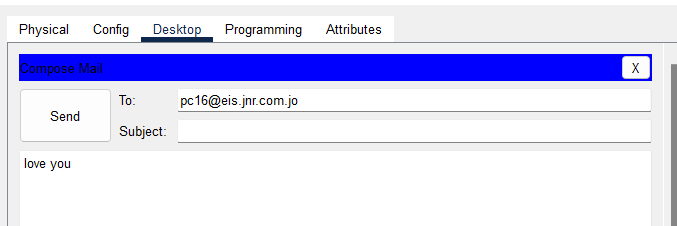


So that’s mean the connectivity between the two clients are good (working) we should do all that between all the clients (devices) in the server.

Now we can check if the Email server working normally or no:

To know that we should send a email from device another one:

That’s how we sent the email:

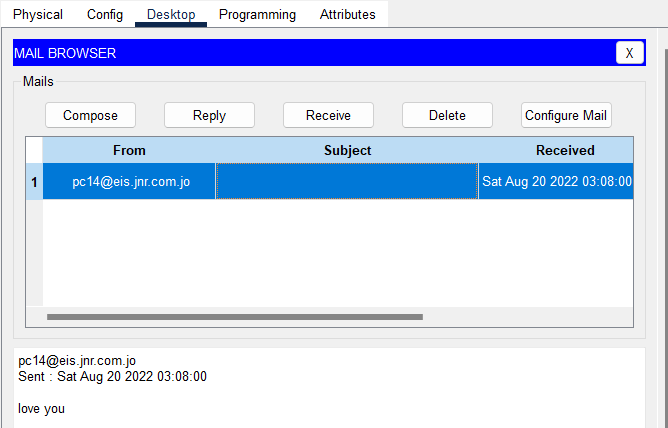


And we got this picture that’s mean the email is sent correctly:

Graphical user interface, text

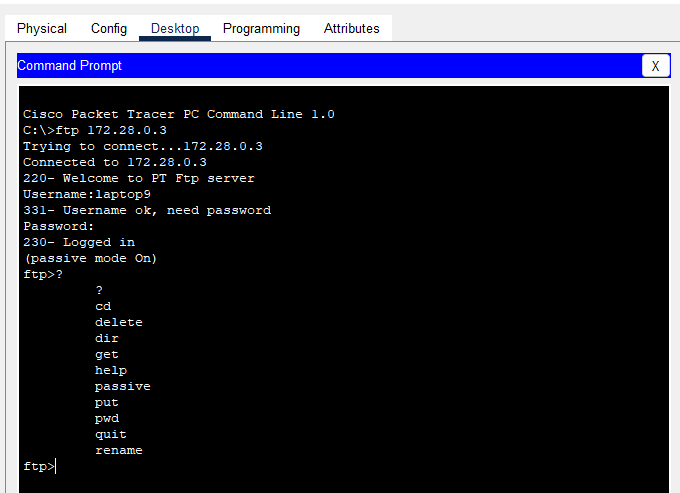
Description automatically generated

Now we have to check the receiver email:

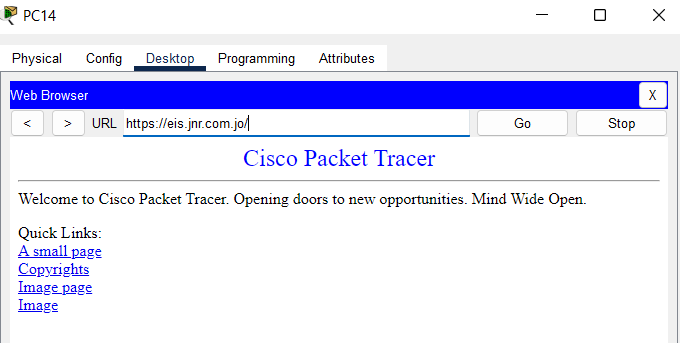


Now we have to check the FTP server:

I will go to any device in the network and try to open it from there if it opens that’s mean it’s working normally:



Now, we have to check the HTPPS server:



**Part 4:**

I recommend changing the physical topology of the WANs from ring topology to mesh topology or partial mesh because if any WAN goes down in the partial mesh or in the mesh topology then the packet will find another fast way but, in the ring topology, if a WAN network is down, the packet will then take the opposite side and that will cost more time.

I recommend putting each service from the FTP, DHCP, DNS, HTTPS, and EMAIL one in each server individually. Also, creating a backup for the servers and I recommend putting that backup in another city such as Irbid. I recommend adding another switch in each Lan network so it’s easy to add new devices. Having more than one central data point like creating one for the networks in the north and one for the networks in the south.

And I recommend using faster cables as the fiber cables. Using the new version of the devices, especially for the routers and the switches. Upgrading the network software and the hardware periodically. Add at least 2 networks and leave them as a backup when you want to expand the network or if any network is down.

**Part 5:**

To improve the security of the network I recommend adding a VPN protocol and adding a firewall in the network. Also, I recommend determining the space of the Wi-Fi access so no one out of the network can have a connection to the network.

Using a very hard password on everything will enhance security. Also, I recommend using wired connections for all the devices because it's more secure. Devices connected to the network should be checked every day. Saving all the data in a backup hard disk so it helps if someone hacked the network.

Hire professional cyber security people to work on protecting the network. Put a password on the servers’ rooms so it won’t be allowed for anyone to enter the data center. Change the passwords the end of the month. Use hashing functions to hash everything and I recommend the RSA function to hash everything the data and passwords (everything can be hashed).

**Part 6:**

After finishing all the parts of the work, now I will do a quick summary of my work:

I see that my work and my design for the network were almost perfect. I designed the network on a way to take the best efficiency from the network as I see. So, I created 8 LANs networks that cover the targeted places and then connected them to create one big WAN network in Jordan. I used many protocols in the network to make the network easier to use and better to communicate between the devices like (Email, OSPF…. etc.). Also, the network is working on the Linux operating system. Also, I used the hybrid physical topology and HDLC, ethernet for the logical protocols. I tried to reduce the costs and increase the efficiency and security but that was not easy and available on all the network parts.

critical reflection:

as with anything in the world, there is nothing perfect 100%, I have some problems and mistakes in my project such as that I connected the printers wirelessly. I did not create any backup servers. There is no backup network for the central data. I did not use the VPN protocol. I did not create any backup cables if any cable is down there no backup for it. Also, the passwords that are used in the network are not that hard and easy to know.

If I got the chance to repeat the project, what would I change?

I would like to use full mesh for the physical topology. And connecting everything wired because it's more secure. Giving every service an induvial server. Adding other services to the network. Creating a backup for everything, especially the central data network. I would like to use fiber cables to transfer the data faster. Also, I would like to use better versions of the devices. And my suggestion for the company is to take all the feedback so you can improve and reach the user's expectations.

A picture containing whiteboard, text

Description automatically generated