­

NETWORKING - FINAL ASSIGNMENT

Instructor Name: Dr. Sami Al-Mashaqbeh / Eng. Elham Derbas

Student Name: Raneem Yahya Sa’deh

Student ID: 22210016

A grey logo on a black background

Description automatically generated with low confidence

18 June 2023

Table of Contents

[| PART ONE|Building a Connected Network Infrastructure for DBSC 5](#_Toc138033730)

[Introduction 5](#_Toc138033731)

[Network Types: 5](#_Toc138033732)

[1- PAN (Personal Area Network): 5](#_Toc138033733)

[2- LAN (Local Area Network): 6](#_Toc138033735)

[3- CAN (Campus Area Network): 6](#_Toc138033736)

[4- MAN (Metropolitan Area Network): 6](#_Toc138033737)

[5- WAN (Wide Area Network): 7](#_Toc138033738)

[The](#_Toc138033739) [Recommendation for DBSC project 7](#_Toc138033740)

[Physical Network Topologies: 8](#_Toc138033741)

[Bus Topology](#_Toc138033742)

[Star Topology: 8](#_Toc138033750)

[Ring Topology: 9](#_Toc138033756)

[Mesh Topology: 9](#_Toc138033763)

[Extended Star Topology: 9](#_Toc138033768)

[Comparison between Star and Bus Topology: 10](#_Toc138033770)

[Logical Topology Protocol (Ethernet) 10](#_Toc138033771)

[Networking Protocol: 11](#_Toc138033772)

[1. DHCP (Dynamic Host Configuration Protocol): 11](#_Toc138033773)

[2. DNS (Domain Name System): 11](#_Toc138033774)

[3. TCP/IP (Transmission Control Protocol/Internet Protocol): 11](#_Toc138033775)

[4. HTTP (Hypertext Transfer Protocol): 12](#_Toc138033776)

[5. SMTP (Simple Mail Transfer Protocol): 12](#_Toc138033777)

[Bandwidth Impact: 12](#_Toc138033778)

[Networking Devices: 12](#_Toc138033779)

[1- Router: 13](#_Toc138033780)

[2- Switch: 13](#_Toc138033784)

[3- Personal Computer (PC): 13](#_Toc138033785)

[4- Server: 14](#_Toc138033786)

[5- Printer: 14](#_Toc138033788)

[6- Firewall: 15](#_Toc138033789)

[Server Types: 15](#_Toc138033790)

[1- Web Server: 15](#_Toc138033791)

[2- File Server: 15](#_Toc138033799)

[3- Mail Server: 16](#_Toc138033805)

[4- DNS Server: 16](#_Toc138033810)

[5- DHCP Server: 16](#_Toc138033816)

[Other Considerations: 17](#_Toc138033817)

[Inter-Dependences: 17](#_Toc138033818)

[|Part Two| Design efficient networked systems 19](#_Toc138033819)

[1- Full Subnetting 19](#_Toc138033820)

[2- OSPF for all networks: 20](#_Toc138033821)

[3- The Final Network Design 23](#_Toc138033822)

[4- Planning the network design 24](#_Toc138033823)

[5- Designing LANs 25](#_Toc138033824)

[6- Building the Data Centre 26](#_Toc138033825)

[Servers Detailed Information 30](#_Toc138033826)

[Detailed Test Plan 30](#_Toc138033827)

[Maintenance Schedule to support the networked system 31](#_Toc138033828)

[|Part 3| Implement, test, and diagnose networked systems 33](#_Toc138033829)

[Network Configuration Verification 34](#_Toc138033830)

[Ping: 34](#_Toc138033831)

[FTP: 35](#_Toc138033832)

[Nslookup 35](#_Toc138033833)

[Testing the connections: 36](#_Toc138033834)

[Recommended Enhancementsto support network growth 39](#_Toc138033835)

[The significance of upgrades and security requirements 40](#_Toc138033836)

[Critical thinking 40](#_Toc138033837)

[References 42](#_Toc138033838)

# | PART ONE|**Building a Connected Network Infrastructure for DBSC**

## Introduction

The DBSC project entails the growth of a Digital Banking Service Company by opening branches outside of its Amman headquarters in Istanbul, Riyadh, Dubai, London, Beirut, and Cairo. The main goal is to establish a connection between these offices and the main data center at the headquarters. The business needs encompass secure wireless connectivity for portable devices, efficient email communication, seamless file sharing between offices, and secure access to internal systems via a Fully Qualified Domain Name (FQDN) that all DBSC offices will be able to collaborate, share data, send/receive emails, and operate more effectively. This part will explore the network infrastructure requirements for the DBSC project, covering hardware devices, protocols, software integration, and their inter-dependences.

## Network Types:

The section discusses the network types that can be considered for connecting the DBSC offices together. The discussion will include the usage, benefits, and constraints of each type: PAN, LAN, CAN, MAN and WAN. The discussion will include the recommended network types for connecting DBSC offices:

### PAN (Personal Area Network):

PAN usually includes wireless connections and one of the most common real-world examples of a PAN is the connection between a Bluetooth earpiece and a smartphone. PANs often use technologies like Bluetooth or Wi-Fi. PANs can also connect laptops, tablets, printers, keyboards, and other computerized devices. So, its internet range is for personal use.

|  |  |
| --- | --- |
| PAN (Personal Area Network) | |
| Benefits | They are safe and protected, Low cost and easy to use. |
| Constraints | The range of PAN is limited, its range is about ten meters, but the protection range is thirty meters, and its connection might be bad to other networks like radio bands. |

However, considering the scope of the project, a PAN would not be suitable for connecting multiple offices located in different countries.

### LAN (Local Area Network):

LAN is a collection of devices connected to one physical location, such as a building, office, or home. LAN can be connected wirelessly, wired, or both together. They typically utilize Ethernet or Wi-Fi technologies.

|  |  |
| --- | --- |
| LAN (Local Area Network) | |
| Benefits | The devices can use a single Internet connection, share files with one another, print to shared printers, and be accessed and even controlled by one another, and the communication is easy and fast, Data is secure because you can manage it in one place.  LANs offer high data transfer speeds, low latency, and easy sharing of resources. |
| Constraints | LAN does not have good privacy, because the admin can reach to the files of the LAN user.  LANs have a limited range and are typically restricted to a single physical location. |

In this project, LANs can be used to connect devices within each office location.

### CAN (Campus Area Network):

 CAN is made by combining small LANs (Local Area Networks). And it is smaller than metropolitan area networks (MAN) and wide area networks (WAN), it also enables connected users to quickly share files and data within the network.

|  |  |
| --- | --- |
| CAN (Campus Area Network) | |
| Benefits | In the CAN network, to use some hardware devices of networking such as a hub, routers, switches, cables, and bridges. Easy accessibility of data, it transfers huge files with higher speed, and CAN is Economical. CANs often use high-speed fiber optic cables for data transmission. |
| Constraints | Maintenance is expensive, it does not support a maximum number of nodes, and the connection is limited in its size. |

While CANs can provide connectivity between multiple offices, their range is still limited and may not be suitable for connecting offices in different countries.

### MAN (Metropolitan Area Network):

 MAN covers a very big area by connecting multiple LANs and CANs within the area. MANs utilize technologies like fiber optics, microwave links, or leased lines to provide high-speed connectivity over longer distances. MAN uses different types of protocols like ATM, ADSL, and RS-232. MAN doesn't have a router and it is usually used for banks.

|  |  |
| --- | --- |
| MAN (Metropolitan Area Network) | |
| Benefits | MAN is a network that spans a larger geographic area, typically covering a city or metropolitan region.  Soldiers use MAN network for communication. |
| Constraints | Securing it against hackers can be challenging.  Connecting several sites frequently necessitates the use of more cables. |

However, setting up and maintaining a MAN can be complex and costly.

### WAN (Wide Area Network):

 A WAN is designed to connect multiple LANs or CANs over a large geographic area, frequently spanning numerous cities, nations, or even continents. To create safe and dependable connections over great distances, WANs use technologies like leased lines, MPLS (Multi-Protocol Label Switching), or VPN (Virtual Private Network).

|  |  |
| --- | --- |
| WAN (Wide Area Network) | |
| Benefits | * Wide coverage: A WAN can connect the DBSC offices in Istanbul, Riyadh, Dubai, London, Beirut, Cairo, and the HQ in Amman, enabling smooth communication and data exchange across locations. * Secure connectivity: Using technologies like VPN, a WAN may offer secure connections, enabling employees to send data securely across the network and access the company's internal systems. * Scalability: WANs may be readily expanded in the future to accommodate more branches or offices, complementing the business's development objectives. * Centralized management: With a WAN, network administration and troubleshooting can be done more easily from the headquarters. |
| Constraints | The cost of building a WAN is quite high, and its security is not rated as very strong. |

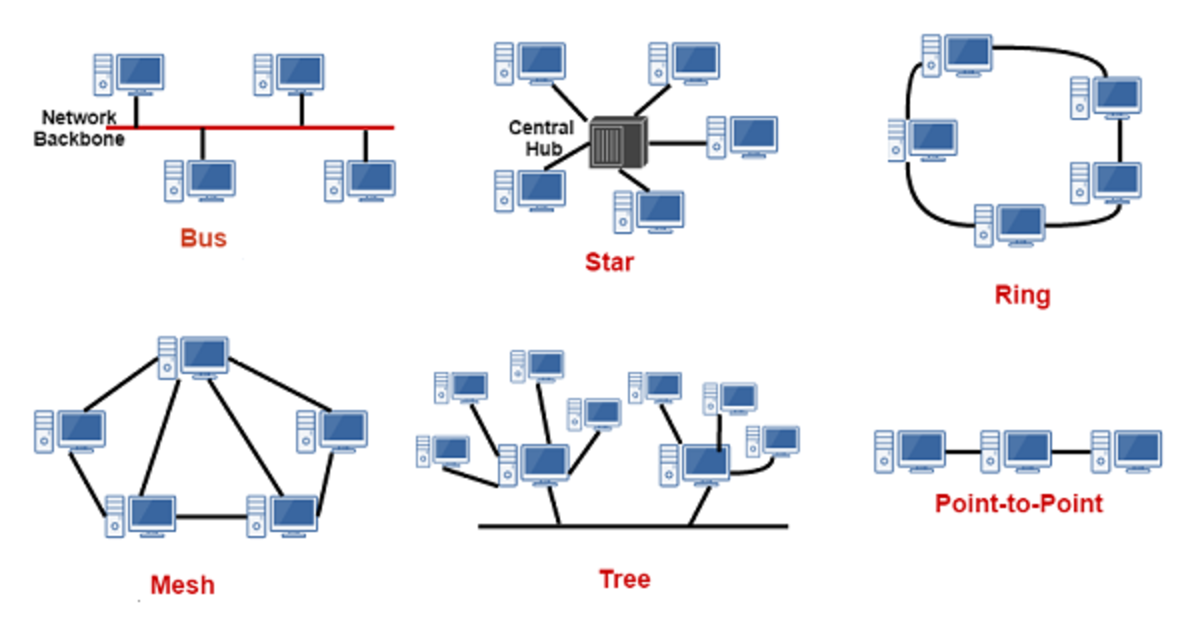
### The Recommendation for DBSC project

A WAN (Wide Area Network) would be the most suitable network type given the project's requirements and the locations of the offices. It would provide the necessary coverage, secure connectivity, scalability, and centralized management needed for efficient collaboration and data sharing among the offices. To implement a WAN, DBSC can consider leveraging technologies like leased lines, MPLS, or VPN, depending on their specific requirements, budget, and desired level of security.

## Physical Network Topologies:

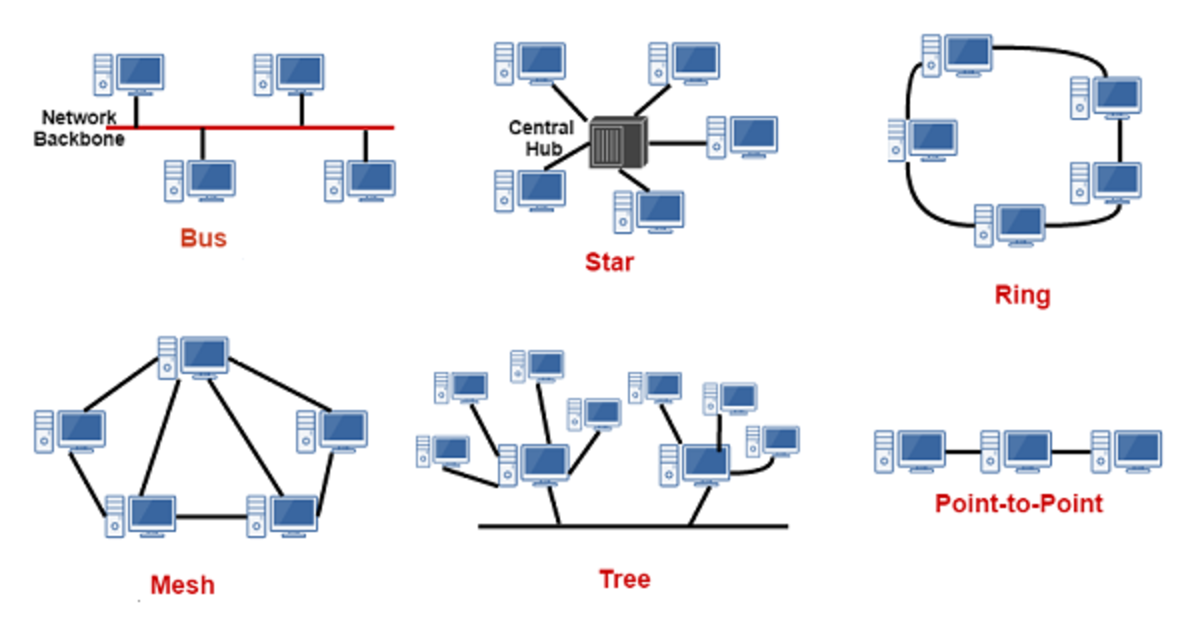
Physical network topologies refer to the physical layout or structure of a network, describing how devices are interconnected. This section explains the Bus, Star, Ring, Mesh, and Extended Star network topologies, and their characteristics. The section includes the recommended physical network topologies for the DBSC project:

### Bus Topology

Bus is the topology where all the devices in the network are connected by one central network cable. The key characteristics of the Bus topology:

1. Better while using small networks.
2. Simple and not expensive as it requires less cabling.
3. Devices are easy to remove or add. If there is a problem in one device, it will not affect the other.
4. Limited scalability and bandwidth because all devices share the same communication medium.
5. If the bus fails, the entire network can be affected.

### Star Topology:

Star is one of the most common topology setups, Where the central network device acts as a server, and the side devices act as clients, such as a switch or hub. Each device has a dedicated point-to-point connection to the central device, forming a star-like structure. Key characteristics of the Star topology:

1. All the devices in the Star Topology are connected to a central device, like a switch, by a separate cable which makes it slightly more expensive.
2. It is suitable for medium and large networks.
3. Centrally controlled and managed as all communication flows through the central device.
4. A broken cable or device won't take down the entire network.
5. Problems are simple to identify and troubleshoot.

### Ring Topology:

A picture containing diagram, line, design, origami

Description automatically generatedRing is a type of network topology where each device is connected to two devices, one on each side as in the picture, And the device’s connections create a circular data path. Key characteristics of the Ring topology:

1. All the devices are connected as a closed loop, forming a ring shape.
2. The data travels in one direction around the closed loop.
3. No central device.
4. It uses fewer cables than the Bus and the Star Topologies.
5. Difficult to reconfigure or add new devices without affecting the entire network.

### Mesh Topology:

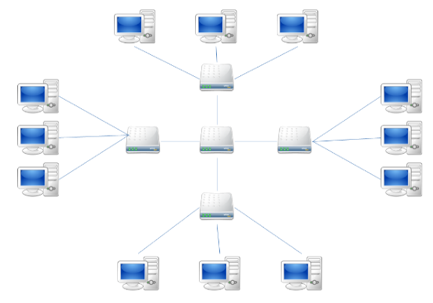
A picture containing diagram, line, design, origami

Description automatically generatedMesh Topology is a network architecture where each device is directly connected to all other devices. So, it creates a fully connected network where each device has a direct link to every other device. Mesh topologies can use wired and wireless connections. Key characteristics of the Mesh topology:

1. It can manage a high amount of traffic.
2. If there is a flaw in a device the network will not be affected, because it can automatically reroute data through other available paths.
3. Because of direct connection the bandwidth will increase, and it will give better network performance.

### Extended Star Topology:

It is an extension of the star topology, where all the devices are connected to a central point like a central switch, its performance is better than bus topology. Key characteristics of the Extended Star topology:



**Extended Star Topology**

1. It is easy to extend the network by adding central switches.
2. You can upgrade the extended star topology to a faster speed.
3. It is easy to find devices and cables that have issues in the network.
4. You can control multiple devices at the same.

### Comparison between Star and Bus Topology:

|  |  |  |
| --- | --- | --- |
| Aspect | Star Topology | Bus topology |
| Connectivity | Devices are connected to a central device (hub or switch). | Devices are connected to a common bus. |
| Scalability | Easy to add more devices to the central device. | Limited because of the common bus. |
| Fault Tolerance | Failure of one device or cable does not affect the network. | Failure of the bus can take down the entire network. |
| Performance | Higher performance as each device has a separate cable. | Relatively low because of shared bandwidth on the bus. |
| Costing | More expensive as each device has a separate link. | Requires less cabling compared to the star topology. |
| Management | Centralized management and easy troubleshooting. | Difficult to troubleshoot and isolate network issues. |

The recommended network topology for the DBSC project is a combination of WAN and Star topology. The WAN connects the offices in a bus topology, enabling access to internal systems, file sharing, and email communication. Each office utilizes a Star topology with a central switch for easy connectivity, management, and a reliable network infrastructure.

## Logical Topology Protocol (Ethernet)

Ethernet would be the appropriate protocol to use for the LANs connectivity. Ethernet provides reliable and efficient communication between devices within the same LAN, that make an effective data transmission and connectivity.

|  |  |
| --- | --- |
| **Performance** | Ethernet should provide good performance in terms of throughput and response times.  Ethernet should minimize network delays, packet loss, and bottlenecks to ensure efficient data transmission. |
| **Scalability** | Ethernet has evolved over time to support increased scalability, and you can add more devices without significant performance degradation and easier because of the Ethernet switches. |
| **Ethernet Timing** | Collisions can occur if two or more devices start transmitting simultaneously or if one device starts transmitting while another is still transmitting. If a collision occurs, all devices wait a random period before listening again.  If media congestion results in the MAC layer being unable to send the frame after 16 attempts, it will send an "Error". |
| **Bandwidth Efficiency** | **1**- 10BASE-T -> 10 Mbps  **2**- 100BASE-TX -> 100 Mbps  **3**- 1000BASE-T -> 1 Gbps  These higher speeds enable faster data transfer rates and efficient utilization of available bandwidth. |

## Networking Protocol:

The networking protocols (DHCP, DNS, TCP/IP, HTTP, and SMTP) are required for the DBSC project to meet its business requirements, including secure and automated IP address assignment, domain name resolution, reliable data transmission, web-based access to business resources and internal systems, and efficient email communication among employees:

### DHCP (Dynamic Host Configuration Protocol):

This network protocol gives devices automatic IP addresses, subnet masks, and other network configuration parameters.

### DNS (Domain Name System):

DNS enables employees in the DBSC offices to access the company's internal system (https://eis.DBSC.com.jo/) using a Fully Qualified Domain Name (FQDN), ensuring reliable and user-friendly access to network resources. So, the DNS makes it easy to enter a website by inputting normal words into the browser (https://eis.DBSC.com.jo/) instead of the IP address.

### TCP/IP (Transmission Control Protocol/Internet Protocol):

This network protocol is used on the Internet and most local networks, it shows how data is exchanged on the Internet by making end-to-end communications that identify how it should be broken into packets and received at the destination.

### HTTP (Hypertext Transfer Protocol):

This network protocol is used on the Internet and most local networks, it shows how data is exchanged on the Internet by making end-to-end communications that identify how it should be broken into packets and received at the destination. (There is also HTTPS it is the same as HTTP but securer).

### SMTP (Simple Mail Transfer Protocol):

This network protocol is used on the Internet and most local networks, it shows how data is exchanged on the Internet by making end-to-end communications that identify how it should be broken into packets and received at the destination.

### Bandwidth Impact:

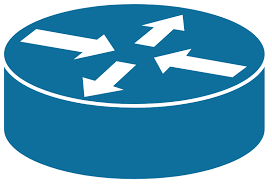
The amount of data that may be transmitted through a network in a specific amount of time is referred to as bandwidth needs. It has a significant impact on several facets of data transmission and is essential in evaluating network performance:

* **Data Transfer Rates**: The data transfer rates that can be achieved on a network are directly impacted by bandwidth. While a lesser bandwidth restricts the speed, a higher bandwidth enables faster data transport. A network with a bandwidth of 100 Mbps, for instance, may move data more quickly than one with a capacity of 10 Mbps.
* **Latency:** Latency, or the amount of time it takes for data to move from its source to its destination, is another factor influenced by bandwidth. In general, decreased latency is achieved by increasing bandwidth because more data can be transferred simultaneously. For real-time applications like phone and video conferencing or online gaming, where delays might affect user experience, lower latency is essential.
* **Concurrent Connections:** The network's capacity to support numerous concurrent connections is impacted by bandwidth availability. A fraction of the bandwidth is used by each connection. Too many connections running at once might cause congestion and poor performance if the bandwidth is constrained. Higher bandwidth, however, enables more simultaneous connections and better scalability.

## Networking Devices:

Networking devices are the hardware devices that are the most important part of a network because they play an important part in making connecting easy and transferring data in the network. They provide connectivity and increase network performance.

### Router:

For the DBSC project, to connect the several offices spread across different countries, routers are essential. They facilitate data routing and ensuring secure and effective communication throughout the (WAN). By installing routers at each office, they connect the (LAN) to the (WAN) and facilitate connectivity to the business's data center.

#### **Operating Principles:**

Routers are network components that work at Layer 3 of the OSI model, which is the network layer. Router connects two networks such as (LANs, and WANs). They take in data packets from one network and choose the best route to send them to another. Based on destination IP addresses, routers use routing tables and algorithms to make informed routing decisions. Additionally, they provide capabilities for firewalls and network address translation (NAT).

### Switch:

A picture containing text, screenshot, logo, font

Description automatically generatedSwitches can be deployed at each office to connect PCs, servers, printers, and other devices, enabling high speed and reliable communication and data transfer within the local network.

#### **Operating Principles:**

Switches operate at the data link layer (Layer 2) of the OSI model. Switches build and maintain MAC address tables to send data between devices in the same network. Switches improve network performance by decreasing smashing and enabling double communication.

### Personal Computer (PC):

A computer and keyboard

Description automatically generated with low confidencePCs are used by employees in the DBSC project to conduct their chores and collaborate through accessing the company's internal systems, share files, send/receive emails, and perform other tasks.

#### **Operating Principles:**

PCs are end-user devices that operate at the application layer (Layer 7) of the OSI model. PCs are used to access and utilize network resources, such as applications, files, and services and they could send and receive data packets over the network. They typically run operating systems like Windows or Linux and connect to the network through wired or wireless connections.

### Server:

A picture containing machine, design

Description automatically generatedServers can be located at the headquarters in Amman to host the company's internal systems, shared files, email services, and other network resources.

#### **Operating Principles:**

Servers are powerful devices that provide resources and services to client devices on a network. Their role and protocol defines the OSI model layer they work in, like web servers that work in the Application layer (Layer 7). Servers are located in data centers and handle requests from client devices, process data, and provide responses or resources accordingly. They have high availability and performance. Servers have different types based on their specific purposes, such as:

1. File Server: Stores and shares files 🡪 (FTP).
2. Web Server: That delivers web pages to clients 🡪 (HTTP).
3. Email Server: Sending and receiving mail messages 🡪 (SMTP).

### Printer:

#### A blue and white printer with a paper Description automatically generated with low confidenceThe DBSC project requires printers so that staff members can print hard copies of documents. In each office, printers can be connected to the local network via switches.

#### **Operating Principles:**

Printers operate at the application layer (Layer 7) of the OSI model. Printer can be connected to a local area network (LAN) or a wireless network which often use protocols like TCP/IP. And once it is connected, the printer becomes accessible to multiple devices on the network, such as PCs, laptops, and other devices. By connecting printers to the network, organizations can streamline their printing processes.

### Firewall:

Firewalls are crucial for securing the DBSC project's network infrastructure at each office and the data center to monitor and control incoming and outgoing traffic.

#### **Operating Principles:**

Firewalls operate at the network layer (Layer 3) or transport layer (Layer 4) of the OSI model. They enforce security policies and control the flow of network traffic. It is a security device for the network that acts as a block between an internal network and external networks, like the Internet. It works as a control of the incoming and outgoing network traffic based on settled security rules. Firewalls protect networks from unknown access and harmful attacks.

## Server Types:

### Web Server:

It is designed to host a website and give web pages to the client. Web servers use HTTP (Hypertext Transfer Protocol).

|  |  |
| --- | --- |
| Hardware Specification | Focus on high CPU performance, enough memory (RAM), and fast storage to improve website loading times. |
| Operating System | Linux distributions like Ubuntu are commonly used because of their stability, security, and cost-effectiveness. |

### File Server:

It is designed to store and share files across the network, File server uses FTP (File Transfer Protocol).

|  |  |
| --- | --- |
| Hardware Specification | Focus on ample storage capacity, redundancy for data protection (such as RAID configurations), and good network connectivity to handle concurrent file transfers. |
| Operating System | Windows Server is commonly used for its native support for SMB/CIFS protocols. |

### Mail Server:

It handles email communications, by sending, receiving, and storing email messages, Mail server uses email protocols (SMTP, IMAP, POP).

|  |  |
| --- | --- |
| Hardware Specification | Sufficient storage for email storage and backups, and reliable networking for email delivery. |
| Operating System | Linux distributions such as CentOS or Ubuntu Server are popular due to their stability and robustness for mail server deployments. |

### DNS Server:

It is designed to translate the web name (eis.DBSC.com.jo) into an IP address, DNS servers use DNS protocol (Domain Name System), So it makes mapping between the name and the IP address.

|  |  |
| --- | --- |
| Hardware Specification | DNS servers typically have lower hardware requirements compared to other server types. However, key considerations include network connectivity for efficient DNS resolution, and enough memory (RAM). |
| Operating System | DNS server software is available for multiple operating systems, including Windows Server with the DNS Server role. Considerations include the operating system, security, and compatibility with other server applications in the environment. |

### DHCP Server:

It is designed to give automatic IP addresses, subnet masks, and other network configuration parameters to devices, DHCP server uses DHCP (Dynamic Host Configuration).

|  |  |
| --- | --- |
| Hardware Specification | DHCP servers typically have moderate hardware requirements. Sufficient processing power and memory are needed to manage concurrent DHCP requests, while storage requirements are very little. |
| Operating System | DHCP server software is available for different operating systems, including Windows Server with the DHCP Server role. Considerations include compatibility with the network infrastructure and familiarity with the chosen operating system. |

### Other Considerations:

The following considerations should be taken into account when choosing servers for the DBSC project:

|  |  |
| --- | --- |
| Infrastructure requirements | Take into account the current network infrastructure and make sure that the components of the network are compatible and integrated. |
| Cost | Strike a balance between the server requirements and the project's financial restrictions.  Take into account economical options without sacrificing quality and dependability. For example, choosing rack-mounted servers over blade servers can result in cost savings. |
| Server performance | It should be optimized to deliver dependable and effective performance. It may also include functions like network load balancing, redundant power supplies, and RAID configurations for data redundancy. For instance, servers with multi-core processors and lots of RAM should be chosen if the project calls for resource-intensive applications or high-speed data processing. Additionally, incorporating solid-state drives (SSDs) instead of traditional hard disk drives (HDDs) can significantly improve data access speeds and overall server performance. |

## Inter-Dependences:

In order for the servers, workstations, client PCs, routers, switches, and other networking equipment used in the DBSC project to operate efficiently and communicate with the network infrastructure, networking software is required. The inter-dependences between hardware and networking software are as follows:

|  |  |  |
| --- | --- | --- |
| **Source Device (Client PC)** | **Hardware** | The packets are transmitted onto the network by the PC’s (NIC) network interface card. |
| **Software** | The networking software will encapsulate the data that will be sent into packets, and then will add the headers like (IP and the transport layer header) and determine the destination IP address. |
| **Switch** | **Hardware** | The switch receives the packet from the source device's NIC, checks the destination MAC address, and determines the outgoing port. |
| **Software** | The switch's software performs knowing the MAC address, maintains the MAC address table, and forwards the packet to the appropriate port based on the destination MAC address. |
| **Router** | **Hardware** | The router receives the packet from the switch, examines the destination IP address, and determines the next hop. |
| **Software** | The router's software executes routing protocols (OSPF) to determine the best path for forwarding the packet based on the destination IP address. It performs routing table lookups, updates routing information, and makes forwarding decisions. |
| **Server** | **Hardware** | The server NIC receives the packet and extracts the encapsulated data. |
| **Software** | The networking software on the server processes the packet, checks for any required services or applications, and delivers the packet to the appropriate software layer. |

# |Part Two| Design efficient networked systems

Step-by-step plan on how to design a Local Area Network

### Full Subnetting

Prepare the subnetting tables for the devices, gateways and serials:

* 172.20.0.0\16
* The Subnetwork = 7
* 2^x=7 --> x=3
* We need the number of hosts:
* Old mask = 255.255.0.0
* 2^x = 60 --> x=6
* 32-6=26
* 255.255.255.192
* 1111 1111.1111 1111.1111 1111.1110 0000
* 172.20.1.0/26
* 2^6 = 64  so every time we will add (64)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Network Address | First IP Address | Last IP Address | Broadcast Address | # Usable Hosts |
| 172.20.1.0 | 172.20.1.1 | 172.20.1.62 | 172.20.1.63 | 62 |
| 172.20.1.64 | 172.20.1.65 | 172.20.1.126 | 172.20.1.127 | 62 |
| 172.20.1.128 | 172.20.1.129 | 172.20.1.190 | 172.20.1.191 | 62 |
| 172.20.1.192 | 172.20.1.193 | 172.20.1.254 | 172.20.1.255 | 62 |
| 172.20.2.0 | 172.20.2.1 | 172.20.2.62 | 172.20.2.63 | 62 |
| 172.20.2.64 | 172.20.2.65 | 172.20.2.126 | 172.20.2.127 | 62 |
| 172.20.2.128 | 172.20.2.129 | 172.20.2.190 | 172.20.2.191 | 62 |
| 172.20.2.192 | 172.20.2.193 | 172.20.2.253 | 172.20.2.254 | 62 |

Full Subnetting

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Network Address | First IP Address | Last IP Address | Broadcast Address | # Usable Hosts |
| 100.0.0.0 | 100.0.0.1 | 100.0.0.2 | 100.0.0.3 | 2 |
| 100.0.0.4 | 100.0.0.5 | 100.0.0.6 | 100.0.0.7 | 2 |
| 100.0.0.8 | 100.0.0.9 | 100.0.0.10 | 100.0.0.11 | 2 |
| 100.0.0.12 | 100.0.0.13 | 100.0.0.14 | 100.0.0.15 | 2 |
| 100.0.0.16 | 100.0.0.17 | 100.0.0.18 | 100.0.0. 19 | 2 |
| 100.0.0.20 | 100.0.0.21 | 100.0.0.22 | 100.0.0. 23 | 2 |
| 100.0.0.24 | 100.0.0.25 | 100.0.0.26 | 100.0.0.27 | 2 |

Serial Subnetting

### OSPF for all networks:

|  |  |
| --- | --- |
| ROUTER 0 | A screenshot of a computer  Description automatically generated with medium confidence |
| ROUTER 1 | A screenshot of a computer  Description automatically generated |
| ROUTER 2 | A screenshot of a computer code  Description automatically generated with low confidence |
| ROUTER 3 | A screenshot of a computer code  Description automatically generated with low confidence |
| ROUTER 4 | A screenshot of a computer code  Description automatically generated with low confidence |
| ROUTER 5 |  |
| ROUTER 6 |  |

### The Final Network Design

|  |  |
| --- | --- |
| PC15 pings HTTPS and DNS servers |  |

### Planning the network design

First, you start planning how many offices you have and give every office a router then how many floors in every office and give every floor a switch and we have two employees in every office so need for them 2 PCs and for the office I need one printer and a WIFI to connect the laptop with it (wireless) and by all of that we make a big WAN includes LANs (Lebanon, Dubai, Cairo, Istanbul….).

Key tools in CISCO packet tracer:

|  |  |
| --- | --- |
| From the network devices, you can have the router and the switch. |  |
| From the end devices, you could add a PC, Laptop, and printer |  |
| From the connections section, you can use the cables to connect the devices |  |

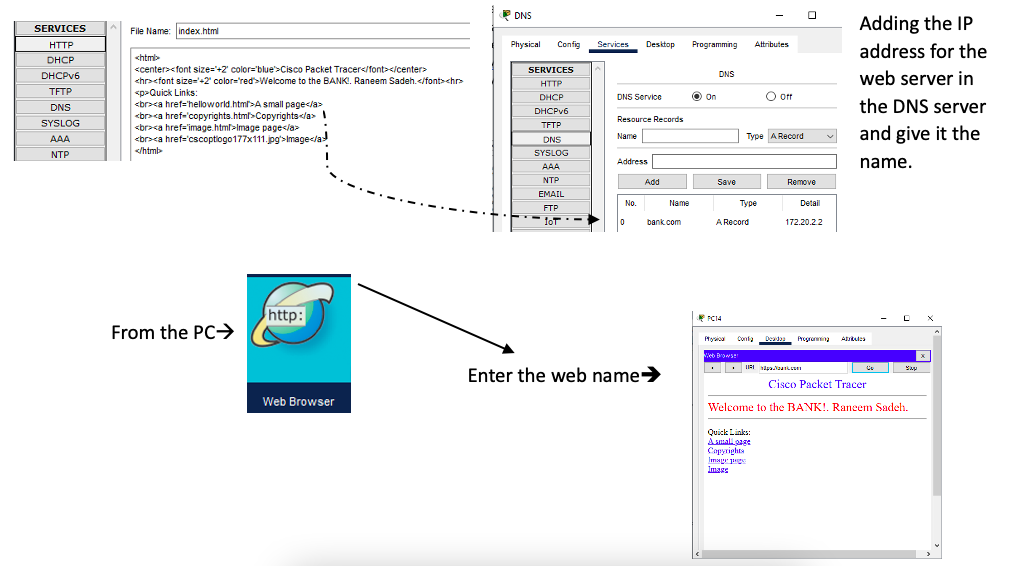
### 5- Designing LANs

|  |  |  |
| --- | --- | --- |
| 1. Connect the first PC by the switch with the Copper Straight-Through cable (wired) and the same to the second PC. | A picture containing text, screenshot  Description automatically generated |  |
| 1. Connect the switch to the router by the Copper Straight-Through cable (wired). |  |
| 1. Then connect the Printer to the switch to let the employee access it and give it an IP address from the subnetting within the range of the usable address |  |
| 1. Adding an Access point and connecting it to the switch so the devices can connect to the Wi-Fi in my network I connected the laptop to the Wi-Fi. The device could connect to it by having the password. |  | |
| 1. Connecting Laptop to access point | The device should have the Linksys-WPC300N module to provide one 2.4GHz wireless interface suitable for connection to wireless networks. And it supports protocols that use Ethernet for LAN access. |  |
| 1. Finally I connect the router by the serial DCE to another LAN. | [DCE devices provide the physical interface and signal conversion, while DTE devices generate or consume data] |  |

### 6- Building the Data Centre

1. A diagram of a computer network

   Description automatically generated with low confidenceAdd two PCs to the network and give them a static IP address from the subnetting which will be down.
2. Adding the web server that uses the HTTP/HTTPS protocols and the port number is 80  HTTP // 443  HTTPS, and give it a static IP.
3. Adding the DNS server (port 53) to open the web I make by its name and no need for its IP address, be giving it a static IP address and then add the IP address for the web server and what I want its name to be.
4. By the PC I can open the web page even by its name or by the IP address.



1. A screenshot of a computer

   Description automatically generated Adding the file server that uses the FTP in port 445, and then add the users that could send and receive files and give the permissions to every employee such as write, read, delete, rename, list.
2. The DHCP that I give all the PCs in my network their IP addresses from it.

* First, I start adding the gateway IP for every network and put the range for every network.
* At the Pool Name, I add the new name.
* At the default gateway, I add the IP address for the network gateway I want to give their PCs a DHCP IP.
* At the DNS server, I add the DNS IP address.
* At the start IP address, I put the first valid IP after I shift 10 addresses and the subnet mask will be 255.255.255.192.

A screenshot of a computer

Description automatically generated

1. Adding the email server which use SMTP and POP3 protocols in the port SMTP🡪587 // POP3🡪110. We set both (on) to let the user send and receive.

|  |  |
| --- | --- |
| A screenshot of a login box  Description automatically generated with medium confidence | A screenshot of a computer screen  Description automatically generated with low confidence |

1. A screenshot of a computer program

   Description automatically generated with medium confidenceAt the end I add a loopback, so if there is an IP address is not in the network the ping will not return unreachable, it will show this message.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Routers | Router0 | Router1 | Router2 | Router3 | Router4 | Router5 | Router6 | datacenter |
| G0/0/0 | 172.20.1.62 | 172.20.1.126 | 172.20.1.190 | 172.20.1.254 | 172.20.2.126 | 172.20.2.190 | 172.20.2.254 | 172.20.2.62 |
| G0/0/1 | - | - | - | - | - | - | - | 172.20.2.62 |
| S0/1/0 | 100.0.0.1 | 100.0.0.2 | 100.0.0.6 | 100.0.0.10 | 100.0.0.14 | 100.0.0.18 | 100.0.0.22 | - |
| S0/1/1 | - | 100.0.0.5 | 100.0.0.9 | 100.0.0.13 | 100.0.0.17 | 100.0.0.21 | 100.0.0.25 | - |

1. A screen shot of a computer

   Description automatically generated with low confidenceTo make my network more secure, I put a two-stage password that the user must enter before entering the command line in the router.

### Servers Detailed Information

|  |  |
| --- | --- |
| Server Function | IP Address |
| Web server | 172.20.2.2 |
| DNS server | 172.20.2.3 |
| File server | 172.20.2.4 |
| DHCP server | 172.20.2.10 |
| Email server | 172.20.2.5 |

For the other details such as services to be installed on each server, DHCP service, and configuration of each service, all screenshots where provided in the previous sections.

### Detailed Test Plan

|  |  |  |  |
| --- | --- | --- | --- |
| Test Objective | What to be tested | Tools or Commands Used | Expected Results |
| Network Connectivity | By making ping between the routers using for example a PC | PC, Command Prompt,  The other PC in the network we want to test the connection with IP address. | Gt for replay message that shows that there is a connection. |
| Bandwidth and Performance | Measure the network's throughput, and latency to make sure it complies with the necessary requirements for bandwidth and performance. | Network Traffic Generators | Desired throughput achieved, latency within acceptable limits |
| OSPF | The connection between the farthest networks | PC, Command Prompt,  The other PC in the network we want to test the connection with an IP address. | If the OSPF is working you must get a replay from the PC |
| Wireless connection | If the laptop can connect to other devices | PC, Command Prompt,  The laptop in the other or the same network we want to test its connection with IP address. | If I got a replay that means that the wireless is working |
| Web server | If I can see the web page I design | Web server and make a website then from other PC you can open the web by writing the IP address for it or it name that it get it from the DNS | If the website I design apper to me that will show that the web server is working and its connection and static IP are all right. |

### Maintenance Schedule to support the networked system

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Daily | Weekly | Monthly | Yearly | If Needed |
| Check the connection of all the devices | x |  |  |  |  |
| Check the network cables | x |  |  |  |  |
| Free up the storage |  |  |  | x |  |
| Software update |  |  | x |  |  |
| Changing cables |  |  |  |  | x |
| Adding devices |  |  |  |  | x |
| Measuring the temperature in the office | x |  |  |  |  |
| Patch Management |  |  | x |  |  |
| Disaster Recovery Testing |  |  |  | x |  |
| System Capacity Planning |  |  |  | x |  |

# |Part 3| Implement, test, and diagnose networked systems

## Network Configuration Verification

### Ping:

A black screen with white text

Description automatically generated with low confidence- Between PCs: to know if there is a connection between the PCs we use the command prompt then type (ping) and the PC IP address we want to see their connection

* Between the printer and the laptop: to know if there is connection between them we use the sending message.

|  |  |
| --- | --- |
| A diagram of a computer network  Description automatically generated with low confidence | A diagram of a computer network  Description automatically generated with low confidence |

### FTP:

We are going to use two PC one of them works as a client it make login at the file server and upload the file in the server then the other PC could login in onto the server and download the file.

|  |  |
| --- | --- |
| A screenshot of a computer  Description automatically generated with medium confidence | A computer screen shot of a computer program  Description automatically generated with low confidence |

Nslookup:

A screenshot of a computer

Description automatically generated with medium confidenceA command-line program called Nslookup is used to query the Domain Name System (DNS) in order to learn DNS-related details about a domain or hostname. It can get DNS records, resolve IP addresses, and run reverse lookups, and here is a screenshot that shows nslookup command.

### Testing the connections:

|  |  |
| --- | --- |
| For the HTTPS server.  Adding the web server that uses the HTTP/HTTPS protocols and the port number is 80 🡪 HTTP // 443 🡪 HTTPS, and give it a static IP. And this is the result I expected. | **A screenshot of a computer program  Description automatically generated with low confidence** |
| For the DNS Server.  Its main function is to translate domain names, which are human-readable website addresses, into IP addresses, which are unique numerical identifiers used by computers to locate and communicate with each other on the internet. And this is the replay I was expecting. | A picture containing text, screenshot, font, design  Description automatically generated |
| For the file server.  Adding the file server that uses the FTP in port 445, and then add the users that could send and receive files and give the permissions to every employee such as write, read, delete, rename, list. And this is the replay I was expecting | A screenshot of a computer screen  Description automatically generated with low confidence |
| For the email server.  Mail server performs, Sending Emails: When an email is composed and sent from an email client, the mail server receives the message and uses SMTP to forward it to the recipient's mail server. Receiving Emails: The mail server listens for incoming email messages addressed to its domain. It accepts and stores the incoming messages until they are retrieved by the recipient's email client using POP3 or IMAP protocols. | A screen shot of a computer  Description automatically generated with low confidence |
| For the DHCP server .  When a device connects to a network, it sends a DHCP request to the DHCP server. The DHCP server receives the request and assigns a unique IP address from the available pool of addresses. Along with the IP address, the DHCP server can also provide other configuration parameters, such as subnet mask, default gateway, DNS server addresses, and lease duration. | A screenshot of a computer program  Description automatically generated with low confidence |
| Here it shows the connection between the first router and the second one so here I know that my subnetting is correct because I get a replay.  The first router IP address (gateway) is 172.20.1.62 and the second one is 172.20.1.126. |  |
| The ping between the third router and the datacenter router at the first it didn’t give me the 4 replays but then after making another ping it give the replay which shows that the subnetting and the connection are right. | A picture containing text, screenshot, font  Description automatically generated |
| The ping between the laptop in network London and the laptop in network Beirut and the command shows that there is a connection. | A computer screen shot of a computer program  Description automatically generated with low confidence |
| Ping between the last two routers (Beirut) and (Cairo) and the result is just like what I excepted. | A screenshot of a computer  Description automatically generated with medium confidence |

### Recommended Enhancementsto support network growth

Network growth was in mind before start building the network, as I kept extra available IP addresses in each LAN or branch in order to not face any problems with devices growth in the network.

1. Security Devices and Tools:
   1. Network Segmentation: Implementing network segmentation using VLANs (Virtual Local Area Networks) can help isolate different parts of the network, enhancing security and reducing the attack surface. It allows for more granular control over network traffic and restricts unauthorized access between segments.
   2. Next-Generation Firewalls (NGFW): NGFWs combine traditional firewall capabilities with advanced security features such as deep packet inspection, intrusion prevention, and application-level controls. Deploying NGFWs can provide enhanced security and threat prevention capabilities.
   3. Endpoint Protection: Deploy endpoint security solutions such as antivirus, anti-malware, and host-based intrusion detection systems (HIDS) on devices to protect against threats originating from within the network.
2. Alternative Network Topologies:
   1. Star Topology: In a star topology, each branch would be connected directly to a central hub or switch. This provides a dedicated connection between each branch and the central device, improving reliability and making it easier to manage and troubleshoot the network.
   2. Mesh Topology: In a mesh topology, every branch would have a direct connection to every other branch. This fully connected topology offers high redundancy and fault tolerance. However, it can be costlier to implement due to increased hardware and cabling requirements.

### The significance of upgrades and security requirements

1. Improved Security: Adding security devices like firewalls and antivirus software strengthens the network's security. These tools protect against unauthorized access, malware, and data breaches, making the network more resilient to attacks.
2. Better Control: Network segmentation separates different parts of the network using VLANs, allowing for more control over traffic and who can access certain areas. This prevents unauthorized access to critical systems and sensitive data, improving overall network security.
3. Improved Performance and Reliability: Using network topologies like star or mesh improves how the network performs and stays reliable. These topologies provide backup routes and optimized paths, ensuring traffic flows smoothly and reducing disruptions. This means better network performance and less downtime.
4. Scalability and Future-Proofing: The recommended enhancements consider future growth and the addition of more devices. By implementing secure network segmentation, scalable security devices, and flexible topologies, the network becomes adaptable and can easily accommodate expansion and changes in the future. This ensures the network can grow alongside the organization's needs without compromising security or performance.

### Critical thinking

1. Bus Topology Limitations: The decision to use a bus topology may have some limitations in terms of scalability, fault tolerance, and performance. Bus topologies rely on a single communication line, which can become a single point of failure. If the central communication line fails, it can disrupt the entire network. Additionally, as the number of branches or devices increases, the network may face challenges in handling increased traffic and maintaining optimal performance.
2. Lack of Redundancy: The bus topology typically lacks redundancy since there is a single communication line connecting the branches. Redundancy is crucial for ensuring network availability and minimizing downtime in case of failures. Considering alternative topologies, such as star or mesh, could have provided better fault tolerance and redundancy by incorporating multiple connections or alternative paths.
3. Security Considerations: While security devices and tools were recommended to enhance network security, it's important to evaluate the initial design's consideration of security measures. The absence of security devices in the original design may have left the network vulnerable to potential security threats. Implementing security measures from the outset is crucial for safeguarding sensitive data and preventing unauthorized access.
4. Scalability and Future-Proofing: The network design and decisions made should be evaluated based on their scalability and future-proofing capabilities. Assess whether the network design adequately accounted for the anticipated growth, addition of communication devices, and changing infrastructure requirements. If the initial design did not adequately consider scalability, it may require modifications or additional enhancements to accommodate future expansion effectively.

# References

* “LAN vs WAN - Comparing Types of Computer Networks - AWS.” Amazon Web Services, Inc., 19 June 2022, <https://aws.amazon.com/compare/the-difference-between-lan-and-wan/#:~:text=LANs%20use%20local%20connections%20like> . Accessed 19 June 2023.
* javaTpoint. “Types of Computer Network - JavaTpoint.” Www.javatpoint.com, 2011, <https://www.javatpoint.com/types-of-computer-network> . Accessed 19 June 2023.
* communications @manageengine.com, ManageEngine. “Network Monitoring Software by ManageEngine OpManager.” ManageEngine OpManager, 19 June 2022, [www.manageengine.com/network-monitoring/tech-topics/network-topology.html#:~:text=Star%20topology%3A%20Star%20topology%20is](http://www.manageengine.com/network-monitoring/tech-topics/network-topology.html#:~:text=Star%20topology%3A%20Star%20topology%20is) . Accessed 19 June 2023.
* CompTIA. “Network Protocol Definition | Computer Protocol | CompTIA.” CompTIA, 2019, [www.comptia.org/content/guides/what-is-a-network-protocol](http://www.comptia.org/content/guides/what-is-a-network-protocol) . Accessed 19 June 2023.
* Professionals, Advanced Network. “7 Tips to Enhance Network Performance.” Advanced Network Professionals, 30 June 2022, [www.getanp.com/blog/65/7-tips-to-enhance-network-performance.php](http://www.getanp.com/blog/65/7-tips-to-enhance-network-performance.php) . Accessed 19 June 2023.
* Mauro, Andrea. “Network Topologies: Logical vs Physical | Aruba Blogs.” Blogs.arubanetworks.com, 24 Sept. 2019, <https://blogs.arubanetworks.com/solutions/network-topologies-logical-vs-physical/> . Accessed 19 June 2023.