**Sarah Alobeytha – 24110331**

**Final Networking Report**

1. **Network Planning: Provide a complete IP addressing plan, including subnetting for each site, justification for subnet sizes, and allocation of IP ranges (static/dynamic). Include subnetting tables and diagrams**.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| subnet | size | Network ID | First IP (default gateway) | Last IP  (usable) | Broadcast Address | Subnet Mask |
| LAN 1 - Amman | 32 | 192.168.1.0 | 192.168.1.1 | 192.168.30 | 192.168.1.31 | 255.255.255.224 |
| LAN 2 - Irbid | 32 | 192.168.1.32 | 192.168.1.33 | 192.168.1.62 | 192.168.1.31 | 255.255.255.224 |
| LAN 3 - Aqaba | 32 | 192.168.1.64 | 192.168.1.65 | 192.168.1.94 | 192.168.1.95 | 255.255.255.224 |
| LAN 4 -Beirut | 32 | 192.168.1.96 | 192.168.1.97 | 192.168.1.126 | 192.168.1.127 | 255.255.255.224 |
| LAN 5 - Cairo | 32 | 192.168.1.128 | 192.168.1.129 | 192.168.1.158 | 192.168.1.159 | 255.255.255.224 |
| LAN 6 - Zarqa | 32 | 192.168.1.160 | 192.168.1.161 | 192.168.1.190 | 192.168.1.191 | 255.255.255.224 |
| LAN 7 -HQ | 32 | 192.168.1.192 | 192.168.1.193 | 192.168.1.222 | 192.168.1.223 | 255.255.255.224 |

Static IP vs Dynamic IP – Why and When to Use Each

Static IP (Fixed Address)

A Static IP is manually assigned to a device and does not change.

Use it when:

* The device needs to be consistently reachable.
* You want to access the device remotely (e.g., servers, printers).
* The device provides network services (like DNS, web, or file servers).

Examples:

* Printers – so users can always print to the same address.
* Servers – must have a known, fixed IP.
* Access Points – for easier management and monitoring.

Dynamic IP (DHCP Assigned)

A Dynamic IP is automatically assigned by a DHCP server and can change over time.

Use it when:

* The device doesn’t need a fixed IP.
* You want easy setup and management.
* You have many devices that connect/disconnect frequently.

Examples:

* User PCs and laptops
* Mobile phones
* Guest devices

|  |  |  |  |
| --- | --- | --- | --- |
| Sub | devices | Static or DHCP | Ip address |
| LAN 1 (Amman) |  |  |  |
|  | Pc1 | DHCP | 192.168.1.2 |
|  | Pc2 | DHCP | 192.168.1.3 |
|  | Laptop | DHCP | 192.168.1.4 |
|  | Printer | static | 192.168.1.5 |
| LAN 2 (Irbid) |  |  |  |
|  | Pc3 | DHCP | 192.168.1.34 |
|  | Pc4 | DHCP | 192.168.1.35 |
|  | laptop | DHCP | 192.168.1.36 |
|  | printer | Static | 192.168.1.37 |
| LAN 3 (Aqaba) |  |  |  |
|  | Pc5 | DHCP | 192.168.1.66 |
|  | Pc6 | DHCP | 192.168.1.67 |
|  | Laptop | DHCP | 192.168.1.68 |
|  | Printer | static | 192.168.1.69 |
| LAN 4 (Beirut) |  |  |  |
|  | Pc7 | DHCP | 192.168.1.98 |
|  | Pc8 | DHCP | 192.168.1.99 |
|  | Laptop | DHCP | 192.168.1.101 |
|  | Printer | static | 192.168.1.100 |
| LAN 5 (Cairo) |  |  |  |
|  | Pc9 | DHCP | 192.168.1.130 |
|  | Pc10 | DHCP | 192.168.1.131 |
|  | Laptop | DHCP | 192.168.1.133 |
|  | Printer | static | 192.168.1.132 |
|  |  |  |  |
| LAN 6 (Zarqa) |  |  |  |
|  | Pc11 | DHCP | 192.168.1.163 |
|  | Pc12 | DHCP | 192.168.1.164 |
|  | Laptop | DHCP | 192.168.1.166 |
|  | Printer | static | 192.168.1.162 |
| LAN 7 (HQ) |  |  |  |
|  | DHCP Server | static | 192.168.1.194 |
|  | Pc13 | DHCP | 192.168.1.195 |
|  | Pc14 | DHCP | 192.168.1.196 |
|  | Pc15 | DHCP | 192.168.1.197 |
|  | HTTP server | static | 192.168.1.198 |
|  | DNS Server | static | 192.168.1.199 |
|  | Email Server | static | 192.168.1.200 |
|  | FTP Server | static | 192.168.1.201 |

**2. Design Blueprint Present a visual representation (snapshot from Packet Tracer) of your network topology, clearly showing routers, switches, end devices, and their interconnections.**

Hybrid Star Topology

1. Star Topology (within each LAN):
   * Each local network (Amman, Irbid, Aqaba, Beirut, Cairo) has devices like PCs, printers, and access points connected to a central device (router or switch).
   * This is a classic star configuration, where all devices connect to a central point.
2. Hybrid Topology (overall structure):
   * The LANs are connected to each other via routers, forming a Wide Area Network (WAN).
   * This combination of multiple star topologies connected together makes it a hybrid topology.

A computer screen shot of a computer network

AI-generated content may be incorrect.

1. **Device Configuration Explain IP assignments, protocols used (e.g., RIP, OSPF), and basic security features applied (e.g., passwords, encryption). Clearly identify which devices use static vs dynamic IPs.**

* Use RIP (Routing Information Protocol) if:
  + Your network is small and simple.
  + You want easy setup with minimal configuration.
* Use OSPF (Open Shortest Path First) if:
  + Your network is large or growing.
  + You need faster convergence and better performance.

I chose OSPF (Open Shortest Path First) as the routing protocol for the following reasons:

1. Scalability  
   My network includes multiple LANs across different cities. OSPF is highly scalable and can efficiently handle large and complex networks.
2. Fast Convergence  
   OSPF quickly updates routing tables when there are changes in the network, which minimizes downtime and improves reliability.
3. Efficient Use of Bandwidth  
   Unlike RIP, which sends updates every 30 seconds, OSPF only sends updates when there is a change. This reduces unnecessary traffic on the network.
4. Supports Hierarchical Design  
   OSPF allows the use of areas (like Area 0 for the backbone), which helps organize and optimize routing in large networks.

**security features:**

Secure access to the console line, Secure Privilege Mode Access (the enable password, the enable secret password), encrypted password to secure access to privileged mode.

 1. Console Password: A password that protects physical access to the router or switch through the console port, it prevents unauthorized users from plugging into the device and gaining access to the CLI

1. Enable password: It adds a layer of protection so that not everyone who accesses the device can make changes.
2. Enable Secret password: A more secure version of the enable password. It also protects access to privileged EXEC mode. It is encrypted by default

Console password

A close-up of a computer code

AI-generated content may be incorrect.

Enable password

A screen shot of a computer

AI-generated content may be incorrect.

Secret password and encrypted passwords

Note: The enable secret password overrides the enable password. So, if both are configured on the router, you must enter the enable secret password to enter privileged EXEC mode.

A screenshot of a computer error

AI-generated content may be incorrect.

1. **Server Installation & Services: Describe the installation and role of at least five servers (e.g., DHCP, DNS, Web, Email, FTP). Include configuration screenshots or commands and justify the choice of each service based on organizational needs.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Server type** | **Role** | **Justification of the use based on connect needs** | **Screen shot of the configuration** |
| **DHCP** | Automatically assigns IP addresses to client devices in the network | Automating IP address assignment reduces manual configuration, speeds up device setup, and minimizes errors. |  |
| **DNS** | Translates domain names into IP addresses. | Enables name-based access to internal web resources, improving user experience and simplifying access. |  |
| **Web** | hosts the organization’s internal website (Intranet). | Provides employees with access to centralized internal information and resources |  |
| **Email** | Handles internal email communication between users. | Facilitates communication among staff and students without relying on external mail providers. |  |
| **FTP** | Allows users to upload and download shared files across departments. | Supports collaborative work and easy file sharing for project teams. |  |

1. **Test Plan Create a test plan outlining what you will test (e.g., connectivity, name resolution), how it will be tested (e.g., ping, traceroute), and expected results.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Test ID** | **Test Objective** | **Test Method/Tool** | **Devices Involved** | **Expected Result** |
| **T1** | Verify device-to-device connectivity | ping | Pc1, pc2, pc3, pc4, pc5, pc6, pc7, pc8,  pc9, pc10, pc11, pc12,  pc13, pc14, pc15 | Ping replies received successfully (between any 2) |
| **T2** | Router Reachability | ping | Pcs and routers | Routers respond to pings |
| **T3** | Test DHCP IP assignment | Ipconfig | PCs, DHCP Server | PC receives IP from correct subnet |
| **T4** | Test DNS name | ping domain | PC2, DNS Server | Domain resolves to correct IP |
| **T5** | Verify web server access | Web browser | PCs, Web Server | Website loads successfully |
| **T6** | Test email sending and receiving | Email client | Pc1, pc5, pc7, pc10 and email server | Email sent and received without error |
| **T7** | Test FTP file | FTP client | Pcs with authorized access, FTP server | Files transferred successfully |
| **T8** | Verify OSPF routing table | show ip route | All routers | OSPF routes are visible |
| **T9** | Test DNS web name | Web browser | PCs, Web and DNS Servers | Domain resolves to correct IP |

1. **Maintenance Schedule Include weekly, monthly, and yearly network maintenance activities. Address updates, backups, monitoring, disaster recovery, and future growth.**

To keep the ConnectX network secure, running smoothly, and ready for future expansion, we need a clear and organized maintenance plan. On a weekly basis, I’ll make sure all devices like routers, switches, and servers are working properly by checking their status and using tools like ping to test connectivity. I’ll also review logs to spot any unusual activity or errors, and double-check that backups are happening as they should. This helps catch problems early before they affect the whole system. On a monthly basis, I’ll focus on performance and security — I’ll look at bandwidth usage, CPU loads, and apply important software or firmware updates. I’ll also audit who has access to what, and run test restores from backups to make sure they actually work. Then on a yearly basis, I’ll update the network documentation, including topology maps and IP addressing plans. I’ll test the disaster recovery plan with a simulation to make sure we’re prepared for any emergency. I’ll also evaluate the hardware to see if anything needs to be upgraded, and plan for any future growth. This way, the network will stay reliable, secure, and ready for whatever the company needs next**.**

**7. Evaluation of Topology and Protocols: Critically analyze the selected logical topology and routing protocol in terms of scalability, performance, and resource utilization.**

The network topology used in this project follows a Hybrid Star design where each office has its own local LAN and devices, but all of them are connected to the HQ in Amman using WAN links. This makes the network more scalable and fault-tolerant, because even if one branch is disconnected, the others can still operate normally. However, the central router can become a single point of failure unless redundancy is implemented. It also allows adding new branches in the future without major redesign.

For routing, we used the OSPF (Open Shortest Path First) protocol. OSPF was chosen because it is more efficient than RIP and supports dynamic routing across a large network like ours. OSPF automatically calculates the best paths between routers and quickly updates routes in case of link failures. This improves performance and reduces manual configuration.

Overall, the network design supports easy connectivity, better resource distribution, and high performance, especially because OSPF helps in managing routing efficiently between multiple sites. The use of both Ethernet (wired) and Wi-Fi (wireless) connections within branches also gives flexibility to users, especially for laptops and mobile devices. It also requires more memory and processing power, especially in large-scale networks

I used a combination of Ethernet (wired connections) and Wi-Fi (wireless access) to provide flexibility and ensure full connectivity for different types of devices and users. Each branch has a switch that connects desktop PCs, printers, and servers using Ethernet cables. This type of connection is fast, stable, and secure, which is ideal for fixed workstations and servers that require reliable performance.

On the other hand, I also added Access Points (APs) in each LAN to support wireless connectivity for laptops. This is especially useful in places like meeting rooms or for employees who move around frequently. The Wi-Fi settings were unified using the same SSID and password for easier access across all branches, while keeping the network secure. Devices that need speed and stability use Ethernet, while portable devices connect through Wi-Fi, making the network more practical and user-friendly.

| **Aspect** | **Hybrid Star Topology** | **OSPF Routing Protocol** |
| --- | --- | --- |
| **Scalability** | Easy to add new LANs or devices without affecting the rest of the network. | Supports large networks with multiple areas and routers. |
| **Performance** | Local traffic is fast and isolated; WAN traffic is efficiently routed. | Fast convergence and intelligent path selection based on bandwidth. |
| **Resource Utilization** | Each LAN uses its own resources (e.g., DHCP, DNS); centralized routing reduces overhead. | Sends updates only when changes occur, saving bandwidth and CPU resources. |

**8. Server Type Justification Evaluate physical server hardware models and operating system choices based on performance, cost, and compatibility. Consider processor type, memory, storage, and form factor in relation to network roles and organizational needs.**

Based on ConnectX's organizational needs and network roles, I recommend the Dell PowerEdge R750 Rack Server. This model offers an excellent balance between performance, cost, and compatibility:

* Processor: Dual Intel Xeon Gold 5318 CPUs provide high core counts suitable for multitasking and running critical network services such as DNS, DHCP, and file sharing. This ensures performance headroom for future expansion.
* Memory: 64 GB ECC DDR4 RAM supports virtualization and ensures data integrity, which is crucial in server environments.
* Storage: 2 TB NVMe SSD delivers high-speed data access and responsiveness, improving the performance of database, file, and web services.
* Form Factor: As a rack-mounted server, it fits efficiently into data center racks, maximizing space usage and facilitating centralized management.
* Operating System: Ubuntu Server 22.04 LTS is selected for its stability, cost-effectiveness (open-source), and excellent support for networking features. It is widely compatible with modern server tools and automation platforms.

This configuration aligns with ConnectX’s requirements for a reliable, scalable server capable of managing both headquarters and branch office services**.[[1]](#footnote-1) [[2]](#footnote-2)**

**9. Hardware & Software Interdependency Describe the journey of a packet as it moves through the network, focusing on how it is encapsulated and de-encapsulated at each OSI layer. Explain how devices like PCs, routers, and switches process the packet using their operating systems (e.g., IOS), and how hardware and software collaborate to ensure successful delivery.**

When a message is sent from Device A to Device B, it travels through the seven layers of the OSI model. Each layer has a specific role and contributes to the successful delivery of the data. The process begins at the Application Layer and ends at the Physical Layer, and then reverses on the receiving device.

**At Device A (Sender):**

1. **Application Layer (Layer 7):**  
   The user interacts with an application (e.g., a web browser or email client). This layer prepares the data for transmission and interacts with lower layers.
2. **Presentation Layer (Layer 6):**  
   Here, the data is formatted (e.g., encoding, compression, encryption) so that both devices understand the format of the transmitted message.
3. **Session Layer (Layer 5):**  
   This layer manages the session or connection between the two devices. It opens, maintains, and closes the communication session.
4. **Transport Layer (Layer 4):**  
   This layer (using TCP or UDP) divides the data into segments, adds port numbers, and ensures reliable transmission using acknowledgments and error checking.
5. **Network Layer (Layer 3):**  
   The segments become packets, and this layer adds the source and destination IP addresses. Routing decisions are made here.
6. **Data Link Layer (Layer 2):**  
   The packets are converted to frames, and MAC addresses are added. This layer ensures node-to-node delivery on the same network segment.
7. **Physical Layer (Layer 1):**  
   Finally, the frames are turned into bits and transmitted through the physical medium (like an Ethernet cable or Wi-Fi).

**At Device B (Receiver):**  
The process is reversed through de-encapsulation:

1. **Physical Layer:** Receives the electrical/optical signal and converts it into bits.
2. **Data Link Layer:** Reconstructs frames, checks for MAC address match, and removes the frame header.
3. **Network Layer:** Extracts the packet, checks the destination IP, and removes the IP header.
4. **Transport Layer:** Reassembles the segments into data, confirms delivery using ACKs (in TCP), and sends it to the correct port (e.g., HTTP).
5. **Session Layer:** Confirms the session is still valid.
6. **Presentation Layer:** Decrypts and decompresses the data if needed.
7. **Application Layer:** Finally, the data reaches the application the user is interacting with, like a web browser or email client.

Throughout the journey, both **hardware** (like NICs, routers, switches) and **software** (like OS, drivers, protocols) work together to ensure smooth communication. For example, the router uses its software (like IOS) to check Layer 3 headers and forward the packet, while switches use Layer 2 MAC addresses for local delivery. Without this collaboration, data wouldn’t travel correctly across the network.

**Section B – Implementation & Enhancement**

**1.Test Execution: Document the actual implementation and include test results compared to your test plan. Include troubleshooting steps if any test failed.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Test ID** | **Test Objective** | **Devices Involved** |  |
| **T1** | Verify device-to-device connectivity | Pc1(Amman) ping pc9(Cairo) |  |
| **T2** | Verify device-to-device connectivity | Pc13(HQ) ping laptop6(Beirut) |  |
| **T3** | Verify device-to-device connectivity | Pc6(Aqaba) ping  Pc3(Irbid) |  |
| **T4** | Verify device-to-device connectivity | Laptop3 (Aqaba) ping pc12(Zarqa) |  |
| **T5** | Router Reachability | Router HQ2 pinged Router HQ1 and the Zarqa office router |  |
| **T6** | Router Reachability | Router Beirut pinged Amman , Irbid , Aqaba, and Cairo offices |  |
| **T7** | Test DHCP IP assignment | PCs, laptops and DHCP Server |  |
| **T8** | Test DNS name | PC2, DNS Server  And any pc in the network to do ping |  |
| **T9** | Verify web server access | PC(any pc in the network), Web Server |  |
| **T10** | Test email sending and receiving | Pc1, pc5, pc7, pc10 and email server |  |
| **T11** | Test FTP file | Pcs(any pc) with authorized access, FTP server |  |
| **T13** | Verify OSPF routing table | HQ1 router |  |
| **T14** | Test DNS web name | PCs, Web and DNS Servers, using domain name |  |

**2. Enhancement Plan Based on your implementation experience, propose improvements such as enhanced security measures, network optimization, or better scalability.**

To improve network efficiency, reduce congestion, and achieve better load balance, I could change the current topology. For example, I might use a mesh topology or hybrid, which provides multiple paths for data and enhances fault tolerance. Alternatively, I could choose a topology that supports easier expansion, such as allowing the addition of new subnets. I could also use IP addressing schemes that support a larger number of host IDs to accommodate future growth.

In terms of security, I can enhance protection by setting stronger passwords on all routers and securing access controls. Additionally, simplifying the network by using fewer routers, where possible, could reduce complexity and potential points of failure.

**3. Critical Reflection Reflect on the challenges faced during design and implementation, decision-making process, and lessons learned for future deployments.**

During the design and implementation of the network, I faced some challenges, particularly in configuring DHCP and applying subnetting across all devices. These tasks required attention to detail and careful planning to avoid IP conflicts. Another major challenge was configuring the routers with OSPF, especially since I had changed the topology multiple times, which required reconfiguring the routers repeatedly.

Although the concepts were not very difficult to understand, the process was time-consuming and repetitive. At times, it felt tedious, but I realized that repetition helped me better understand the commands and improved my confidence in working with routing protocols.

The main lesson I learned is the importance of careful planning before implementation, especially in larger network designs. Additionally, I found that persistence and practice are key to overcoming technical challenges, even when the task becomes repetitive.

1. DELL EMC Poweredge R750 Server Review - newserverlife [↑](#footnote-ref-1)
2. [↑](#footnote-ref-2)