**Networks Project**

Name: Muhamed Ali Jinnah

TABLE OF CONTENTS:

1. Introduction ………………………………………………………………………………………..3

**2. Project Requirements** ……………………………………………………………………………3-4

3. Expected Outcomes ………………………………………………………………………………4

4. Network Design ……………………………………………………………………………………4

4.1. MAN ………………………………………………………………………………………………5

4.2. LAN and V-LAN segments of each Building ……………………………………………………..5-8

5. IP Addressing Scheme and VLAN Assignments ………………………………………………8

5.1 VLAN Subnet Table ……………………………………………………………………………….8

5.2. Router – Router IP Assignment ………………………………………………………………….8

5.3. IP Addressing Table (Aim) …………………………………………………………………….9-10

5.4. V-LAN SETUP …………………………………………………………………………………10-11

5.5. DHCP Configuration on routers with VLAN ……………………………………………………11-13

6. Routing Protocol Configuration …………………………………………………………………13-14

7. Network Connectivity Verification ………………………………………………………………14-17

8. Security Policies & Threat Analysis …………………………………………………………….17

**8.1. Firewall Rulesets Planned and In Place** ……………………………………………………….17-18

8.2. ACL Configurations ……………………………………………………………………………18-19

8.3. Security Threats ………………………………………………………………………………….19

8.4. Mitigation Strategies …………………………………………………………………………….19

9. Conclusion …………………………………………………………………………………………20

10. References ………………………………………………………………………………………20

TABLE OF FIGURES:

|  |  |
| --- | --- |
| **Figure** | **Page No.** |
| 4.1 - 4.6 | 5,6,7 |
| 5.1 - 5.13 | 8-13 |
| 6.1 - 6.3 | 13,14 |
| 7.1 - 7.5 | 14 - 17 |
| 8.1 - 8.5 | 18,19 |

**1. Introduction:**

Being the Network Administrator of Global Enterprices my goal is to build a secure, efficient, and well sized network supporting five distinct segments required by the company.

This report emphasizes on the design, configuration, and security implementation of a network infrastructure for Global Enterprises, a multinational corporation undergoing global expansion.

I have structured this report in order to demonstrate my knowledge and practical skills on network design, routing configuration, and security implementation. By this project, I was able to explore real-world tasks of a network administrator and implement best practices in network segmentation, dynamic routing, and secure communication.

The steps that I have taken for the designing aspect of the network is based on industry standards, making sure that the network layout is efficient and secure. I’ve employed certain design methodologies in order to identify and organize the network layers to optimize communication and data flow. This design enabled me to integrate certain security measures and firewall like function using access control lists (ACLs), and network identification tools to protect the network against threats and maintain good network performance.

I have done my best to clearly document all of my workings in this report.

### ****2. Project Requirements:****

This project is based on the design and implementation of a secure, multi-branch network structure for Global Enterprises using Cisco Packet Tracer. The following are requirements based on the assignments brief:

* **Design a network topology** connecting five distinct networks: Headquarters, Branch Office 1, Branch Office 2, Data Center, and a DMZ.
* **Implement an efficient IP addressing scheme** and configure appropriate VLAN for each of the segment.
* **Verify network connectivity** using ten successful ping tests across different network segments .
* **Configure two different dynamic routing protocols**, one for internal routing and one for external routing .
* **Set security policies**, including firewall rules and access control lists, to protect against unauthorized access and cyber threats.
* **Document all aspects** of this project with diagrams, configuration details, connectivity tests, and a security analysis.

**Tools:**

* **Software Used For Simulation:** I have used Cisco Packet Tracer to simulate the network architecture, test device connectivity and set as well as to check security policies. Cisco Packet Tracer has given me hands-on experience on designing, configuring, and troubleshooting the network.

**3. Expected Outcomes:**

* Set a reliable network structure capable of Global Enterprise’s future global expansion.
* Optimize subnetting methods that ensures smooth inter network communication and ease of management.
* Design good Firewall like ACLs rule sets to prevent unauthorized access and mitigate common cyber threats.
* Properly implement dynamic routing protocol (OSPF) to reduce latency and enhance data transfer efficiency.

**4. Network Design:**

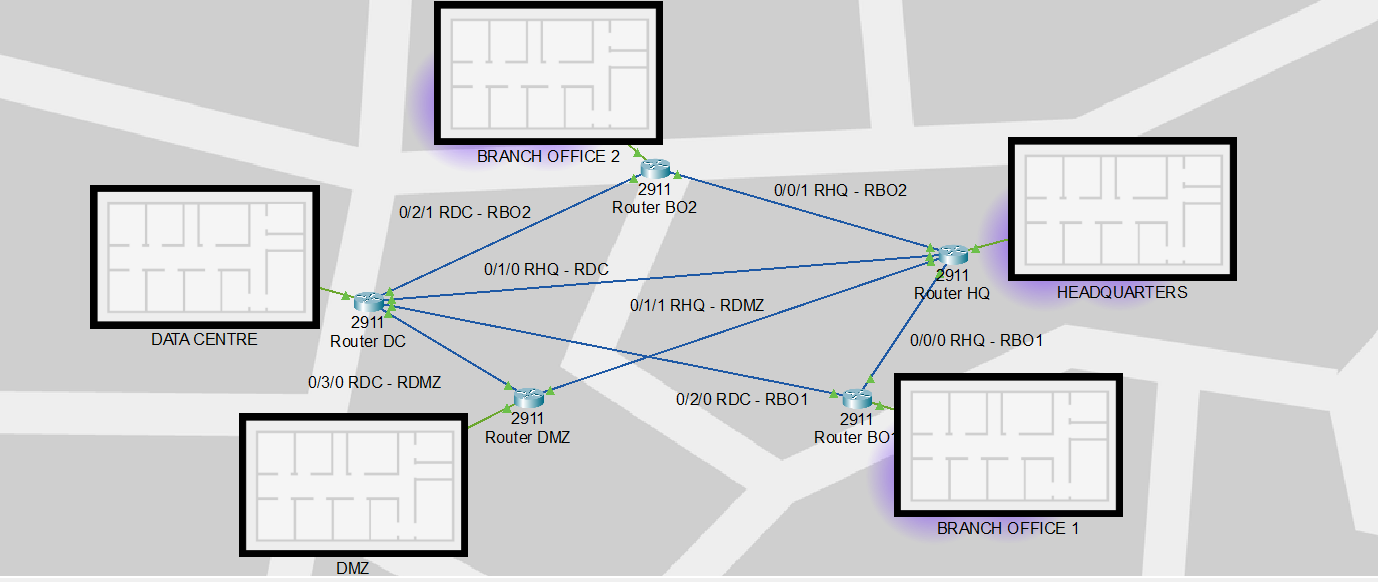
I have designed a network topology in Cisco Packet Tracer that covers the 5 distributed office buildings and the distinct networks within the buildings as required by Global Enterprises. The five distinct networks locations are: Headquarters, Branch Office 1, Branch Office 2, Data Center, and the DMZ.

Each of these networks includes routers for connection between buildings, switches for internal LAN segments, and end devices like PCs, laptops, servers, and printers. And also firewalls are positioned at key junctions to protect internal networks from unauthorized access and also external threats.

For the departments within the organization I will be assuming 2 departments and will be segmenting them into 2 different LAN segments and these departments will be scattered among HQ, BO1 and BO2 networks:

|  |  |  |
| --- | --- | --- |
| DEPARTMENT | LAN SEGMENT (SEGMENT COLOUR) | SUBNET |
| IT | VLAN 10 – Green | 255.255.255.192 /26 |
| Finance | VLAN 20 – Red | 255.255.255.240 /28 |
| DC | VLAN 150 - Orange | 255.255.255.0 /24 |
| DMZ | VLAN 100 - Violet | 255.255.255.0 /24 |

**4.1. MAN :**

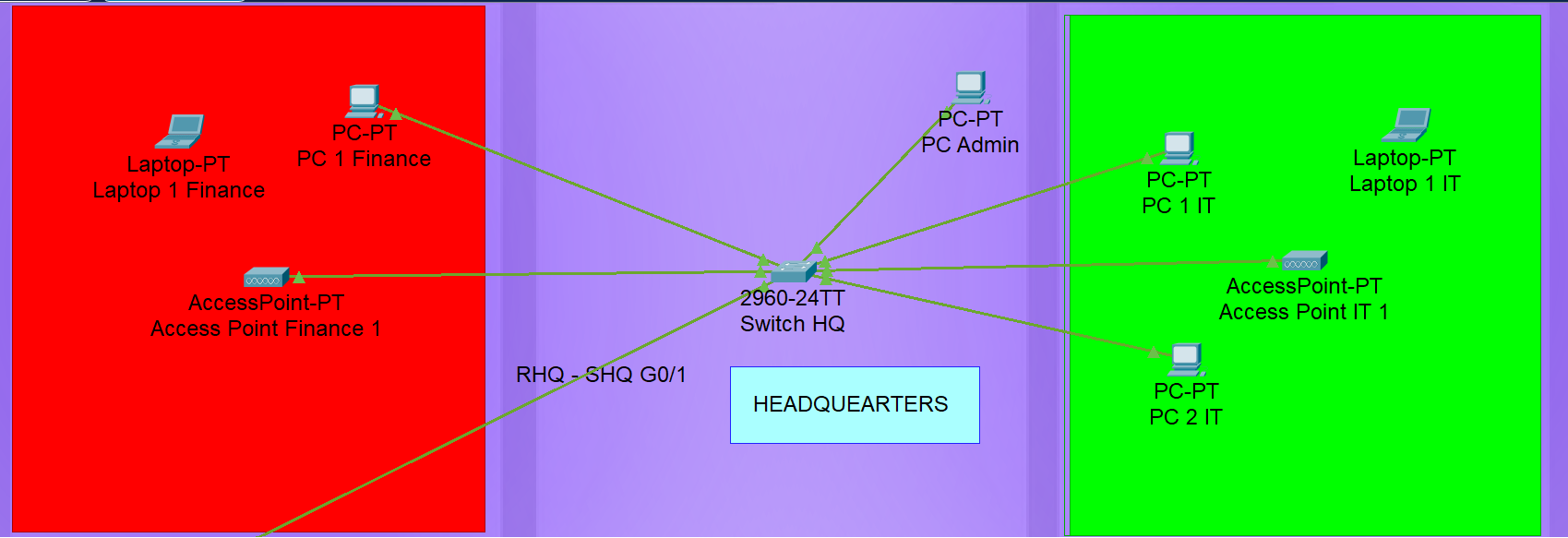




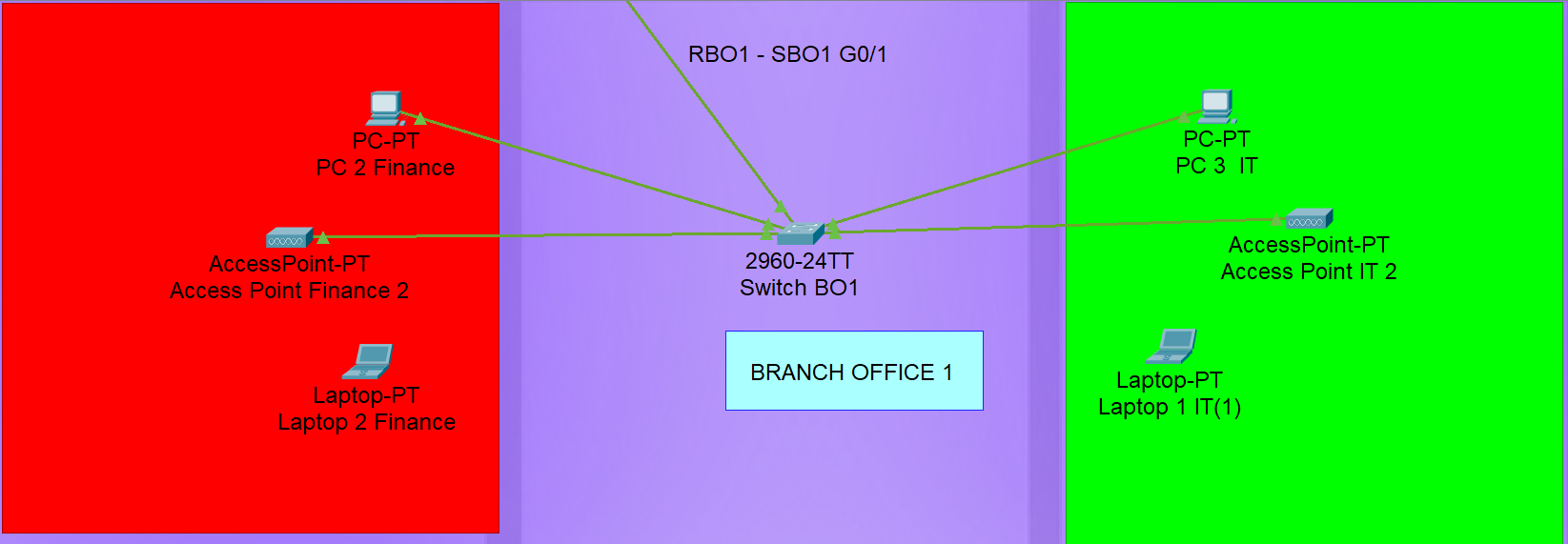
In a real-world deployment, high-speed fiber optics would be used for connection between core routers and data centers, ensuring high bandwidth and minimal latency , but where as in my case I have used Serial DTC cables.

**4.2. LAN and V-LAN segments of each Building:**

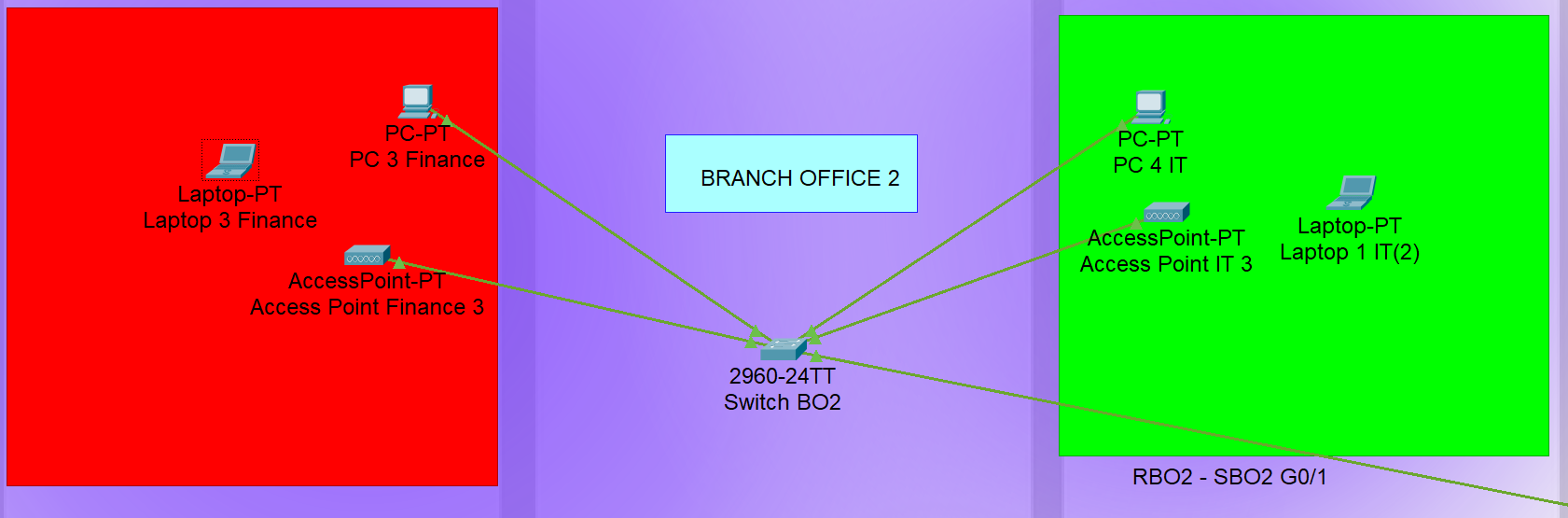
**HQ:** Figure 4.2

****

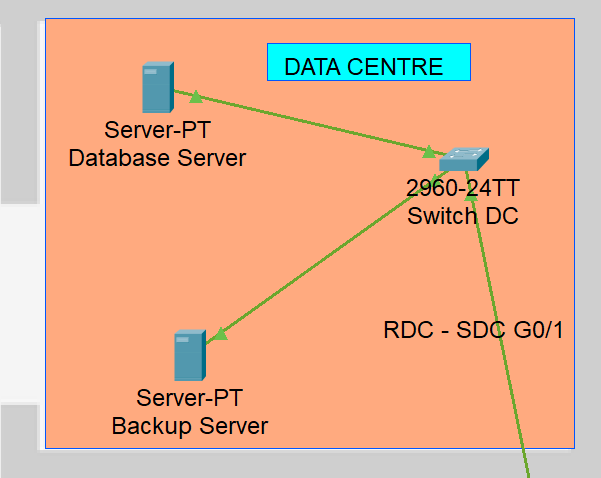
**BO1:** Figure 4.3

****

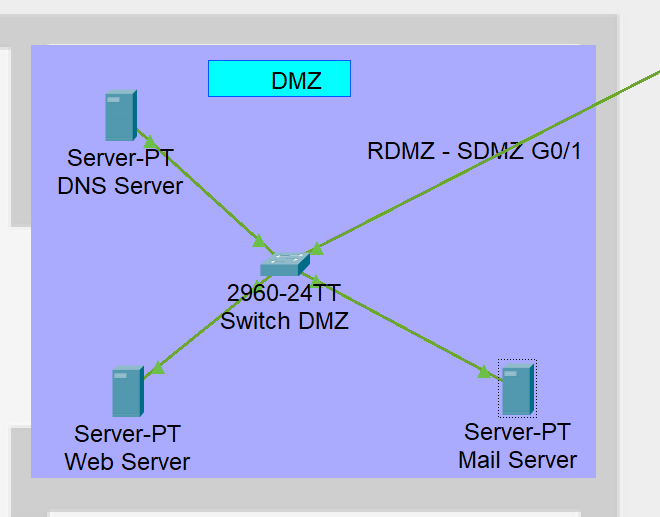
**BO2:** Figure 4.4

****

**DC:** Figure 4.5

****

**DMZ:** Figure 4.6

****

**Key Components:**

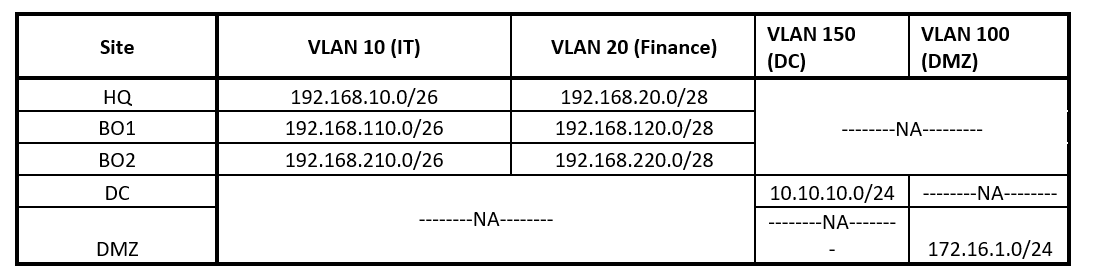
* **Routers:** Cisco 2911 series routers were used for WAN connectivity and routing functions.
* **Switches:** Cisco 2960 switches provided Layer 2 switching capabilities.
* **Access points:** Access points have been used to connect employees to their respective dept network through wireless means
* **End Devices:** PCs and laptops are distributed among all locations to simulate employee and administrative access.
* **Servers:** Each network contains servers for DNS, Mail, and Web services.

The design ensures that the network remains scalable, flexible, and easy to maintain. I have opted for a semi mesh topology to ensure connectivity even if any lines are faulty.

**5. IP Addressing Scheme and VLAN Assignments:**

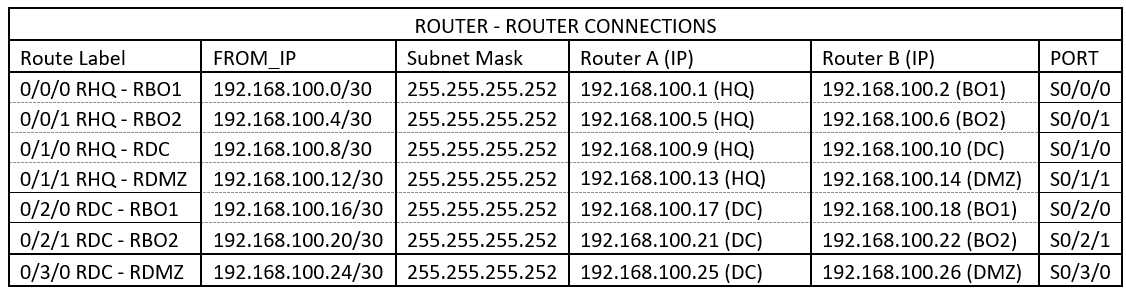
I tried my best to make an efficient IP addressing scheme using private IPv4 addresses and also established VLAN segments. Where each branch was assigned a different subnet using /24, /26 and /28 subnets for easier troubleshooting.

**5.1 VLAN Subnet Table :** Figure 5.1

****

Using VLANs, each department was separated to reduce broadcast domains and increase internal security. Trunk links between switches and routers were configured to carry multiple VLANs.

**5.2. Router – Router IP Assignment:** Figure 5.2

****

**5.3. IP Addressing Table (Aim) :**

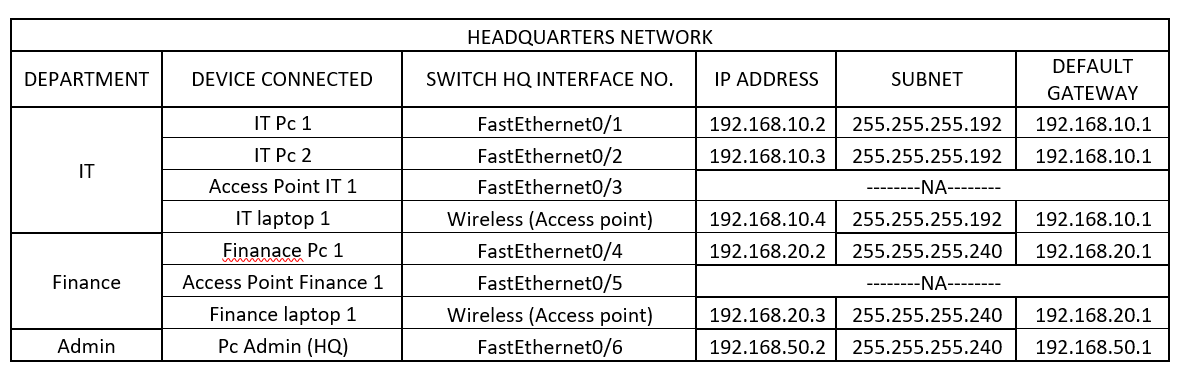
****

Figure 5.3

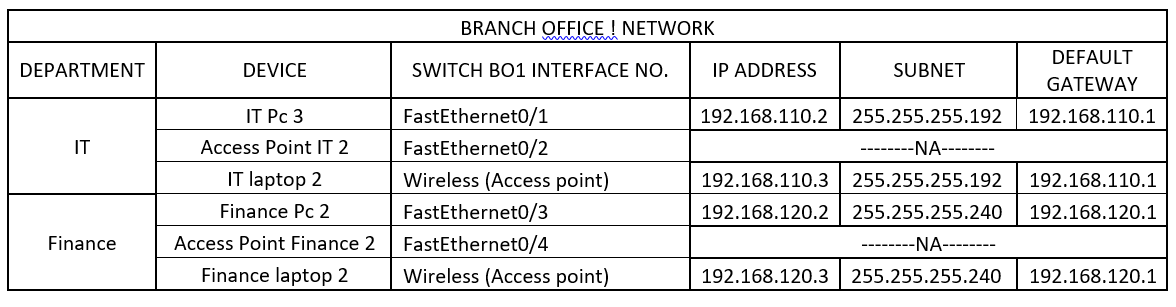
****

Figure 5.4

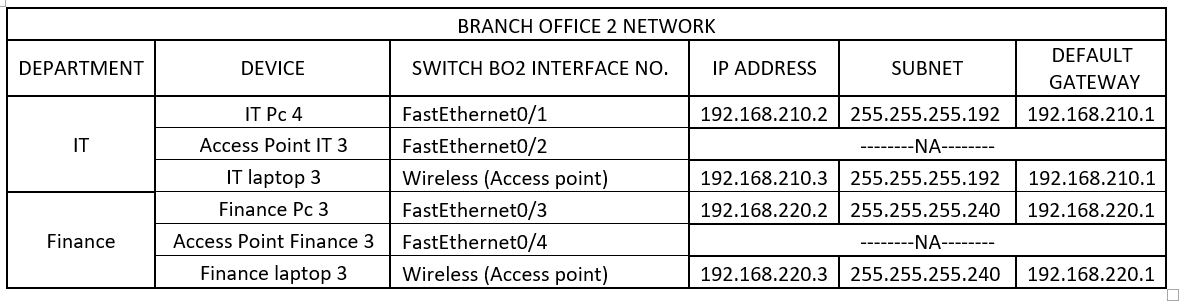
****

Figure 5.5

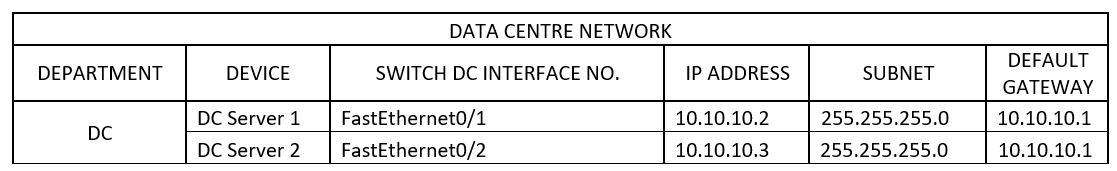
****

Figure 5.6

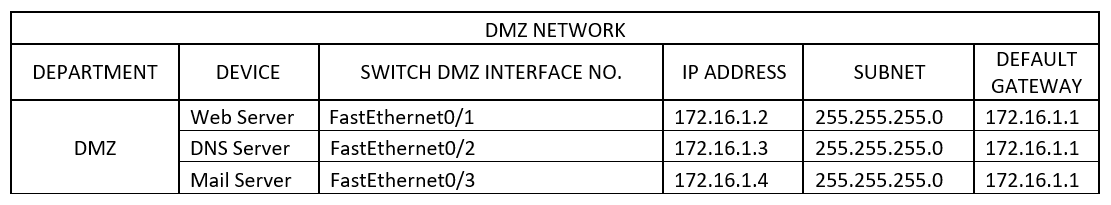
****

Figure 5.6

**5.4. V-LAN SETUP:**

* **Sub-Interface setup on Routers (for VLANs) :** This setup is also known as router on a stick

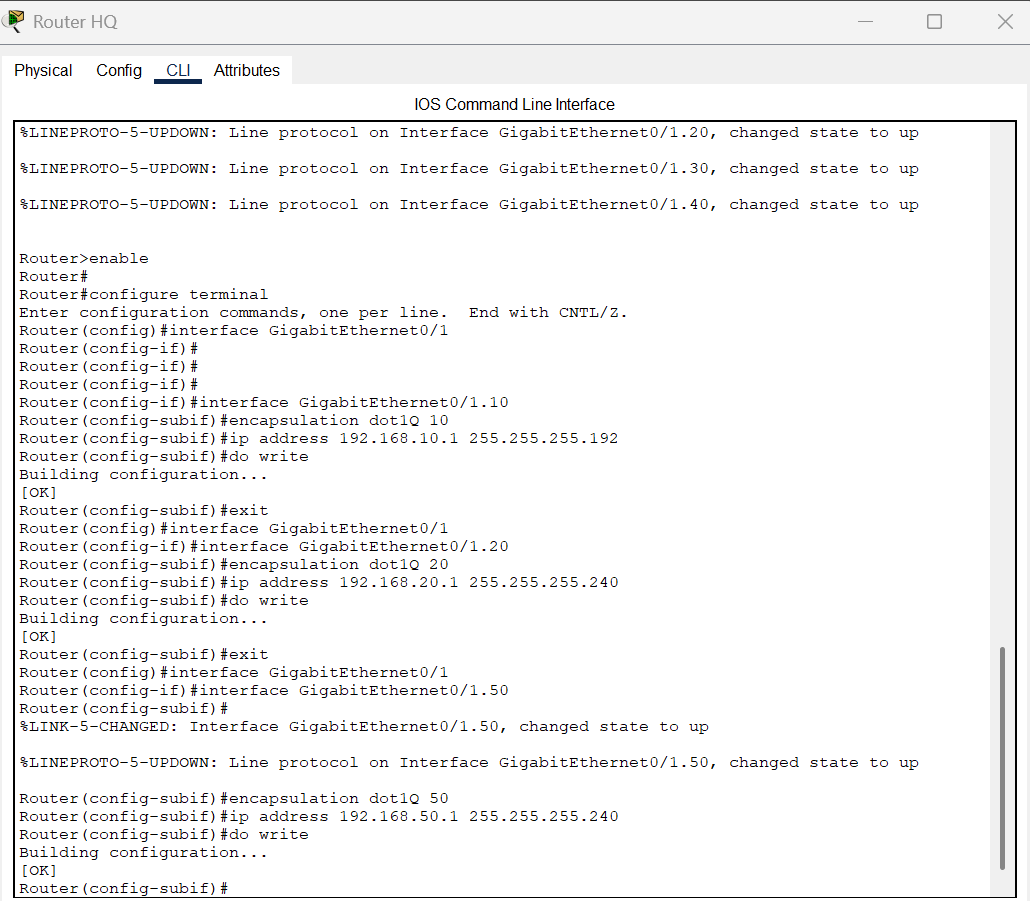
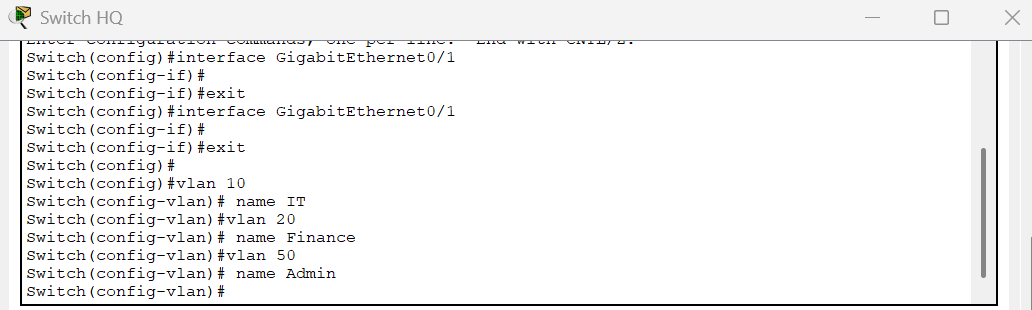
****

Figure 5.7

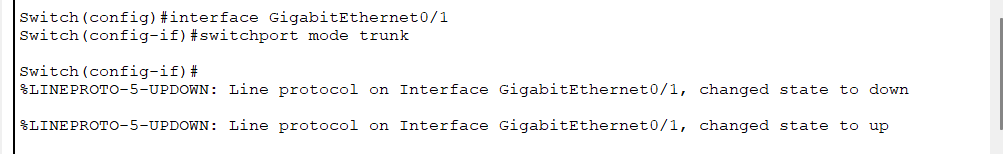
At BO1 and BO2 only VLAN 10 and 20 (no Admin VLAN 50).

* **Creating VLANs on Switches:** Figure 5.8

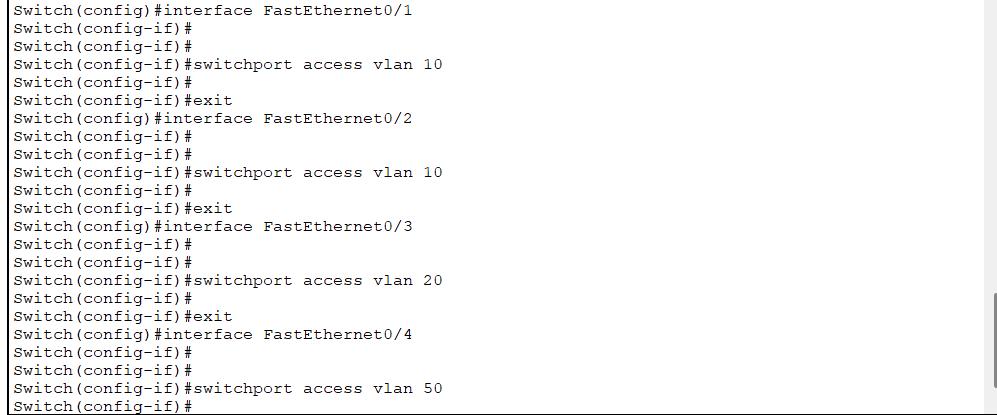
****

At BO1 and BO2 only VLAN 10 and 20 (no Admin VLAN 50) also at Dc and DMZ I set up VLAN 150 and 100 respectively

* **Setting Router – switch connection to VLAN trunk :** Figure 5.9



* **Setting Switch – End devices connections to VLAN access** : Figure 5.10

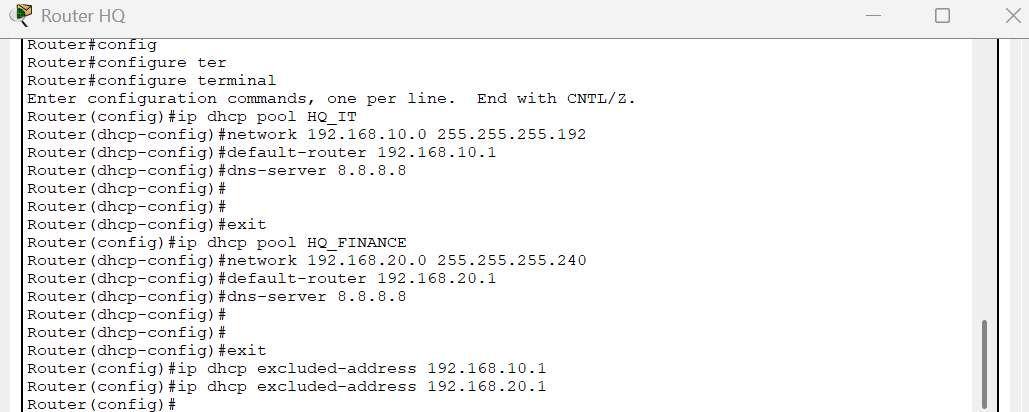


10 for IP , 20 for Finance , 50 for Admin PC

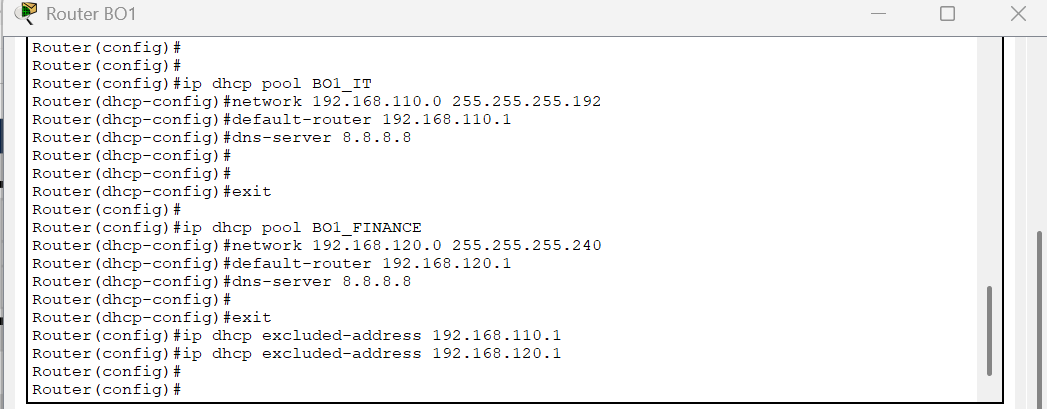
For Proof of concept I have posted only the CLI commands that have been done on HQ router and switch

**5.5. DHCP Configuration on routers with VLAN:**

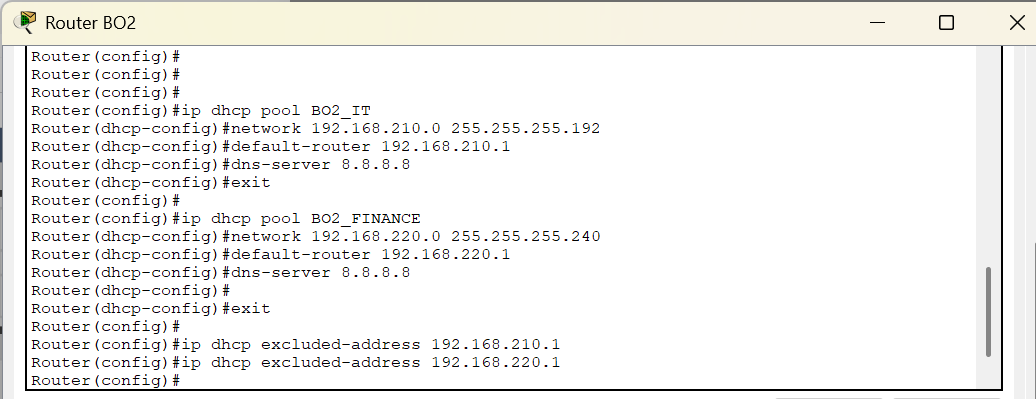
**HQ Router:** Figure 5.11



**BO1 Router:** Figure 5.12

****

**BO2 Router:** Figure 5.13



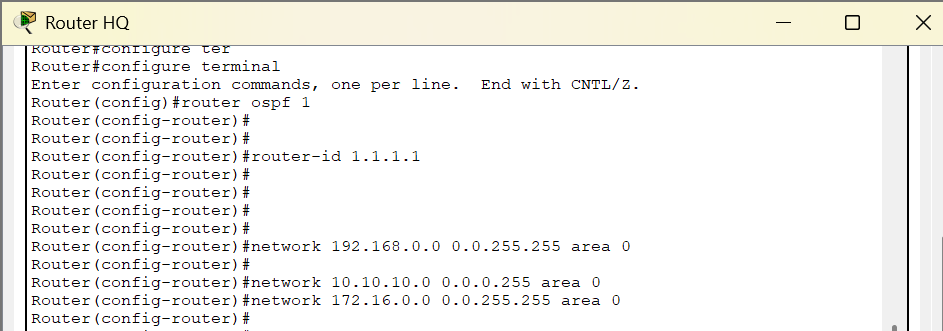
( FOR Data Centre and DMZ I have assigned the Ip statically )

**6. Routing Protocol Configuration**

For Internal routing I have chosen OSPF for its fast convergence and efficient route calculation in internal networks. While searching for dynamic routing options, I also considered EIGRP for internal routing as its simple and has hybrid features, I haven’t used it as it can only be used on Cisco Routers and doesn’t support on other types of routers.

And for external routing I planned to use BGP but I couldn’t find a way to implement it and I didn’t know a way to simulate internet in cisco packet tracer, I planned to use a RIP as I leaned from lectures but it is not viable as OSPF is a better alternative for RIP in terms of bigger network.

**OSPF Configuration Example (Router HQ):** Figure 6.1



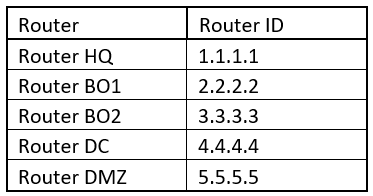


Figure 6.2

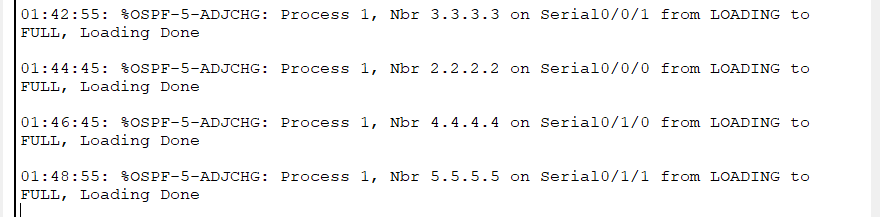


Figure 6.3

### ( Same has been done on ****every other router**** (BO1, BO2, DC, DMZ) )

**7. Network Connectivity Verification**

To verify inter-network communication, I have done 10 ping tests from PC 1 IT to the rest of the devices across the network. Each test showed successful connectivity, proving that routing and subnetting was correctly configured

**Ping Test Results:**

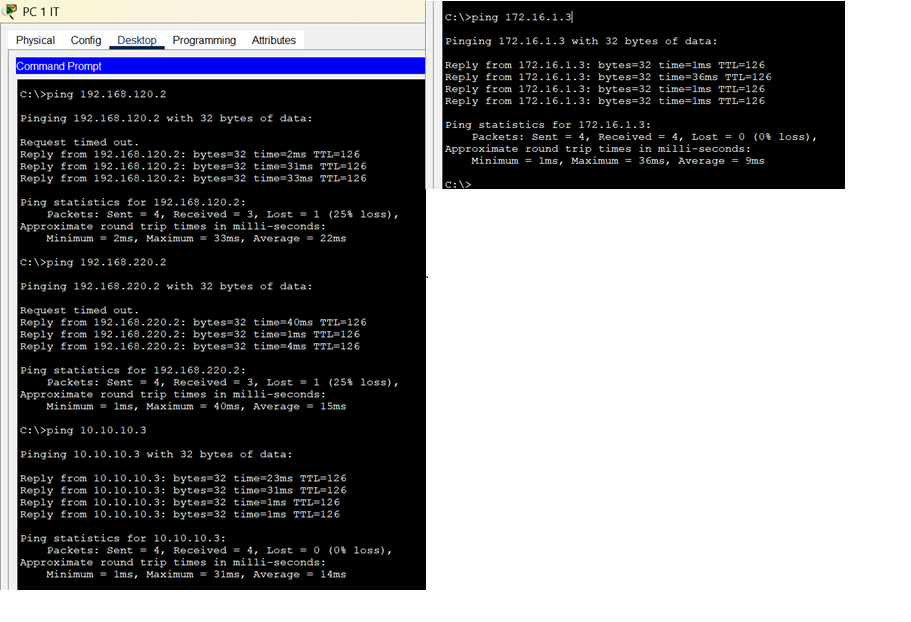


Figure 7.1

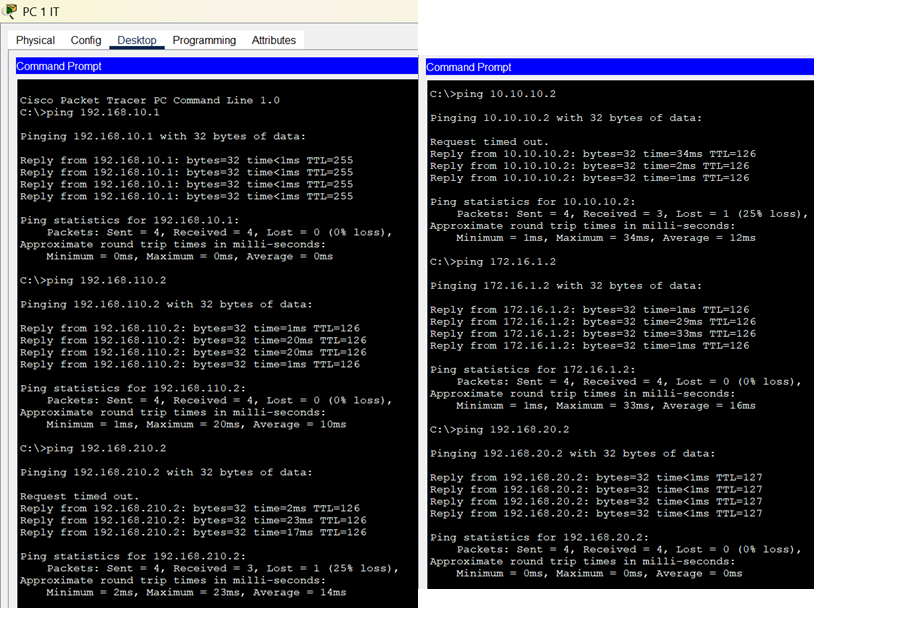


Figure 7.2

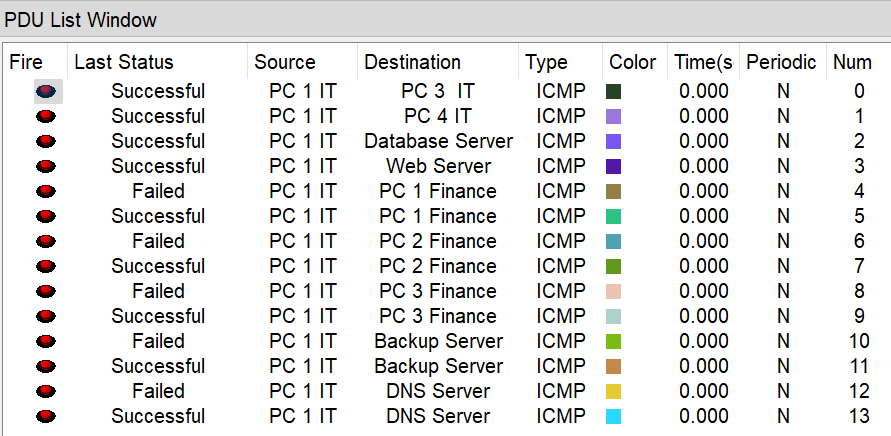


Figure 7.3

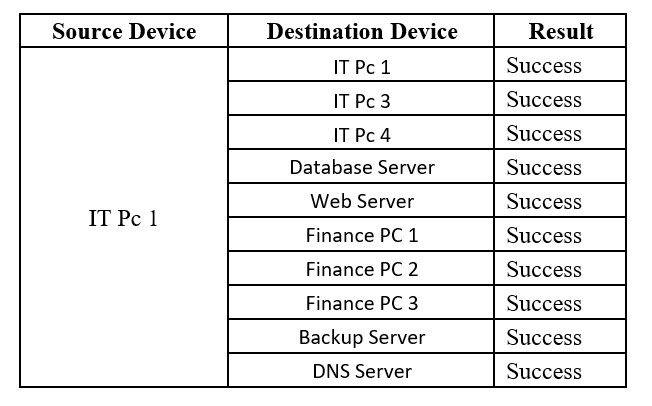


Figure 7.4

All of the ping test was done on Pc 1 IT and was successful , similarly I have tested from other devices they were also successful.

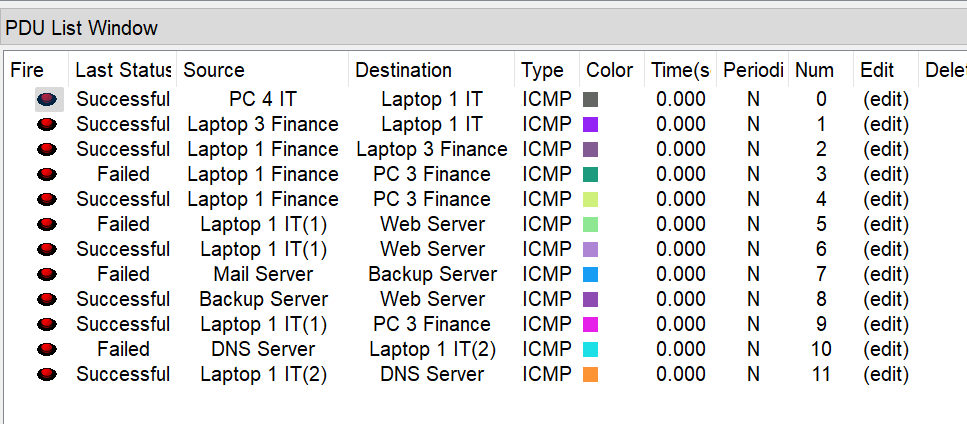


Figure 7.5 – Some random Ping tests between different devices in different networks

**8. Security Policies & Threat Analysis**

### ****8.1. Firewall Rulesets Planned and In Place:****

### For Firewall set up I have used ACL on each of the networks routers for internal communication rather than using a device as firewall.

#### **Between Internet and DMZ (Perimeter Firewall)**

#### These rules are put in place to protect the internal network while allowing public acces to the services provided by the company like the mail server and web server.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ACCESS LIST | Rule ID | Source | Destination | Protocol | Port | Action | Description |
| 104 | 10 | Any (Internet) | Web Server (DMZ) | TCP | 80, 443 | Allow | Allow WWW |
| 104 | 20 | Any (Internet) | Mail Server (DMZ) | SMTP | 53 | Allow | Allow SMTP |
| 104 | 30 | Any | Internal Networks | Any | Any | Deny | Block all access to LAN/Servers |

#### **Between Internal Network and DMZ**

#### **These rules are set to l**imit unnecessary movement and prevent the internal users from accessing the public services in DMZ.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Access list | Rule ID | Source | Destination | Protocol | Port(s) | Action | Description |
| 100 | 50 | HQ all | DMZ | Any | Any | Deny | Block unnecessary communication to DMZ |
| 101 | 30 | BO1 all | DMZ | Any | Any | Deny | Block unnecessary communication to DMZ |
| 102 | 30 | BO2 all | DMZ | Any | Any | Deny | Block unnecessary communication to DMZ |

#### **Between LAN and Data Center**

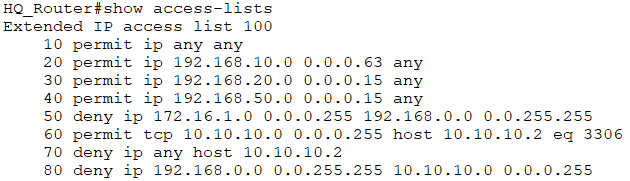
**These rules are in place to** protect the database server and ensure only backend dept has access.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Access list | Rule ID | Source | Destination | Protocol | Port(s) | Action | Description |
| 100 | 60 | Backend VLAN (DC) | DB Server (DC) | TCP | 3306 | Allow | Allow MySQL access from internal users |
| 100 | 70 | Other VLANs (HQ, BO) | DB Server (DC) | Any | Any | Deny | Block database access from non-backend depts |

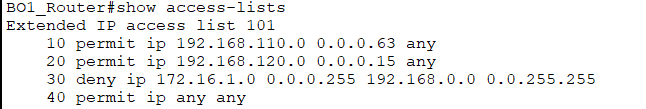
All of these rules have been implemented in the overall network architecture along with some basic rulesets that allow dept-dept communications as well , below is the proof for it.

**8.2. ACL Configurations:**

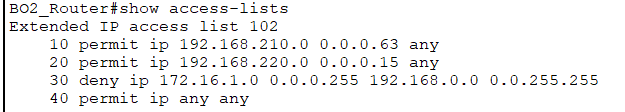
**Accesslist 100:** Figure 8.1



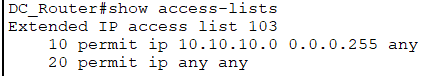
**Accesslist 101:** Figure 8.2



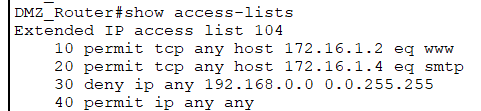
**Accesslist 102:** Figure 8.3



**Accesslist 103:** Figure 8.4



**Accesslist 104:** Figure 8.5



**8.3. Security Threats:**

* Inconsistent ACL / Firewall set up
* External Attacks on DMZ is highly possible
* Employees could be compromised (Hypothetically)
* Unauthorized devices in internal networks could act as DHCP servers
* Man-in-the-Middle (MITM) Attacks on Access points
* Denial-of-Service (DoS) Attacks on web server and other services

**8.4. Mitigation Strategies:**

* IPS and IDS can be used to monitor, detect, and respond to possible threats and suspicious activities within the network.
* Regularly updating the routers, switches, and firewalls in terms of their firmware will help to patch the bugs and improve security features also.
* I have segmented the departments by using VLANs to limit the broadcast domains and restrict any movement between different departments in case of a breach.
* Used WPA2-PSK on access points of each department to add an extra layer of login security.
* Using ACLs I prevented unauthorized access and ensured only authorized users could access their respective devices.
* Used anti-spoofing ACLs on routers to block incoming packets with invalid internal IP addresses.
* Limited DDOS attacks through rate limiting ACLs and continuous network traffic monitoring to detect and control abnormal activity.

**9. Conclusion:**

This project was a highly valuable learning experience. By simulating a real-world enterprise network, I gained practical experience in configuring routers and switches, implementing dynamic routing protocols, and designing IP schemes. Using Cisco Packet Tracer enabled visualization of network behavior and enhanced my troubleshooting skills.

I particularly found VLAN implementation and OSPF configuration challenging but rewarding, as it helped me understand routing tables and inter-VLAN communication and configuration and applying ACLs reinforced the importance of precise access control that’s a great part that ensures security of the network.

I also followed best practices in VLAN configuration by avoiding default VLAN IDs and assigning higher custom numbers (e.g., VLAN 10 for Finance, VLAN 20 for Marketing), which reflects real-world standards and enhances network security and manageability.

I was unable to configure BGP and Internet traffic as I thought to but I set up some ACL and did my best to make a good internal network for Global Enterprices.

Overall, the project gave me good knowledge into the responsibilities of a network administrator and highlighted the importance of layered security in defending against modern cyber threats.

**10. References:**

* Exploring Networking with Cisco Packet Tracer (no date). <https://www.netacad.com/courses/exploring-networking-cisco-packet-tracer?courseLang=en-US>.
* Easttom, C. (2022) Network Defense and Countermeasures. 6th edn. Cengage Learning.
* Forouzan, B.A. (2017) Data Communications and Networking. 5th edn. McGraw-Hill Education.
* Harris, S. and Maymi, F. (2021) CISSP All-in-One Exam Guide. 9th edn. McGraw-Hill Education.
* Keary, T. and Keary, T. (2024) ‘Types of routing Protocols – the ultimate guide’, Comparitech, 14 November. Available at: <https://www.comparitech.com/net-admin/routing-protocol-types-guide/>
* Mitchell, B. (2023) Understanding VLANs and Subnetting. Lifewire. Available at: <https://www.lifewire.com/understanding-vlans-and-subnetting-817963>
* Odom, W. (2020) CCNA 200-301 Official Cert Guide, Volume 1. Cisco Press.
* Scarfone, K. and Hoffman, P. (2009) Guidelines on Firewalls and Firewall Policy (NIST SP 800-41 Rev.1). National Institute of Standards and Technology. Available at: <https://doi.org/10.6028/NIST.SP.800-41r1>
* Stallings, W. (2020) Network Security Essentials: Applications and Standards. Pearson.
* Tanenbaum, A.S. and Wetherall, D.J. (2021) Computer Networks. 5th edn. Pearson.
* Keary, T., & Keary, T. (2024, November 14). *Types of routing Protocols – the ultimate guide*. Comparitech. <https://www.comparitech.com/net-admin/routing-protocol-types-guide/>