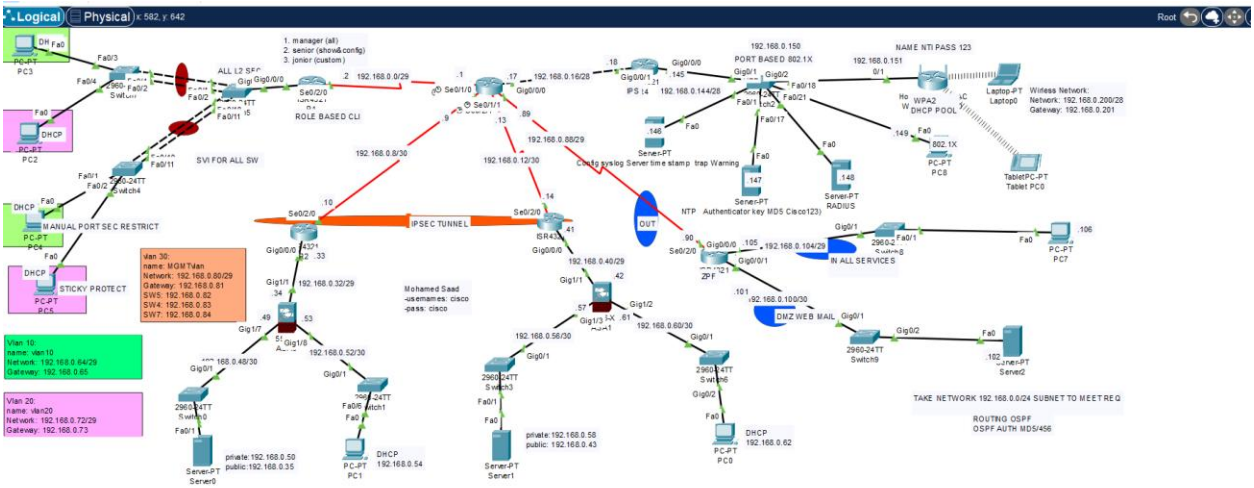
PACKET TRACER LAB

Mohamed Saad Abdelwahab Essa

DEPI_1_ONL1_ISS8_S1E FORTINET CYBERSECURITY ENGINEER

The objective of this final lab is to configure and secure a network consisting of 5 routers, switches, and various network services. This lab involves implementing a wide range of networking and security protocols, including VLANs, DHCP, SSH, VPN, NAT, wireless security, IPS, firewall configuration, and OSPF routing. Below is the breakdown of the tasks:

Topology



1. Basic Router Configuration (All Routers)

- **Router Setup:**
  - Configure **5 routers** (R1 to R5) with synchronized IP addressing and connectivity.
- **Basic Configuration:**
  - Set **hostname** for each router.
  - Configure a **banner** for security and information purposes.
  - Set **time zone** and synchronize the router time.
  - Enable **local authentication** for user access and secure administrative access.
  - Enable **SSH v2** and configure SSH with time-out and authentication retries.
  - Set **SSH time-out** to 100 seconds and **authentication retries** to 3.

---

2. Router 1 Configuration (VLANs, DHCP, Security)

- **VLAN Configuration:**
    - Create **VLAN 10, VLAN 20, and VLAN 30** for management purposes.
    - Assign each VLAN to the corresponding router interfaces and configure **Inter-VLAN routing**.
- **DHCP Configuration:**
    - Configure **DHCP pools** for each VLAN (VLAN 10, VLAN 20, and VLAN 30) to provide IP addresses dynamically to clients.
- **Administrative Access:**
    - Implement **role-based CLI access** with an **access list** for restricted administrative access.
    - Configure access for **3 users** with limited administrative roles.
- **Switch Security:**
    - Configure each switch to enhance security by disabling **DTP (Dynamic Trunking Protocol)**, enabling **Port Security**, and setting up **Spanning Tree Protocol** (STP).
    - On Switch 4, configure **manual MAC address** binding for a specific port (PC 4) and configure **sticky port security** for dynamic MAC learning.
    - Set up **EtherChannel** for uplink connections and ensure the **down EtherChannel** is correctly configured.

---

3. Router 2 and Router 3 Configuration (NAT, VPN)

- **Router 2 Configuration:**
    - Set up **DHCP** for internal networks and **dynamic PAT (Port Address Translation)** for internal hosts.
    - Configure **static PAT** for the **DMZ** (Demilitarized Zone) network.
- **Site-to-Site VPN between R2 and R3:**
    - Implement a **site-to-site VPN** between R2 and R3 to securely connect the internal networks of both routers.

- **Router 3 Configuration:**
    - Configure **DHCP** for internal devices.
    - Set up **dynamic PAT** for the internal network and **static PAT** for the DMZ network.

---

4. Router 4 Configuration (IPS, Wireless Security, RADIUS, Syslog)

- **IPS Configuration:**
    - Configure **IPS (Intrusion Prevention System)** to protect against external threats.
- **Disable Ping from Outside:**
    - Disable ICMP responses from external networks to enhance security.
- **Wireless Security:**
    - Configure **SSID** to **NTI** with WPA2 encryption for security.
    - Implement **802.1X** protocol for PC authentication using **RADIUS**.
    - Configure **EAP (Extensible Authentication Protocol)** for enhanced security during user authentication.
- **NTP Configuration:**
    - Set up an **NTP server** to synchronize time between routers and switches.
- **Syslog Configuration:**
    - Configure **syslog** to send logs to a central **syslog server** for monitoring and auditing.

---

5. Router 5 Configuration (Zone-Based Firewall and OSPF Routing)

- **Zone-Based Policy Firewall (ZPF):**
    - Configure **Zone-Based Policy Firewall** to secure traffic between different zones (Inside and DMZ).
    - Allow specific services (HTTP, HTTPS, and SMTP) from the outside to the DMZ.

- **OSPF Routing:**
    - Configure **OSPF** routing protocol with **MD5 authentication** for all routers to ensure secure routing updates.
    - Configure **OSPF network types** and enable routing for all connected networks.
- **IP Addressing:**
    - Assign any IP address from the **192.168.0.0/24** network range to your own devices and configure static routes where needed.

Conclusion:

By the end of this lab, you will have successfully configured a secure, scalable network infrastructure with proper IP management, VLANs, security features like SSH, port security, VPN, firewall policies, IPS, and routing protocols. This setup ensures a robust network suitable for various business or educational applications, with secure remote access and proper traffic management.