Network Simulation Report

1. Connectivity Tests

Purpose: To ensure that all devices (wired and wireless) across different VLANs and subnets can communicate properly and receive the correct IP settings.

What was done:

- **Ping:** Used ping to test ICMP connectivity between devices in different locations and VLANs.
- **DNS Resolution:** Verified DNS resolution by checking if domain names could be resolved to IPs using the internal DNS server.
- **HTTP Access:** Simulated HTTP access from client PCs to web servers using web browser tools.
- **DHCP Assignments:** Tested DHCP assignments to ensure clients received valid IP addresses from the DHCP server.

Simulation Outcome:

- All devices successfully communicated, confirming proper IP addressing and routing.
- No packet loss observed in ping, meaning stable Layer 3 routing.
- DHCP leases and DNS queries worked as expected.

---

2. Firewall & ACLs

Purpose: To restrict and secure communication between networks and devices based on defined rules.

What was done:

- **Host-based Firewalls:** Configured host-based firewalls on individual PCs in Location A to allow/block certain traffic (e.g., allow HTTP but block ICMP).
- **Network-based Firewall Rules:** Implemented network-based firewall rules between the core router and the switch at Location B.
- **Access Control Lists (ACLs):** Applied Access Control Lists (ACLs) on routers to filter traffic between VLANs.

Simulation Outcome:

- Unauthorized attempts (e.g., pinging restricted servers) were blocked.

- Approved services (HTTP, DNS) were allowed through the firewall, proving policy-based access control works correctly.

---

3. Inter-VLAN Routing

Purpose: To allow devices in different VLANs to communicate through a Layer 3 device.

What was done:

- **Layer 3 Devices:** Used Layer 3 switches and router-on-a-stick configuration to route between VLANs.
- **Configuration:** Configured sub-interfaces on routers or SVI (Switched Virtual Interface) on multilayer switches.
- **Trunk Links:** Ensured trunk links were active between switches and routers.

Simulation Outcome:

- Devices in VLAN 10, 20, 30, etc., could access each other through the core router or switch.
- Verified by ping and service access tests across VLANs (e.g., PC in VLAN 10 accessing server in VLAN 20).

---

4. Wireless Behavior

Purpose: To test secure and seamless wireless connectivity for mobile clients.

What was done:

- **WLC and LWAPs:** Deployed a Wireless LAN Controller (WLC) with Lightweight Access Points (LWAPs).
- **Client Connections:** Connected multiple laptops and smartphones to the wireless network.
- **VLAN Tagging:** Enabled VLAN tagging for wireless clients to segregate them into VLAN 50/60.
- **Monitoring:** Monitored client roaming and connection persistence across APs.

Simulation Outcome:

- Wireless clients received IPs from DHCP and connected to the internet.
- Roaming between access points didn't disrupt sessions.

- Policies were enforced successfully by the WLC.

---

5. Dynamic Routing (OSPF)

Purpose: To automate routing and ensure resilience in case of link failure.

What was done:

- **OSPF Configuration:** Configured OSPF (Open Shortest Path First) between all routers in the ring topology.
- **Verification:** Verified neighbor relationships and LSAs (Link-State Advertisements).
- **Link Failure Simulation:** Simulated a link failure by disabling an interface or connection between routers.
- **Observation:** Observed the recovery behavior and route recalculation.

Simulation Outcome:

- Routes were automatically updated when a link went down.
- Network remained accessible through alternate paths.
- OSPF convergence confirmed network resilience.

---

6. Server Accessibility

Purpose: To ensure that clients in any location can access services (web, DNS, file sharing) hosted on the servers.

What was done:

- **Server Deployment:** Deployed Server0 and MAN-SERVER with services like HTTP, DNS, and DHCP.
- **Security Rules:** Applied firewall rules and ACLs to control access.
- **Access Testing:** Accessed these servers from PCs in Location A, Location B, and external location (LOC/DMZ).

Simulation Outcome:

- Verified access from all locations where rules permitted.
- Blocked traffic when firewall/ACL denied it.
- Demonstrated policy-driven service accessibility.