Testing Scenario:

---

1. Inter-VLAN Communication

Objective: Ensure that devices in different VLANs can communicate where allowed.

Test Steps:

- From the **Test-PC in the IT Department (VLAN 34)**, ping:
    - A **PC in Sales (VLAN 30)** – Expected: Success (allowed inter-departmental communication).
    - A **PLC in Production Zone (VLAN 60)** – Expected: Fail (restricted by ACLs).
    - The **Primary Database Server (Static IP 172.16.209.2)** – Expected: Success.

Expected Result:

- Pings to VLANs allowed by ACLs succeed.
- Pings to restricted VLANs fail, confirming ACLs are functioning.

---

2. Internet Connectivity via NAT (PAT)

Objective: Validate that internal clients can access the internet through NAT.

Test Steps:

- From the **Guest WiFi client (VLAN 10)** and **HR Workstation (VLAN 31)**, try to access an external server (simulate using a cloud DNS or web server).

Expected Result:

- Internet access is successful through NAT configured on core routers (R1/R2).
- HSRP failover maintains connectivity if one router goes down.

---

3. DHCP Operation

Objective: Verify that devices in each department receive correct IPs.

Test Steps:

- Connect a new PC in VLAN 33 (PR Dept).
- Monitor IP assignment from the centralized DHCP server.

Expected Result:

- Device receives an IP within the 172.16.160.1–172.16.167.254 range.
- Gateway and DNS configurations are correct.

---

4. VLAN Segmentation & Security Policies

Objective: Ensure network isolation as per the design.

Test Steps:

- Try pinging between:
  - **Sales (VLAN 30)** and **Finance (VLAN 32)** – Expected: Fail.
  - **Engineering Server (VLAN 21)** to **Design Workstation (VLAN 20)** – Expected: Success.

Expected Result:

- Communication is restricted between business units unless explicitly allowed.
- Engineering zone allows intra-zone communication.

---

5. Redundancy and Failover (HSRP + Redundant Links)

Objective: Test high availability in case of router failure.

Test Steps:

- Shut down **Router R1**.
- Monitor internet connectivity from IT workstation.

Expected Result:

- Traffic reroutes through **Router R2** using HSRP.
- No downtime observed for end users.

---

6. Wireless Connectivity

Objective: Confirm proper SSID-based wireless access.

Test Steps:

- Connect a wireless laptop to "Sales_WiFi" and access internal resources.
- Connect another device to "Guest_WiFi" and attempt access to internal VLANs.

Expected Result:

- **Sales_WiFi** user has internal access.
- **Guest_WiFi** user is isolated (access only to the internet).

---

7. Remote Management via SSH

Objective: Validate secure management access.

Test Steps:

- From **Test-PC**, SSH into core switch and router using configured credentials.

Expected Result:

- SSH session is established securely.
- Device configuration is accessible only with proper login.

---

8. Monitoring and Logging (SNMP/Syslog)

Objective: Ensure real-time monitoring is operational.

Test Steps:

- Force a port security violation by plugging in a rogue device to an access port.

- Observe if alert is generated in the Syslog server.

Expected Result:

- Port enters shutdown state.
- SNMP trap or Syslog message is logged confirming the violation.

Summary of Results

Test Case	Expected Outcome	Status
Inter-VLAN Communication	Allowed where configured	Success
NAT Internet Access	Works via core routers	Success
DHCP Allocation	Dynamic IPs assigned correctly	Success
VLAN Security	Isolation maintained	Success
Redundancy	No downtime during failover	Success
Wireless SSIDs	Secure access & guest isolation	Success
SSH Management	Secure remote access works	Success
Port Security & Logging	Unauthorized device blocked & logged	Success

---