Problem: A small company running on a flat network and employees from other departments might gain potentially unauthorized access of other department devices. That might arise the security concern and may lead to unauthorized access to the system files and resources. They wanted to have separate networks for departments such as IT, FINANCE, SALES and GUEST. By creating a separated network for each group of devices, we can reduce the attack surface and shrink down the broadcast domain for better efficiency and speed.

OBJECTIVES:-

- Secure and Efficient Network
- Internet should be accessible by everyone
- Only IT department can access others departments network
- Create isolated broadcast domains for each groups (IT, HR, Finance, Guest & Security)

IP SCHEME & VLANs:-

- Small company usually have up to 10-20 employees per department
- We use VLSM ranging from /25 to /27 based on department size
- One VLAN per department

Total IP addresses:

- Assuming 20 employees × 3 devices per employee = 60 hosts per department.
- For 50% future growth: 60 × 1.5 = 90 IPs per department (future proof).
- Current subnets: 5 departments + 2 point-to-point links = 7 subnets.
- With 50% growth: 7 × 1.5 = 10.5, rounded up to 11 subnets.
- Total IP requirement: 90 IPs × 11 subnets = 990 IPs.
- To contain 990 IPs, we need a parent block with at least 1024 IPs.

Parent IP block:-

- 192.168.0.0/22

Network Services:-

- DHCP Server
- NAT (PAT)
- File Server
- Printer
- Wireless Network using WLC & L-APs.
- Firewall

Configurations:-

- Create VLANs & SVIs
- Assign IP addresses
- Enable Portfast on Access Ports
- Enable Trunking for WLC & APs
- Enable Intervlan Routing on L3 Switch
- Apply ACLs
- Add ISP routing to Edge Router
- Set-up Firewall

SSIDs & VLAN Mapping:-

- SSID: Guest -- Mapped to VLAN 50
- SSID: IT -- Mapped to VLAN 30
- SSID: HR -- Mapped to VLAN 10
- SSID: Finance -- Mapped to VLAN 20
- SSID: Security -- Mapped to VLAN 40

Security Features and Practices:-

- **ACLs Planning**
  - Block guest to access other Internal VLANs
  - Allow IT VLAN to access all VLANs
  - Allow DHCP from IT VLAN to access other VLANs
  - Other departments shouldn't be able to access each other networks
- **DHCP Snooping**
- **Firewall Rules**
- **Port Security**
- **Device Hardening (AAA Framework, Role Based Access Control, Syslog and Local User Databases)**

IP Address Table

Departments and other Links	Number of Host IP	Network Address	Gateway	Usable IP Range	VLAN ID
Guest	120	192.168.0.0/25	192.168.0.1	192.168.0.1 - 192.168.0.126	50
Finance	90	192.168.0.128/25	192.168.0.129	192.168.0.129 - 192.168.0.254	20
HR	60	192.168.1.0/26	192.168.1.1	192.168.1.1 - 192.168.1.62	10
IT	50	192.168.1.64/26	192.168.1.65	192.168.1.65 - 192.168.1.126	30
Security	25	192.168.1.128/27	192.168.1.129	192.168.1.129 - 192.168.1.158	40
Edge Router Link	2	192.168.1.192/30	NA	192.168.1.193 - 192.168.1.194	NA
Firewall Link	2	192.168.1.196/30	NA	192.168.1.197 - 192.168.1.198	NA

SW-CORE Port-to-VLAN Mapping

VLAN ID	VLAN NAME	Access Ports (Range)	Trunk Ports
10	HR	Gig1/0/7 - 10	-
20	Finance	Gig1/0/11 - 14	-
30	IT	GIg1/0/2 - 3	-
40	Security	Gig1/0/15 - 18	-
50	Guest	Gig1/0/19 - 20	-
-	-	-	Gig1/0/4 - 6

Logical Network Topology