Problem Statement for Minor Project:

Develop a scalable network for a manufacturing plant, integrating different units like Assembly, Quality Control, Logistics, and Administration. The network must support:

- Seamless communication between production lines and inventory systems.

- VLAN segmentation for secure communication between IoT devices, SCADA systems, and enterprise networks.

- Real-time monitoring to detect and respond to network issues without disrupting operations.

Challenge:

Ensure high availability and protection against industrial cyber threats targeting OT systems.

Scenario:

Manufacturing Plant with different zones likes Production Zone, Engineering Zone, Corporate Zone, Storage Zone, DMZ (Demilitarized Zone), Guest & Miscellaneous Areas with VLAN segmentation, IoT devices, SCADA systems.

Scenario Overview: Designing and implementing a comprehensive network for a manufacturing plant which deals with both manufacturing and trading. The plant has five zones, with multiple departments distributed across in each zone. The network must ensure seamless wired and wireless connectivity, VLAN segmentation for secure communication between IoT devices, SCADA systems, and enterprise networks, real-time monitoring to detect and respond to network issues without disrupting operations, ensuring high availability and protection against industrial cyber threats targeting OT systems. Additionally, the network should be future-proofed to handle scalability.

Zone Layout:

❖ Production Zone: Includes industrial devices such as Programmable

Controllers (PLCs), sensors, and actuators that control and monitor production

lines.

❖ Engineering Zone: Houses engineering workstations and servers used for desicung and maintaining production systems.

- Corporate Zone: Supports administrative systems for HR, finance, and general operations.
- Storage Zone: Contains servers for storing production data, inventory management systems, and backups.
- Guest & Miscellaneous Areas (Separate VLANs within Corporate Zone for Limited Access): Contains WAP for guests and outside visitors.
- DMZ (Demilitarized Zone): Hosts public-facing services such as vendor portals and communication systems.

This segmentation enhances performance, ensures security, and supports scalability while protecting critical systems from external threats.

Department Distribution:

- **Production Zone:**
  - Industrial devices (PLCs, sensors, actuators)
  - Manufacturing production lines
- **Engineering Zone:**
  - Engineering workstations
  - Design and maintenance servers
- **Corporate Zone:**
  - Sales and Marketing
  - Human Resources
  - Finance and Accounts
  - Administrator and Public Relations
  - IT Department
- **Storage Zone:**
  - Inventory management systems
  - Production data servers

  - Backup storage
  - Logistics
- **DMZ (Demilitarized Zone):**
  - Vendor Portals & Communication Systems
  - Security Department
  - Server Room
- Guest & Miscellaneous Areas
  - Reception and Visitor Lounge
  - Cafeteria

Network Design:

Hierarchical Network Design Mapping

A **hierarchical network** is structured into three layers:

1. Core Layer (High-Speed Backbone)

- Connects all major zones with high-speed switching and redundancy.
- Typically includes **high-performance routers and core switches**.
- Provides fast, resilient connectivity between data centers, corporate networks, and production systems.
- **Zones Connected:**
  - Production Zone
  - Engineering Zone
  - Corporate Zone
  - Storage Zone
  - DMZ

2. Distribution Layer (Policy Enforcement & Security)

- Aggregates connections from different zones.

- Implements **VLANs, routing, firewall rules, and network access control** to enforce security.
- Manages **Quality of Service (QoS)** for traffic prioritization (e.g., real-time production data).
- **Departments Managed:**
    - Security controls for **Production & Engineering Zones** (OT Security)
    - Secure segmentation of **Corporate IT & Storage Zone**
    - Controlled access for **DMZ services**

3. Access Layer (Edge Devices & User Connectivity)

- Provides connectivity for **end devices** such as workstations, IoT devices, and wireless access points.
- Implements **Access Control Lists (ACLs), VLAN tagging, and security policies** to restrict unauthorized access.
- **Devices Connected:**
    - **Production Zone**: PLCs, sensors, industrial controllers
    - **Engineering Zone**: Workstations, CAD/PLM servers
    - **Corporate Zone**: Employee workstations, office networks
    - **Storage Zone**: Inventory systems, database servers
    - **DMZ**: External vendor portals, firewalls

VLANs and IP Addressing:

- Each department should be in a separate VLAN and subnet to segregate traffic and enhance security.
- Use the base network **172.16.0.0/16** for subnetting and allocate IP addresses dynamically (DHCP) for devices in each department.

- Static IPs will be assigned for servers and critical devices in the Server Room.

. Multilayer Switches ↔ Firewalls (`/30 = 255.255.255.252`)

Link	Subnet	Subnet Mask	ML Switch IP	Firewall IP
MLS1 ↔ FW1	172.16.240.0/30	255.255.255.252	172.16.240.1	172.16.240.2
MLS1 ↔ FW2	172.16.240.4/30	255.255.255.252	172.16.240.5	172.16.240.6
MLS1 ↔ FW3	172.16.240.8/30	255.255.255.252	172.16.240.9	172.16.240.10
MLS2 ↔ FW1	172.16.240.8/30	255.255.255.252	172.16.240.9	172.16.240.10
MLS2 ↔ FW2	172.16.240.12/30	255.255.255.252	172.16.240.13	172.16.240.14
MLS2 ↔ FW3	172.16.240.28/30	255.255.255.252	172.16.240.29	172.16.240.30
MLS3 ↔ FW1	172.16.240.16/30	255.255.255.252	172.16.240.17	172.16.240.18
MLS3 ↔ FW3	172.16.240.32/30	255.255.255.252	172.16.240.30	172.16.240.29
MLS3 ↔ FW2	172.16.240.20/30	255.255.255.252	172.16.240.21	172.16.240.22

🔁 2. Firewalls ↔ Routers (`/30 = 255.255.255.252`)

Link	Subnet	Subnet Mask	Firewall IP	Router IP
FW1 ↔ R1	172.16.240.24/30	255.255.255.252	172.16.240.25	172.16.240.26
FW1 ↔ R2	172.16.240.28/30	255.255.255.252	172.16.240.29	172.16.240.30
FW2 ↔ R1	172.16.240.32/30	255.255.255.252	172.16.240.33	172.16.240.34
FW2 ↔ R2	172.16.240.36/30	255.255.255.252	172.16.240.37	172.16.240.38

☁️ 3. Routers ↔ Cloud (`/30 = 255.255.255.252`)

Link	Subnet	Subnet Mask	Router IP	Cloud Gateway IP
R1 ↔ Cloud	172.16.240.40/30	255.255.255.252	172.16.240.41	172.16.240.42
R2 ↔ Cloud	172.16.240.44/30	255.255.255.252	172.16.240.45	172.16.240.46

Each `/30` subnet has:

- **Network address** (first IP, e.g., `172.16.240.0`)
- **2 usable host IPs** (e.g., `.1` and `.2`)
- **Broadcast address** (last IP, e.g., `.3`)

- **VLAN and Subnet Allocation:**

- **VLAN Assignment and Subnet Mapping**

Zone	Department	VLAN ID	Subnet	Subnet Mask	IP Range
Production Zone	Industrial Devices (PLCs, Sensors, Actuators)	60	172.16.0.2/20	255.255.240.0	172.16.0.1 – 172.16.15.254
	Manufacturing Production Lines	11	172.16.16.2/20	255.255.240.0	172.16.16.1 – 172.16.31.254
Engineering Zone	Engineering Workstations	20	172.16.64.2/19	255.255.224.0	172.16.64.1 – 172.16.95.254
	Design & Maintenance Servers	21	172.16.96.2/19	255.255.224.0	172.16.96.1 – 172.16.127.254
Corporate Zone	Sales & Marketing	30	172.16.128.2/20	255.255.240.0	172.16.128.1 – 172.16.143.254
	Human Resources	31	172.16.144.2/21	255.255.248.0	172.16.144.1 – 172.16.151.254
	Finance & Accounts	32	172.16.152.2/21	255.255.248.0	172.16.152.1 – 172.16.159.254
	Administrator & PR	33	172.16.160.2/21	255.255.248.0	172.16.160.1 – 172.16.167.254
	IT Department	34	172.16.168.2/21	255.255.248.0	172.16.168.1 – 172.16.175.254
Storage Zone	Inventory Management	40	172.16.192.2/22	255.255.252.0	172.16.192.1 – 172.16.195.254
	Backup Storage	42	172.16.200.2/22	255.255.252.0	172.16.200.1 – 172.16.203.254
	Logistics	43	172.16.204.2/22	255.255.252.0	172.16.204.1 – 172.16.207.254

Zone	Department	VLAN ID	Subnet	Subnet Mask	IP Range
DMZ Zone	Vendor Portals & Security	50	172.16.208.2/24	255.255.255.0	172.16.208.1 - 172.16.208.254
	Server Room (Static IPs)	51	172.16.209.2/25	255.255.255.128	172.16.209.1 - 172.16.209.126
	Security Department	52	172.16.210.2/25	255.255.255.128	172.16.210.1 - 172.16.210.126
Guest & Public Access	Cafeteria WiFi (Guests Only)	10	172.16.216.2/24	255.255.255.0	172.16.216.1 - 172.16.216.254
	Reception & Visitor Lounge	61	172.16.217.2 /24	255.255.255.0	172.16.217.1 - 172.16.217.254

Static IP Assignments for Critical Devices in Server Room:

Device	Static IP
Main Firewall	172.16.209.1
Primary Database Server	172.16.209.2
Secondary Database Server	172.16.209.3
Web Server	172.16.209.4
Backup Server	172.16.209.5
Active Directory Server	172.16.209.6
Network Switch 1	172.16.209.10
Network Switch 2	172.16.209.11
Network Printer	172.16.209.20

Routing:

- Use **OSPF** as the routing protocol to advertise internal routes across the network.
- Configure **NAT Overload (PAT)** on the core routers for internet access.

Wireless Connectivity:

- Deploy one **Cisco Access Point (AP)** per department for mobile devices, smartphones, and laptops to connect wirelessly.
- Use SSIDs to each department (e.g., "Sales_WiFi," "HR_WiFi") with WPA3 encryption for security.specific
- Set up a **Guest WiFi network** isolated from the corporate network.

DHCP and IP Allocation:

- Configure a **dedicated DHCP server** in the Server Room to dynamically allocate IPs to all devices (except those in the server room, which use static IPs).
- Each router will act as a DHCP relay for devices on its floor.

Redundancy:

- Use two core routers connected to two ISPs with static public IPs (195.136.17.0/30 and 195.136.17.4/30) for internet redundancy.
- Use **HSRP (Hot Standby Router Protocol)** or similar for failover between core routers.
- Configure redundant links between distribution and access layers.

Security:

- Deploy a **firewall** in the Server Room to control incoming and outgoing traffic.

- Enable **port security** on all access switches to prevent unauthorized devices.
    - For all other zones except DMZ, allow only one device per switchport using the sticky MAC method, with violation mode set to "shutdown."
- Configure **SSH** on all routers and multilayer switches for secure remote management.
- Use **ACLs** to restrict access to sensitive resources.

Testing and Monitoring:

- Add a **Test-PC** in the IT department to test connectivity and remote login via SSH.
- Configure SNMP and Syslog for network monitoring.
- Test inter-VLAN communication, internet access, and failover mechanisms.

Future-Proofing:

- Reserve unused VLANs for future departments or expansions.
- Implement scalable cabling infrastructure (Cat6 or fiber optic) to support higher speeds.
- Ensure devices support IPv6 for future adoption.

Technologies and Tools Used:

1. **Cisco Packet Tracer** for simulation and implementation.

2. **Hierarchical Network Design** for scalability and redundancy.
3. **VLANs and Inter-VLAN Routing** for traffic segregation and communication.
4. **OSPF Routing** for dynamic route advertisement.
5. **Port Address Translation (PAT)** for internet access.
6. **Port Security** to restrict unauthorized access.
7. **SSH and ACLs** for secure management and resource control.
8. **DHCP Server** for dynamic IP allocation.
9. **Wireless Access Points** for seamless WiFi connectivity.
10. **SCADA Network Security** to protect industrial control systems from cyber threats.
11. **Real-time Network Monitoring (SNMP, Syslog, NetFlow)** to detect and respond to issues proactively.
12. **Industrial Firewalls & Intrusion Prevention Systems (IPS)** to safeguard OT (Operational Technology) networks.
13. **Redundant Links & Failover Mechanisms (HSRP, VRRP)** to ensure high availability.
14. **IoT Device Segmentation** for secure communication between sensors, actuators, and enterprise systems.
15. **Network Time Protocol (NTP)** for synchronized time across all network devices.
16. **Zero Trust Security Model** to enforce strict access controls for critical systems.

17. **Multi-Factor Authentication (MFA) & Role-Based Access Control (RBAC)** for network security.