Network Design Request for Project

---

1. Project Overview:

We are requesting a full network design for a **multi-branch organization** including a **main headquarters**, multiple **branch offices**, and integration of a **Data Center** and **DMZ zone**.
The design should prioritize **security, high availability, redundancy, and centralized services** (such as DHCP, Syslog, NTP, and TFTP).

---

2. Scope of Work:

- Design a **Layer 2/3 network** that supports multiple VLANs and departments.
- Implement **firewall policies** to control traffic between different network segments.
- Enable **redundancy** at core devices using technologies like **HSRP** or **EtherChannel**.
- Provide **secure remote access** via **IPsec VPN tunnels** between branches and HQ.
- Set up network services servers (Syslog, DHCP, DNS, AAA, TFTP, NTP) distributed between the **Data Center** and the **DMZ** according to best practices.
- Enable **Voice VLAN** for IP Phones with proper DHCP Option 150.
- Configure **DHCP snooping**, **Port Security**, and **Dynamic ARP Inspection** for Layer 2 security.
- Configure firewall to allow internal services (Syslog, NTP, TFTP) and external services (web browsing, mail).
- Implement proper **logging and monitoring** for network activities.
- Prepare full **network documentation**: topology diagrams, IP addressing, VLAN plans, security policies, NAT configurations, and access-lists.

---

3. Specific Requirements:

Item	Details
Firewall	Cisco ASA / Firepower with NAT and VPN configured
Core Switches	Multilayer Switches (with HSRP redundancy)
WAN Connectivity	IPsec Site-to-Site VPN over Internet
DMZ	Web, Email, TFTP servers hosted securely
Data Center	Core services like Syslog, NTP, DHCP, DNS, AAA
Redundancy	Dual routers, dual switches, and failover links
Security	Segmentation, ACLs, DHCP Snooping, Option 82

---

4. Deliverables:

- Full logical and physical network design diagrams.
- IP Addressing scheme and VLAN assignment.
- Routing protocols and redundancy configurations.
- Firewall rules (Inbound and Outbound).
- NAT policies.
- Server placement and access-control between zones.
- Final testing plan for validation before deployment.

---

5. Notes:

- The design should consider **future scalability**.
- Use of **standard Cisco best practices** for security and performance.
- Ensure **minimal downtime** during failover scenarios.