Enterprise LAN Design Project

This project outlines the design and implementation of a secure, scalable, and reliable enterprise Local Area Network (LAN) using a hierarchical network design model. The network is developed to support multiple departments, ensure uninterrupted availability of services, and enforce strong security controls. The design emphasizes redundancy, performance optimization, and future scalability to accommodate organizational growth.

The organizational network is structured to serve several functional departments, each logically separated through VLAN segmentation. This approach minimizes broadcast traffic, enhances security, and simplifies network management. The proposed design allows seamless expansion of users and services without requiring major architectural changes.

The following components have been incorporated for robust IT infrastructure:

- **Internet Services Provider (ISP):** An external ISP connection is used to provide internet access and enable communication with external networks. For redundancy 2 ISP have been used
- **Hierarchical Architecture:** Instead of traditional design, 3-tier hierarchical design have been implemented which consist of core, distribution, and access layer.
- **Network Routing:** Routers and multilayer switches are deployed to efficiently route traffic between VLANs, internal networks, and external destinations.
- **Switching Infrastructure:** Core, distribution, and access switches are used to ensure structured traffic flow, scalability, and high-speed connectivity across the network.
- **Server Infrastructure:** Internal servers deliver essential services such as DHCP, DNS, and application hosting, providing centralized control and secure data access.
- **Wireless Infrastructure:** Wireless connectivity is integrated to support modern communication needs for users across all departments using centralized control with WLC
- **PAT:** Dynamic NAT(PAT) is used for network translation while connecting to external networks.

The network follows a **three-tier hierarchical architecture** consisting of the Core, Distribution, and Access layers:

- **Core Layer:** Acts as the network backbone, providing high-speed and resilient connectivity between distribution blocks. Redundancy is achieved through multiple core devices, dynamic routing, and link aggregation mechanisms.

- **Distribution Layer:** Serves as the policy enforcement point, handling inter-VLAN routing, applying access control policies, and providing gateway redundancy using first-hop redundancy protocols.
- **Access Layer:** Provides direct connectivity to end-user devices such as computers, IP phones, and wireless access points. VLAN assignments are enforced at this layer, and trunk links connect access switches to the distribution layer.

Dynamic routing throughout the network is implemented using the **Open Shortest Path First (OSPF)** routing protocol, enabling fast convergence and efficient route selection. High availability is ensured through redundancy mechanisms such as HSRP for default gateway resilience and EtherChannel for link redundancy and increased bandwidth.

The following technologies and configurations have been implemented to meet the network design requirements and ensure secure, reliable, and efficient operation:

- **Design Tool:** Cisco Packet Tracer is used to design, configure, and simulate the entire network infrastructure.
- **Hierarchical Network Design:** A three-tier hierarchical model (Core, Distribution, and Access layers) is implemented to enhance scalability, performance, and fault tolerance.
- **Internet Connectivity:** The network is connected to an external Internet Service Provider (ISP) to enable access to external networks and cloud-based services.
- **Wireless LAN Controller (WLC):** Wireless Access Points are centrally managed using a Wireless LAN Controller to provide secure and consistent Wi-Fi access for users and guests.
- **Virtual LANs (VLANs):** VLANs are configured to logically separate LAN, WLAN, and VoIP traffic, reducing broadcast traffic and improving network security.
- **EtherChannel (LACP):** Link Aggregation Control Protocol (LACP) is implemented to combine multiple physical links into a single logical link for increased bandwidth and redundancy.
- **Spanning Tree Enhancements:** Spanning Tree Protocol (STP) PortFast and BPDU Guard are enabled to improve convergence time and protect the network from accidental loops.
- **Subnetting:** IP subnetting is used to efficiently allocate address space to different departments and network segments.
- **Inter-VLAN Routing:** Multilayer switches are configured to enable communication between VLANs while maintaining logical separation.
- **Dynamic Routing:** Open Shortest Path First (OSPF) is used as the routing protocol to dynamically advertise routes across routers and multilayer switches.

- **High Availability:** First Hop Redundancy Protocols such as HSRP are implemented to provide gateway redundancy and failover capabilities.
- **DHCP Services:** End devices obtain IP addresses dynamically from centralized DHCP servers, while critical infrastructure devices use static addressing.
- **Network Security:** Access Control Lists (ACLs) and firewall policies are applied to restrict unauthorized access and control traffic flow.
- **Secure Management:** Secure Shell (SSH) is enabled for remote device management, with access limited to authorized administrative systems.
- **Access Control:** Devices from a particular department are denied having access to server of another department except IT and Administration Department.

IP Addressing:

Connection Between Core Switches and Distribution Switches	192.168.10.0/25
VLAN 20 (Server Room)	192.168.20.0/25
VLAN 30 (IT Department)	192.168.30.0/25
VLAN 40 (Administration Department)	192.168.40.0/25
VLAN 50 (Sales Department)	192.168.50.0/25
VLAN 60 (Marketing Department)	192.168.60.0/25
VLAN 70 (Public Relation Department)	192.168.70.0/25
VLAN 80 (Human Resource Department)	192.168.80.0/25
VLAN 90 (Finance Department)	192.168.90.0/25
VLAN 100 (Research and Development Department)	192.168.100.0/25
VLAN 300 (Remote Management of Access Switch)	172.16.30.0/26

Remote Management:

Core SW1	172.16.10.1 (Loopback Interface)
Core SW2	172.16.10.2 (Loopback Interface)
Distribution 1 SW1 (Floor 1)	172.16.20.1 (Loopback Interface)
Distribution 1 SW2 (Floor 1)	172.16.20.2 (Loopback Interface)
Distribution 2 SW1 (Floor 2)	172.16.20.3 (Loopback Interface)
Distribution 2 SW2 (Floor 2)	172.16.20.4 (Loopback Interface)
Distribution 3 SW1 (Floor 3)	172.16.20.5 (Loopback Interface)
Distribution 3 SW2 (Floor 3)	172.16.20.6 (Loopback Interface)
Access 1 SW 1 (Server Room)	172.16.30.11 (VLAN 300)
Access 1 SW 2 (IT Dept)	172.16.30.12 (VLAN 300)
Access 1 SW 3 (Administration Dept)	172.16.30.13 (VLAN 300)
Access 2 SW 1 (Sales Dept)	172.16.30.71 (VLAN 300)
Access 2 SW 2 (Marketing Dept)	172.16.30.72 (VLAN 300)

Access 2 SW 3 (PR Dept)	172.16.30.73 (VLAN 300)
Access 3 SW 1 (HR Dept)	172.16.30.141 (VLAN 300)
Access 3 SW 2 (Finance Dept)	172.16.30.142 (VLAN 300)
Access 3 SW 3 (R&D Dept)	172.16.30.143 (VLAN 300)

Servers:

WLC	192.168.20.10
DHCP & DNS	192.168.20.11
IT SERVER	192.168.20.12
Administration SERVER	192.168.20.13
Sales SERVER	192.168.20.14
Marketing SERVER	192.168.20.15
PR SERVER	192.168.20.16
HR SERVER	192.168.20.17
Finance SERVER	192.168.20.18
R&D SERVER	192.168.20.19

Through the Access Control List only the PC from their respective department have access to their respective Server except http connection. Also, IT and Administration Dept can access every server.

In conclusion, this LAN networking project demonstrates a well-structured enterprise network design that aligns with industry best practices. By combining hierarchical architecture, VLAN segmentation, dynamic routing, redundancy, and layered security, the network ensures the confidentiality, integrity, and availability of data while remaining scalable and robust for future growth.