Network Infrastructure Design & Implementation

This project involved the comprehensive design and implementation of a robust, scalable, and highly available network infrastructure. The design incorporates best practices for performance, redundancy, and security, utilizing a hierarchical model and a variety of Cisco networking technologies to support diverse departmental and operational needs, including cloud integration and telephony services.

Objectives:

- Create a resilient and high-performing network infrastructure.
- Implement redundancy for critical services to ensure high availability.
- Ensure scalability for future growth and expansion.
- Enhance network security through a multi-layered approach using a dedicated firewall and access controls.
- Integrate voice over IP (VoIP) and centralized wireless capabilities across the organization.
- Establish secure connectivity to a cloud platform for service delivery and data storage.

Requirements:

The network design emphasizes top-tier performance, redundancy, scalability, and availability. The following specific IP address ranges have been designated for different network segments:

- WLAN: `10.10.0.0/16`
- LAN: `192.168.0.0/20`
- Voice (VoIP): `172.16.0.0/20`
- DMZ: `10.20.10.0/26`

Network Components:

The setup uses high-quality hardware and trusted software to provide a stable and efficient network infrastructure.

Internet Connectivity: Provided by Airtel, ensuring external access for your services and users.
Network Security: A **Cisco ASA 5506-X Firewall** serves as the central security appliance, protecting your internal network from external threats and controlling access to your Demilitarized Zone (DMZ) and server farm.

Core Routing & Switching:

- Two Cisco Catalyst 3850 48-Port Switches form the core of your network, providing high-speed routing and switching capabilities.
- Ten Cisco Catalyst 2960-24TT 24-Port Switches are deployed as Layer 2 access switches in all departments, connecting user devices and wireless access points.
- **WAN Router:** A Cisco 2811 series WAN Router manages external connectivity and provides essential Voice over IP (VoIP) services

Server Hardware & Virtualization: Two HP ProLiant DL38 Gen10 servers utilize **VMware ESXi** for virtualization. These host critical virtual machines, including:

- Our **primary server (ESXi Primary Server) now hosts your DHCP (for automatic IP address assignment) and DNS (for domain name resolution) services**, ensuring central management and reliability.
- A secondary server for failover purposes, enhancing service continuity.

Internal Servers: Dedicated servers for your Health Information System, Email, and File storage.

Network Storage: Two NetApp storage devices provide robust and scalable centralized data storage.

Voice & Wireless Infrastructure:

- Cisco Voice Gateways handle your VoIP and telephony services.
- A Cisco Wireless LAN Controller (WLC) centrally manages the ten Lightweight Access Points (LAPs) deployed across your premises, providing seamless and secure wireless connectivity.

Cloud Integration: Dedicated connections to the AWS cloud platform ensure your healthcare system and other cloud-based services are accessible and well-integrated.

Features:

Hierarchical Design: Explicitly shows the three-layer hierarchical model (Access, Distribution, Core).

Virtual Local Area Networks (VLAN): Your network is segmented into isolated VLANs for different types of traffic (LAN, WAN, VoiP). This enhances security, improves performance by reducing broadcast traffic, and simplifies management.

High Availability with HSRP & EtherChannel:

- **Hot Standby Router Protocol (HSRP)** ensures that if one of your core routers fails, another immediately takes over, preventing network downtime.
- **EtherChannel** bundles multiple physical links into a single logical link between switches, increasing bandwidth and providing redundancy.

Robust Security: Beyond the firewall, Access Control Lists (ACLs) are deployed to restrict unauthorized access, and specific policies are in place to inspect network traffic. Remote access for network administration is secured using SSH.

Dynamic IP Addressing (DHCP): Devices automatically receive IP addresses from centralized servers, simplifying network administration and ensuring efficient IP address management.

Efficient Routing (OSPF): The Open Shortest Path First (OSPF) routing protocol ensures that network traffic always takes the most efficient path, adapting dynamically to changes in the network.

Unified Communications: Your IP phones and wireless devices seamlessly integrate into the network, supported by dedicated voice VLANs and a centralized Wireless LAN Controller.

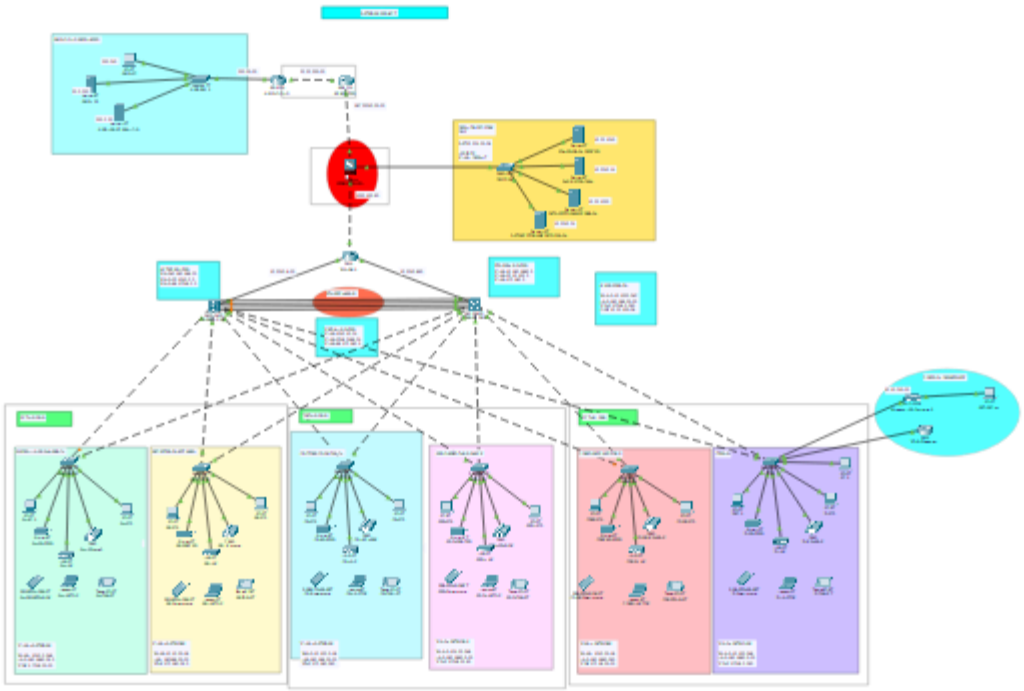
IP Addressing Strategy:

Network Segment	IP Address Range
WLAN	`10.10.0.0/16`
LAN	`192.168.0.0/20`
VoIP	`172.16.0.0/24`
.DMZ	`10.20.10.0/26`

Configuration Steps and Implementation

This section provides a summary of the core technologies implemented and the key configuration steps undertaken to build a robust, secure, and scalable network infrastructure.

- **Network Design and Refinement:** Initial conceptualization, detailed logical and physical design, and ongoing refinement.



- **Hierarchical Design:** Implemented a standard three-tier hierarchical model (Access, Distribution, Core) incorporating redundancy mechanisms for enhanced network resilience and scalability.
- **Internet Service Providers (ISPs):** Established primary internet connectivity through an Airtel ISP Router integrated into the network.
- **Wireless LAN Controller (WLC) & Access Points:** Deployed a Wireless LAN Controller for centralized management of Ten Lightweight Access Points (LAPs), ensuring comprehensive WiFi access across all departments for employees, corporate users, external auditors, and guests.
- **Voice over IP (VoIP):** Implemented IP phones in each department to support Voice over IP (VoIP) communication.

- **VLAN Segmentation:** Maintained distinct VLANs across the entire network for logical traffic separation: VLAN 10 for LAN (Wired), VLAN 50 for WLAN (Wireless), and VLAN 99 for VoIP (Voice).
- **EtherChannel:** Configured Link Aggregation Control Protocol (LACP) for EtherChannel on inter-switch links to enhance bandwidth aggregation and provide link redundancy.
- **STP PortFast and BPDUguard:** Configured Spanning Tree Protocol (STP) PortFast on all access ports to expedite port transitions to a forwarding state, and BPDUguard to prevent accidental loops by shutting down ports receiving BPDUs.
- **Subnetting & IP Addressing**: Utilized precise subnetting techniques to efficiently allocate IP addresses to each network group and departmental segment, aligning with the defined IP addressing scheme.
- **Basic Device Settings:** Configured fundamental device settings across all network devices, including hostnames, console and enable passwords, banner messages, password encryption, and disabling IP domain lookup for security and efficiency.
- **Inter-VLAN Routing:** Enabled devices across all departments to communicate by configuring the respective multilayer switches for inter-VLAN routing.
- **Core Switch Configuration:** Multilayer switches were assigned IP addresses and configured to perform both routing and switching functionalities at the core/distribution layer.
- **DHCP Server:** Ensured that all network devices (excluding IP phones) dynamically obtain IP addresses from Active Directory (AD) integrated DHCP servers located at the server farm site.
- **Cisco 2811 Router:** Deployed a Cisco Catalyst 2811 router specifically configured to support telephony services as the voice gateway.
- **HSRP (High Availability):** Implemented Hot Standby Router Protocol (HSRP) on the multilayer switches to provide gateway redundancy, load balancing, and seamless failover capabilities.
- **Static Addressing:** Allocated static IP addresses to critical devices located in the server room (e.g., servers, storage, management interfaces) for stable and predictable access.
- **Telephony Service:** Configured Voice over IP (VoIP) functionalities on the WAN router, assigning dial numbers in a consistent format .
- **Routing Protocol (OSPF):** Utilized Open Shortest Path First (OSPF) as the dynamic routing protocol, implementing it on the firewall, routers, and multilayer switches to advertise routes and ensure efficient network convergence.

- **Standard ACL for SSH:** Established a standard Access Control List (ACL) on the VTY lines of network devices to restrict remote administrative access via SSH exclusively to the designated Senior Network Security Engineer PC, enhancing management security.
- **Cisco ASA Firewall Configuration:** Configured default static routes, essential security settings, interface security levels and zones (Inside, Outside, DMZ), and detailed inspection policies on the Cisco ASA 5506-X Firewall to define access control and optimize resource utilization within the network.
- **Final Testing & Verification:** Conducted thorough testing procedures to verify proper communication and ensure that all configured elements function precisely as intended, adhering to design specifications.

🗺️ Network Topology File:
"D:\cisco packet traser\Network_Topology.pkt.pkt"