Implementing a Secure Multi-Branch Office Network

1. Executive Summary

This document details the design and implementation of a robust and secure network infrastructure for a company, a fast-growing telecommunication one. The network is designed to support the company's operations across its floors. The network infrastructure will provide reliable connectivity, secure communication, and internet access. The design prioritizes high performance, redundancy, scalability, and security, ensuring the confidentiality, integrity, and availability of data and communications. Key network components include Cisco routers, switches, firewalls, a wireless LAN controller, and Servers for directory services and DHCP. The network will implement network segmentation, robust security measures, and secure interoffice communication and protection against cyber threats.

2. Company Profile

- **Industry:** Telecommunications and IT Solutions

- **Departments:**
  - **4th Floor:** HR and Sales, Product Brand and Marketing, Admin and IT
  - **5th Floor:** IT Network & Support, Software Engineering, Cloud Engineering

- **Key Infrastructure:**
  - ISP
  - Cisco ASA 5525-X Firewall
  - Cisco Catalyst 3850 48-Port Switch
  - 3x Cisco Catalyst 2960 48-Port Switches
  - 2x Cisco Catalyst 2960 24-Port Switches
  - Cisco Voice Gateway (2811)
  - Cisco Wireless LAN Controller (WLC)
  - 6x Lightweight Access Points (LAPs)
  - Windows Server 2022 (Active Directory, RADIUS, DNS, DHCP)
  - Internally hosted ERP, Email, and File Servers
  - Google Cloud Platform

3. Business Requirements

The network design must address the following business requirements:

- Provide reliable and high-performance network connectivity for all departments.
- Ensure secure communication and access to internal resources.
- Enable access to Google cloud resources for developers and cloud engineers.
- Implement network segmentation to isolate LAN, WLAN, and VoIP traffic.
- Protect the network from external threats using a firewall.
- Support VoIP telephony services.
- Provide centralized management for wireless access points.
- Facilitate seamless business continuity.
- Adhere to the principles of Confidentiality, Integrity, and Availability (CIA).

4. Network Design

The network is designed using a hierarchical model to provide scalability, redundancy, and ease of management.

4.1. Network Topology

- A hierarchical topology is implemented, comprising the following layers:
    - **Core Layer:** The Cisco Catalyst 3850 Multilayer switch acts as the core layer, providing high-speed switching and routing between different network segments.
    - **Distribution Layer:** The Cisco Catalyst 2960 switches aggregate connections from access layer switches and provide redundancy.
    - **Access Layer:** Cisco Catalyst 2960 switches provide connectivity for end-user devices (PCs, laptops, IP phones, and wireless access points).
- **Internet Connectivity:** A connection to ISP is established through the Cisco ASA 5525-X Firewall.
- **DMZ:** A Demilitarized Zone (DMZ) is implemented to host the internal servers (ERP, Email, and File) and provide controlled access from the internal network and the internet.
- **Wireless Network:** A Cisco Wireless LAN Controller (WLC) manages Lightweight Access Points (LAPs) distributed across both floors to provide wireless connectivity for employees and guests.

4.2. IP Addressing Scheme

The following IP address ranges are used:

- WLAN: 10.20.0.0/16
- LAN: 192.168.10.0/24
- Voice: 172.16.10.0/24
- DMZ: 10.10.10.0/28
- Public Addresses: 197.200.100.0/30

4.3. VLAN Design

VLANs are used to segment the network traffic for improved security, performance, and manageability.

- VLAN 20: LAN (for wired devices in each department)
- VLAN 30: WLAN (for wireless devices used by employees and guests)
- VLAN 50: VoIP (for IP phones)

4.4. Subnetting

Subnetting is employed to efficiently allocate IP addresses to each department and network segment. The specific subnetting scheme is as follows:

- **LAN Subnetting (192.168.10.0/24):**
  - HR & Finance: [To be determined based on user count, e.g., 192.168.10.0/27]
  - Product Brand & Marketing: [To be determined based on user count, e.g., 192.168.10.32/27]
  - Admin & Corporate: [To be determined based on user count, e.g., 192.168.10.64/27]
  - IT Network & Support: [To be determined based on user count, e.g., 192.168.10.96/27]
  - Software Engineering: [To be determined based on user count, e.g., 192.168.10.128/27]
  - Cloud Engineering: [To be determined based on user count, e.g., 192.168.10.160/27]
- **WLAN Subnetting (10.20.0.0/16):**
  - Subnets will be created for each floor and/or department if needed for further segmentation.

- **Voice Subnetting (172.16.10.0/24):**
  - The entire 172.16.10.0/24 subnet can be used for VoIP devices, or it can be further subnetted if required.
- **DMZ Subnetting (10.10.10.0/28):**
  - The 10.10.10.0/28 subnet provides addresses for the servers in the DMZ.

4.5. Routing

- OSPF (Open Shortest Path First) is used as the routing protocol for dynamic routing within the internal network. This includes routing between VLANs and to the core router.
- Static routes and default routes are configured on the Cisco ASA Firewall to direct traffic to and from the internet and the internal network.
- Inter-VLAN routing is configured on the Layer 3 switch (Catalyst 3850) to enable communication between devices in different VLANs.

4.6. High Availability and Redundancy

- The hierarchical design provides redundancy.
- Link aggregation (EtherChannel/LACP) is implemented to increase bandwidth and provide link redundancy between switches.
- STP PortFast and BPDU Guard are configured to minimize downtime during topology changes and prevent spanning-tree loops.

4.7. Security Design

Security is a critical aspect of network design. The following measures are implemented:

- **Firewall:** A Cisco ASA 5525-X Firewall is deployed as the perimeter firewall to protect the network from external threats.
  - Security zones are defined (e.g., Inside, Outside, DMZ).
  - Security policies are configured to control traffic flow between zones.
  - Network Address Translation (NAT) is used to translate private IP addresses to public IP addresses.
  - Firewall inspection policies are implemented.

- **Access Control:**
  - Standard ACLs are configured on the Cisco devices to restrict access to sensitive network resources. Specifically, an ACL is used to limit SSH access to authorized administrators.
- **Device Hardening:**
  - Strong passwords are used for all network devices.
  - Unused ports and services are disabled.
  - IP domain lookup is disabled.
  - All passwords are encrypted.

5. Implementation

The network implementation involves the following steps:

- **Device Configuration:**
  - Configure basic settings on all network devices (hostnames, console passwords, enable passwords, banner messages).
  - Configure VLANs on the switches and assign ports to the appropriate VLANs.
  - Configure IP addressing on all interfaces.
  - Configure OSPF routing on the routers and Layer 3 switch.
  - Configure EtherChannel (LACP) where required.
  - Configure STP PortFast and BPDU Guard on access ports.
  - Configure the Cisco ASA Firewall with security zones, policies, and NAT.
  - Configure the Cisco WLC and Lightweight Access Points (LAPs) for wireless connectivity.
  - Configure the Cisco Voice Gateway for VoIP services.
  - Configure a Standard ACL for SSH access.

- **DHCP Configuration:**
  - Configure the Windows Server 2022 to provide DHCP services for LAN and WLAN clients.
  - Configure the Cisco Voice Gateway (or a separate router) to provide DHCP services for IP phones.

- **Server Configuration:**
  - Configure static IP addresses on the internal servers (ERP, Email, and File) within the DMZ.

- **Cabling:**
  - Connect network devices using the appropriate cables (Ethernet).

- **Testing and Verification:**
  - Test connectivity between all network devices and departments.
  - Verify VLAN configuration and inter-VLAN routing.
  - Test DHCP functionality.
  - Verify OSPF routing.
  - Test VoIP functionality.
  - Test WLAN connectivity and security.
  - Test firewall rules and security policies.
  - Test SSH access with the configured ACL.
  - Test access to internal servers from the LAN and the internet (if required).
  - Verify access to Google cloud resources.

6. IP Address Allocation

This table will map out each subnet, the devices in that subnet, and the specific IP addresses assigned:

Device/Location	Subnet	IP Address Range	Assigned IP Address(es)
ISP Router	197.200.100.0/24	197.200.100.1 - 197.200.100.254	197.200.100.1 (Example)
ASA Firewall (Outside)	197.200.100.0/30	197.200.100.1 - 197.200.100.254	197.200.100.2
ASA Firewall (Inside)	10.30.30.0/30	10.10.10.1 - 10.10.10.14	10.30.30.1
DMZ Server 1	10.10.10.0/28	10.10.10.1 - 10.10.10.14	10.10.10.5

DMZ Server 2	10.10.10.0/28	10.10.10.1 - 10.10.10.14	10.10.10.6
DMZ Server 3	10.10.10.0/28	10.10.10.1 - 10.10.10.14	10.10.10.7
DMZ Server 4	10.10.10.0/28	10.10.10.1 - 10.10.10.14	10.10.10.8
Core Switch (VLAN 20)	192.168.10.0/24	192.168.10.1 - 192.168.10.254	192.168.10.1
Core Switch (VLAN 30)	10.20.0.0/16	10.20.0.1 - 10.20.255.254	10.20.0.1
Core Switch (VLAN 50)	172.16.10.0/24	172.16.10.1 - 172.16.10.254	172.16.10.1
Windows Server 2022	192.168.10.0/24	192.168.10.1 - 192.168.10.254	192.168.10.2
Voice Gateway	172.16.10.0/24	172.16.10.1 - 172.16.10.254	172.16.10.1
Department 1 Switch	192.168.10.0/27	192.168.10.1 - 192.168.10.30	192.168.10.2
Department 1 PC 1	192.168.10.0/27	192.168.10.1 - 192.168.10.30	192.168.10.16
WLC	10.20.0.0/16	10.20.0.1 - 10.20.255.254	10.20.0.10
LAP 1	10.20.0.0/16	10.20.0.1 - 10.20.255.254	10.20.0.34

7. Device Configuration Standards

The following configuration standards are to be followed:

- **Hostnames:** Use a consistent naming convention for all devices (e.g., Core-SW-01, Dist-SW-01, Access-SW-01, FW-01, Rtr-01, WLC-01) We have used more memorable names.

- **Passwords:**
  - Strong, complex passwords must be used for all user and privilege levels.
  - Console, VTY, and enable passwords must be configured.
  - All passwords must be encrypted using service password-encryption
- **Banner Message:** A Message of the Day (MOTD) banner should be configured on all devices to provide a warning to unauthorized users.
- **IP Domain Lookup:** Disable IP domain lookup using the no ip domain-lookup command to prevent unnecessary DNS queries.
- **SSH:** SSH should be the only protocol allowed for remote management. Telnet should be disabled.

8. Technologies Implemented

The following technologies are implemented in this network:

- Hierarchical Network Design
- VLANs (802.1Q)
- Subnetting and IP Addressing (IPv4)
- OSPF Routing Protocol
- EtherChannel (LACP)
- Spanning Tree Protocol (STP) with PortFast and BPDU Guard
- DHCP Server
- SSH (Secure Shell)
- Access Control Lists (ACLs)
- VoIP (Voice over IP)
- WLAN (Wireless LAN)
- Cisco ASA Firewall
- Network Address Translation (NAT)

This documentation provides a comprehensive framework for the design and implementation of the network infrastructure. It can be used as a guide for network engineers during the implementation phase and as a reference for network administrators for ongoing maintenance and troubleshooting.

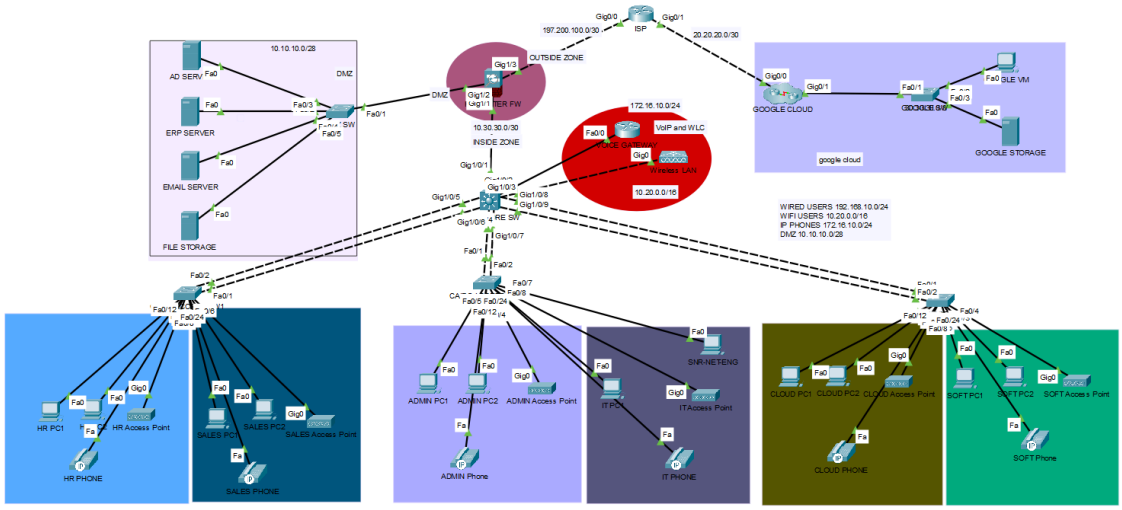

Figure (1) project final diagram