Telecom Company Network Design - Cisco Packet Tracer Project

Project Summary

This project simulates a real-world enterprise network using Cisco Packet Tracer. It is designed to be scalable, secure, and support modern services like VoIP, wireless access, and cloud integration. The architecture follows a hierarchical model and includes VLAN segmentation, OSPF routing, NAT, and access control.

---

1. Network Architecture

1.1 Hierarchical Design

The network follows the three-tier model for scalability, manageability, and fault isolation.

- **Core Layer**: Cisco Catalyst 3850
  - Handles inter-VLAN routing using SVIs.
  - Runs OSPF to dynamically share routes between network segments.
  - Chosen for high-performance and centralized traffic management.
- **Distribution Layer**: Cisco Catalyst 2960
  - Aggregates traffic from the access layer and uplinks to the core.
  - **EtherChannel (LACP)** is configured to bundle physical links, ensuring redundancy and increased bandwidth.
  - **Spanning Tree Protocol (STP)** is enabled to prevent Layer 2 loops and ensure a loop-free topology.
- **Access Layer**: Cisco Catalyst 2960
  - Directly connects to end-user devices such as PCs, printers, IP phones, and access points.
  - Separates traffic via VLANs and applies security features.

1.2 IP Addressing & VLANs

Logical segmentation improves security, management, and performance.

- **VLAN 50** - LAN (Wired Clients): 192.168.10.0/24
- **VLAN 60** - WLAN (Wireless): 10.20.0.0/16
- **VLAN 101** - VoIP: 172.16.10.0/24
- **DMZ Servers**: 10.10.10.0/28

Each VLAN isolates traffic and applies access policies. The DMZ is isolated for hosting public-facing services securely.

---

2. Security Configuration

2.1 Cisco ASA Firewall

The ASA provides perimeter security, protecting internal resources from external threats.

- **Security Zones**: Inside (trusted), Outside (untrusted/ISP), DMZ (semi-trusted)
- **NAT (PAT)** is configured to allow internal hosts to access the internet while masking private IPs.
- **Access Control Lists (ACLs)**:
  - Only allow **SSH** access from the **Senior Network Engineer's IP**, preventing unauthorized access.
  - Public access to DMZ is limited to **HTTP/HTTPS**, restricting unwanted services.

2.2 STP Hardening

To prevent Layer 2 attacks and accidental loops:

- **PortFast**: Speeds up port initialization for edge ports.
- **BPDU Guard**: Shuts down ports if rogue switches send BPDU frames.

---

3. VoIP and Wireless Integration

3.1 VoIP

Integrating VoIP reduces communication costs and adds flexibility to internal communication.

- **Cisco 2811 Voice Gateway**:
  - Provides telephony features and acts as the call manager.
  - Implements a dial plan with `1XXX` extensions.
- **VLAN 101**: Dedicated to voice traffic for better QoS and isolation.
- Switch ports use **voice VLAN tagging**, separating voice and data streams on the same cable.

3.2 Wireless

Wireless access is essential for mobility and BYOD (Bring Your Own Device) support.

- **Cisco WLC 2504** provides centralized wireless management.
- **6 Lightweight Access Points (LAPs)** offer scalable wireless coverage.
- SSIDs:
    - `Employee-WiFi` (WPA2): Secure internal access
    - `Guest-WiFi` (WPA2): Isolated network for visitors
- Wireless traffic is separated using VLAN 60 for proper segmentation.

---

4. Routing & Services

4.1 OSPF (Open Shortest Path First)

Dynamic routing is used instead of static to enhance network flexibility.

- OSPF is deployed on core switches, routers, and ASA to exchange routes dynamically.
- Ensures **redundancy and failover**—critical for enterprise availability.
- Routes verified using `show ip route ospf`.

4.2 Windows Server 2022 Roles

Windows Server provides essential infrastructure services:

- **Active Directory (AD)**: Centralized user/group authentication and policy enforcement.
- **DHCP Server**: Dynamically assigns IP addresses, simplifying client configuration.
- **DNS Server**: Enables name-to-IP resolution for internal services.
- **RADIUS**: Adds authentication for wireless users, enhancing security.

---

5. Testing and Validation

All services were thoroughly tested to ensure stability and functionality.

- **Ping tests**: Across VLANs and to DMZ hosts.
- **SSH restrictions**: Confirmed only the authorized engineer could connect.
- **VoIP**: Internal call routing between IP phones tested.
- **Wireless**: LAPs validated for roaming and SSID separation.
- **Routing**: OSPF tables confirmed for convergence and failover.

6. Tools Used

- **Cisco Packet Tracer** – Network design and simulation.
- **Cisco IOS** – Switches, Routers, ASA firewall.
- **Windows Server 2022** – AD, DHCP, DNS, RADIUS.
- **Technologies/Protocols**:
  - VLAN, OSPF, EtherChannel (LACP), NAT, DHCP, DNS, ACLs, VoIP, STP, RADIUS

Conclusion

This project provides a detailed look at building a functional enterprise network. Every component was selected for a specific purpose—whether to increase security, enhance scalability, improve redundancy, or support critical services like VoIP and wireless. It's a practical foundation for anyone learning networking, cybersecurity, or preparing for certifications like CCNA or CompTIA Network+.