Enterprise Network Design Documentation

Date : June 8, 2025

1. Project Overview

This project simulates a comprehensive network infrastructure for a medium-sized company using Cisco Packet Tracer. The design demonstrates the implementation of key networking principles and technologies to provide a secure, scalable, and resilient network environment. The goal was to create a functional enterprise network with multiple departments, redundant internet connectivity, and secure access controls.

2. Network Features and Technologies

This network design incorporates a wide range of features to meet modern business needs. The following technologies were implemented and configured:

- VLANs (Virtual LANs): Six distinct VLANs were created to segment the network, separating different departments (e.g., HR, Finance, IT) to improve security and network performance.
- Inter-VLAN Routing: A Layer 3 switch was configured to enable seamless communication between the different VLANs.
- OSPF (Open Shortest Path First): This dynamic routing protocol was used to ensure efficient routing within the internal network. It automatically handles path selection and provides network redundancy.
- Primary and Backup ISPs: The network is designed with dual connections to the internet. This provides redundancy and ensures continuous service even if one connection fails.
- DHCP (Dynamic Host Configuration Protocol): DHCP servers were configured to automatically assign IP addresses to devices, simplifying network administration.
- ACLs (Access Control Lists): ACLs were implemented on routers and switches to filter traffic and enforce security policies, such as restricting access between departments or to specific services.
- PAT (Port Address Translation): PAT was configured to allow multiple internal devices to share a single public IP address for internet access.
- DNS (Domain Name System): A DNS server was configured to resolve domain names to IP addresses, making it easier for users to access internal and external resources.
- SSH (Secure Shell): Devices were configured for secure remote management using SSH, protecting administrative access from eavesdropping.
- Wireless Access Points: Wireless connectivity was integrated into the network, providing flexible access for mobile devices.
- Port Security: This feature was enabled on switches to prevent unauthorized devices from connecting to the network by limiting the number of MAC addresses per port and using Sticky MAC to learn and remember connected devices.

3. Skills Demonstrated

This project showcases a solid understanding and practical application of the following networking skills:

- Cisco IOS CLI: Proficiency in configuring Cisco devices using the command-line interface.
- Subnetting: Effective use of subnetting to create a logical and efficient IP addressing scheme.
- Routing Protocols: Implementation and configuration of OSPF for dynamic routing.
- LAN Switching: Configuration of VLANs, Inter-VLAN routing, and security features like Port Security.
- Network Security: Application of ACLs, SSH, and other security measures to protect the network.
- Layer 2/3 Design: An understanding of both Layer 2 and Layer 3 concepts and their application in a hierarchical network design.

4. Conclusion

This project demonstrates a comprehensive understanding of designing, configuring, and securing an enterprise-level network. The combination of logical network segmentation with VLANs, robust routing with OSPF, and strict access control with ACLs results in a network that is both secure and scalable, ready to support a growing organization.