HRADYESH SAVALIYA

Enterprise Networking Project – Detailed Report

1. Introduction

This project represents a complete enterprise network design for a multi-floor office building. The objective of the project is to design, implement, and document a secure, scalable, and highly available network that supports multiple departments, users, servers, and wireless devices across four floors. The network is structured using industry-standard practices that are commonly followed in real-world enterprise environments.

The design focuses on proper VLAN segmentation, inter-VLAN routing, redundancy, efficient IP addressing, centralized services, and ease of management. Every component in this network has been selected and placed with a clear purpose, ensuring smooth communication, security, and future expansion.

This report explains the network from A to Z, covering what is used, why it is used, and how everything works together.

---

2. Project Objectives

The main objectives of this enterprise networking project are:

- To design a structured and hierarchical enterprise network
- To separate departments using VLANs for security and performance
- To implement inter-VLAN routing for controlled communication
- To ensure redundancy and high availability across floors
- To provide wired and wireless connectivity
- To centralize server services such as DHCP and Email
- To follow best practices used in enterprise data centers

---

3. Network Overview

The enterprise network spans four floors:

- **First Floor**: Management, Research, and Human Resources
- **Second Floor**: Marketing, Accounts, and Finance
- **Third Floor**: Logistics, Customer, and Guest departments

- **Fourth Floor**: Administration, ICT, and Server Room

Each floor is equipped with access switches, connected to Layer 3 switches and routers for routing and redundancy. Core routing is achieved using multiple routers interconnected with point-to-point links.

---

4. Network Architecture

The project follows a **three-tier hierarchical network model**:

1. **Access Layer** – End devices such as PCs, printers, and access points connect here.
2. **Distribution Layer** – Layer 3 switches perform inter-VLAN routing and policy enforcement.
3. **Core Layer** – Routers provide high-speed routing between floors and ensure redundancy.

This architecture improves scalability, troubleshooting, and performance.

---

5. VLAN Design and Purpose

VLANs are used to logically separate departments even though they may be physically connected to the same switch infrastructure.

VLAN List:

- VLAN 10 – Management
- VLAN 20 – Research
- VLAN 30 – Human Resources
- VLAN 40 – Marketing
- VLAN 50 – Accounts
- VLAN 60 – Finance
- VLAN 70 – Logistics
- VLAN 80 – Customer
- VLAN 90 – Guest
- VLAN 100 – Admin
- VLAN 110 – ICT
- VLAN 120 – Server Room

Why VLANs are Used:

- Improves security by isolating departments
- Reduces broadcast traffic
- Simplifies network management

- Allows flexible user movement

---

6. IP Addressing Scheme

The network uses private IP addressing with proper subnetting. Each VLAN is assigned a **/26 subnet**, providing up to 62 usable IP addresses per department.

Examples:

- VLAN 10: 192.168.10.0/26
- VLAN 20: 192.168.10.64/26
- VLAN 30: 192.168.10.128/26
- VLAN 40: 192.168.10.192/26

This structured addressing makes troubleshooting and expansion easier.

Point-to-point links between routers use **/30 subnets**, which is an efficient and standard practice.

---

7. Switching Infrastructure

Access Switches

Each department has its own access switch:

- Connects PCs, printers, and wireless APs
- Configured with access ports assigned to VLANs
- Provides local connectivity

Layer 3 Switches

- Perform inter-VLAN routing using SVIs
- Act as the default gateway for VLANs
- Reduce load on routers

Using Layer 3 switches improves performance and reduces latency.

---

8. Routing Design

Multiple routers are deployed across floors to provide redundancy and load distribution.

Routing Features:

- Point-to-point serial and gigabit links
- Redundant routing paths

- Logical separation of traffic between floors

Routing between floors ensures that all VLANs can communicate as required while maintaining control and security.

---

9. Inter-VLAN Routing

Inter-VLAN routing is achieved using **SVIs on Layer 3 switches**.

How It Works:

- Each VLAN has a corresponding SVI
- End devices use the SVI IP as the default gateway
- Traffic between VLANs is routed internally on the switch

This method is faster and more scalable than router-on-a-stick.

---

10. Redundancy and High Availability

Redundancy is built into the design to avoid single points of failure.

Redundancy Methods Used:

- Multiple uplinks between switches
- Multiple routers per floor
- Mesh-style interconnections

If one link or device fails, traffic automatically takes an alternate path.

---

11. Wireless Network Design

Wireless Access Points (APs) are deployed in each department.

Purpose of Wireless:

- Mobility for users
- Support for laptops and mobile devices
- Reduced cabling requirements

Each AP is mapped to the appropriate VLAN to maintain security.

---

12. Server Room Design

The server room is located on the fourth floor and isolated in VLAN 120.

Servers Deployed:

- DHCP Server
- Email Server
- HTTPS Server

Why a Separate VLAN:

- Increased security
- Controlled access
- Better performance

---

13. DHCP Services

The DHCP server automatically assigns IP addresses to all end devices.

Benefits:

- Eliminates manual IP configuration
- Prevents IP conflicts
- Centralized management

DHCP relay is configured on Layer 3 devices where required.

---

14. Security Design

Security is implemented at multiple levels.

Security Measures:

- VLAN isolation
- Controlled inter-VLAN routing
- Dedicated guest VLAN
- Server VLAN separation

The guest VLAN is isolated from internal resources to protect corporate data.

---

15. Guest Network Design

VLAN 90 is dedicated to guest users.

Guest Network Characteristics:

- Internet-only access
- No access to internal servers

- Separate IP subnet

This protects internal users while still providing visitor connectivity.

---

16. Cabling and Interfaces

- FastEthernet used for end devices
- Gigabit Ethernet used for uplinks
- Serial interfaces used for router interconnections

High-speed links are used where traffic volume is high.

---

17. Network Management

Management Features:

- Dedicated Management VLAN
- Centralized monitoring
- Clear documentation

This allows network administrators to manage devices securely.

---

18. Scalability

The network is designed to grow.

Scalability Features:

- Unused VLAN IDs
- Extra IP address capacity
- Modular switch and router placement

New departments can be added with minimal changes.

---

19. Troubleshooting and Maintenance

Structured design makes troubleshooting easier.

Advantages:

- Clear VLAN boundaries
- Logical IP addressing
- Layered architecture

Problems can be isolated quickly to a specific layer or floor.

---

20. Real-World Relevance

This project closely matches real enterprise networks used in offices, hospitals, universities, and corporate buildings. The technologies and design principles used here are industry standard.

---

21. Conclusion

This enterprise networking project demonstrates a complete and professional network design covering all essential aspects of modern enterprise networking. From VLAN planning to routing, redundancy, security, and server integration, every component serves a clear purpose.

The network is secure, scalable, easy to manage, and reliable. This design can be confidently presented as a real-world enterprise network implementation and serves as a strong foundation for advanced networking concepts and professional roles.

---

22. Detailed Floor-Wise Network Explanation

First Floor Network Design

The first floor hosts three critical departments: Management (VLAN 10), Research (VLAN 20), and Human Resources (VLAN 30). These departments handle sensitive and operational data, which makes proper segmentation and controlled access extremely important.

Each department is connected to its own access switch. End devices such as desktop computers, printers, and wireless access points are connected using FastEthernet interfaces. Access ports are statically assigned to their respective VLANs to prevent accidental or unauthorized VLAN hopping.

Uplinks from the access switches connect to a Layer 3 switch using GigabitEthernet links. These uplinks are configured as trunk ports, allowing multiple VLANs to pass between switches efficiently. The Layer 3 switch on this floor provides default gateway functionality using SVIs for VLAN 10, 20, and 30.

This design ensures that broadcast traffic is limited within each department while still allowing controlled communication through routing policies.

Second Floor Network Design

The second floor includes Marketing (VLAN 40), Accounts (VLAN 50), and Finance (VLAN 60). These departments generate significant transactional and reporting traffic, so network reliability and performance are priorities.

Each department again has a dedicated access switch to maintain logical separation. Finance and Accounts VLANs are particularly protected to ensure data confidentiality. Printers are placed within the same VLANs to simplify access control and reduce cross-VLAN dependencies.

The Layer 3 switch on the second floor aggregates traffic from all access switches and forwards it toward the core routing layer. Redundant uplinks are used to improve availability and ensure that a single cable or port failure does not disrupt operations.

Third Floor Network Design

The third floor is designed for external-facing and semi-public users, including Logistics (VLAN 70), Customer (VLAN 80), and Guest (VLAN 90).

The guest network is intentionally isolated from internal VLANs. Access control policies ensure that guest users can only access external networks and not internal enterprise resources. This is a common enterprise practice to protect internal systems while still providing convenience to visitors.

Wireless access points play a major role on this floor. They are connected to access switches and mapped to their appropriate VLANs. This ensures consistent security policies across both wired and wireless users.

Fourth Floor Network Design

The fourth floor contains Administration (VLAN 100), ICT (VLAN 110), and the Server Room (VLAN 120). This floor is considered the operational backbone of the enterprise.

The ICT department manages the network infrastructure, so its VLAN is positioned close to core devices. Administrative users are provided stable and secure connectivity for policy and decision-making tasks.

The server room is isolated in its own VLAN to enhance security and performance. Only authorized VLANs are allowed to communicate with the server network.

---

23. Core Routing and Inter-Floor Connectivity

Routers are deployed to interconnect all floors using point-to-point links. These links are configured using /30 subnets, which is a best practice for router-to-router communication.

Multiple routing paths exist between floors. This design ensures high availability and fault tolerance. If one router or link fails, traffic can still reach its destination through alternate paths.

Dynamic routing concepts can be applied to this topology in real-world scenarios to further enhance resilience and adaptability.

---

24. Link Redundancy and Failover Strategy

Redundancy is achieved through:

- Multiple uplinks between access and distribution layers
- Multiple inter-router connections
- Use of high-speed GigabitEthernet links

This approach ensures continuous network availability. Failover occurs transparently to end users, maintaining productivity and minimizing downtime.

---

25. Broadcast Control and Performance Optimization

By dividing the network into multiple VLANs, broadcast domains are kept small. This significantly reduces unnecessary broadcast traffic and improves overall performance.

Layer 3 switching ensures that routing decisions are made quickly without sending traffic to external routers unnecessarily. This results in lower latency and higher throughput.

---

26. Access Control and Policy Enforcement

Access control is achieved through:

- VLAN-based segmentation
- Controlled inter-VLAN routing
- Server VLAN isolation
- Guest VLAN restrictions

Policies can be applied at the Layer 3 switches or routers to further restrict or allow traffic based on organizational requirements.

27. Printer and Peripheral Integration

Printers are deployed within the same VLAN as their respective departments. This simplifies network design and avoids the need for complex access rules.

Peripheral devices such as printers are placed on static IP addresses or reserved DHCP leases to ensure consistent accessibility.

---

28. Wireless Network Policy Design

Wireless networks follow the same security and segmentation principles as wired networks. Each wireless SSID maps to a specific VLAN.

This design ensures that:

- Wireless users follow the same security rules
- Guest wireless users remain isolated
- Network policies remain consistent

---

29. Server Access and Traffic Flow

Servers provide centralized services for the entire enterprise. Traffic to the server VLAN is carefully controlled.

Only authorized VLANs are permitted to access specific services such as email or HTTPS. This reduces the attack surface and protects critical infrastructure.

---

30. Address Management and Documentation

Consistent IP addressing and documentation are essential in enterprise networks. This project follows structured subnet allocation, making it easy to identify:

- Department
- Floor location
- Network function

Proper documentation reduces operational errors and simplifies onboarding of new network engineers.

---

31. Change Management Considerations

The modular design of this network supports safe and controlled changes. New VLANs, switches, or departments can be added without impacting existing services.

Changes can be tested floor by floor, reducing risk during upgrades or expansions.

---

32. Compliance and Best Practices

This network design aligns with widely accepted enterprise best practices, including:

- Hierarchical network model
- VLAN-based segmentation
- Redundant routing paths
- Secure server isolation

Such practices are commonly required for regulatory compliance and audits.

---

33. Operational Benefits

The completed network provides:

- High reliability
- Strong security
- Efficient management
- Scalability for future growth

Departments can operate independently while still benefiting from shared enterprise services.

---

34. Learning Outcomes

Through this project, key networking concepts are demonstrated, including:

- VLAN planning and implementation
- Inter-VLAN routing
- Enterprise IP addressing
- Redundancy and high availability
- Wireless integration
- Server network design

These skills directly map to real-world enterprise networking roles.

---

35. Final Conclusion

This expanded enterprise networking project represents a complete, realistic, and professional network implementation suitable for modern organizations. Every design decision is based on proven industry standards and practical requirements.

The network is secure, efficient, fault-tolerant, and ready for real-world deployment. It demonstrates not only technical knowledge but also structured thinking, planning, and documentation skills expected from a professional network engineer.

End of Report