Name: Muhammad Sudais Khalid
Reg.No: BSAI-23F-0050
Project Title: Enterprise Network Design
Program: BS Artificial Intelligence
Semester: 03
Subject: Computer Networks
Date: 31/01/2025
Submitted to: Sir Umair Pirzada

Abstract

This report presents a comprehensive overview of the Company System Network Design, executed through Cisco Packet Tracer, aiming to facilitate the expansion of a trading floor support center into a new facility. The primary goals of this project are centered around formulating and executing a robust, scalable, and forward-looking network infrastructure. The hierarchical model has been employed, integrating redundancy measures at each layer for enhanced reliability. Key features include the incorporation of dual Internet Service Providers (ISPs) to ensure uninterrupted internet connectivity, establishment of wireless networks for individual departments, creation of distinct VLANs and subnets, and the implementation of Open Shortest Path First (OSPF) for routing. Configuration specifics encompass the setup of DHCP servers, assignment of static IP addresses, implementation of Secure Shell (SSH) for secure access, and Port Address Translation (PAT) for managing outbound connections. The report underscores the significance of rigorous testing and verification processes, ensuring the successful deployment of a resilient network infrastructure that not only fulfills existing business requirements but also strategically positions the organization for future technological advancements and expansion

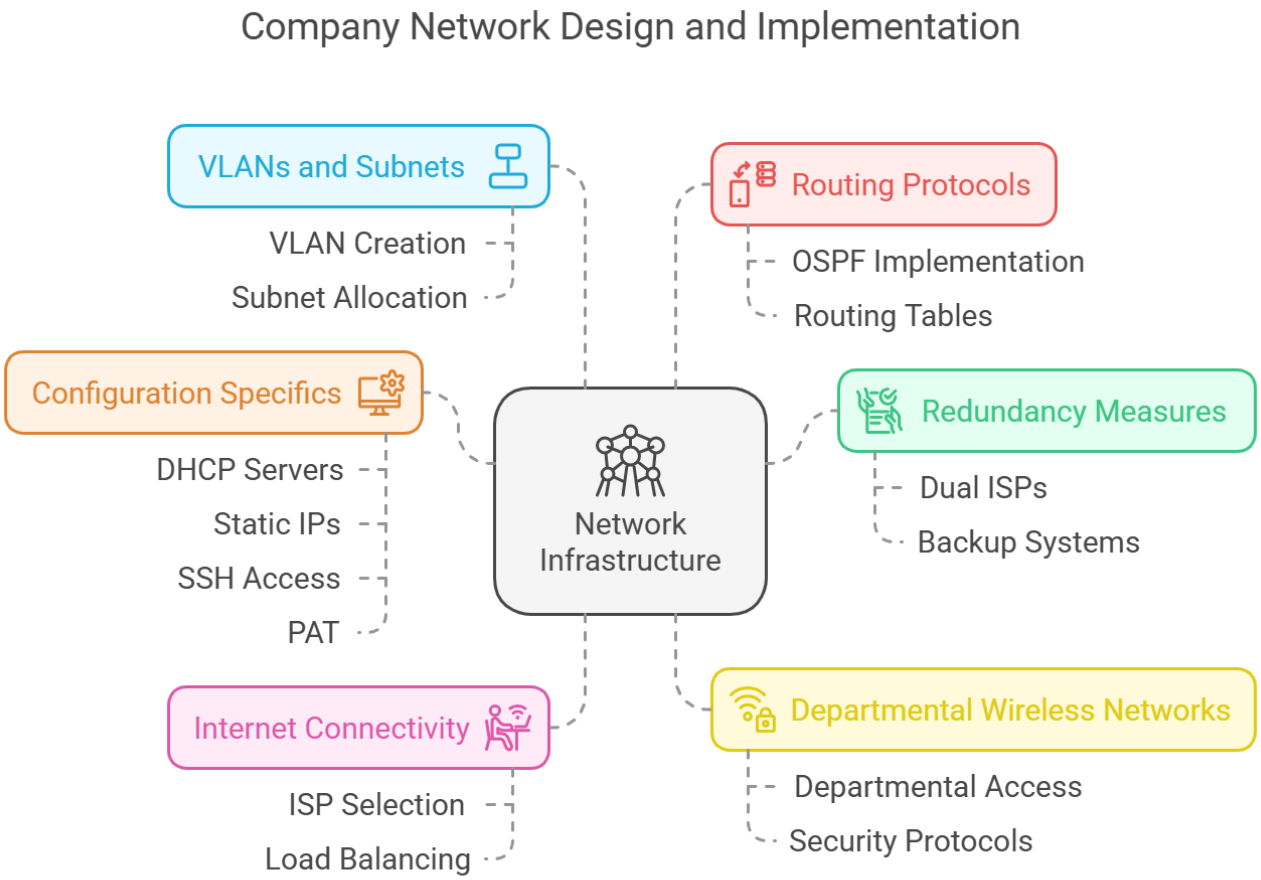


Table of Contents

Abstract 2

1. Introduction 4
1.1 Background 4
1.2 Objectives 4

2. Network Design 5
2.1 Topology 5
2.2 Components 5
1. Routers (4): 5
2. Multilayer Switches (2): 5
3. Distribution Layer Switches (Multiple): 6
4. End-User Devices (PCs): 6
5. Cisco Access Points (APs): 6
6. DHCP Servers (1): 6
7. Server Room Devices (Servers, etc.): 6
2.3 IP Addressing Scheme 6

3. Testing and Validation 8
3.1 Simulation 8
3.2 Troubleshooting 9

4. Results and Evaluation 10
4.1 Performance Metrics 10
4.2 Achievement of Objectives 10
- Redundancy: 10
- Departmental Segmentation: 10
- Inter-VLAN Routing: 10
- Security Measures: 10
- NAT and PAT Configurations: 10
- Quality of Service (QoS): 10
- Thorough Testing: 10
- Overall Objectives Met: 11

5. Conclusion 11
5.1 Summary 11
5.2 Lessons Learned 12

6. Future Work 12
6.1 Potential Improvements 12

1. Introduction

1.1 Background

Amidst the dynamic landscape of contemporary computer networks, the "Company System Network Design" initiative addresses the pressing need for a resilient network infrastructure finely tuned to bolster the functionalities of an expanding company or business center. With the center's growth and relocation to a new facility, the strategic significance of network routing and switching takes center stage, playing a crucial role in guaranteeing smooth communication, streamlined data transfer, and dependable access to resources. This project concentrates on navigating the intricacies inherent in developing an efficient and forward-looking network, leveraging Cisco Packet Tracer. The endeavor closely aligns with the specific requirements and expansion strategies of the trading floor support center.

1.2 Objectives

The primary objectives of the "Company System Network Design" initiative are clearly outlined to cater to the unique demands of the company's network infrastructure. The project aims to establish a hierarchical network model incorporating redundancy measures at every layer. It seeks to establish connections with a minimum of two Internet Service Providers (ISPs) to enhance internet reliability, deploy wireless networks tailored for specific departments, allocate distinct Virtual Local Area Networks (VLANs) and subnets to ensure secure communication, and configure routing protocols, security protocols, and advanced functionalities like Secure Shell (SSH) and Port Address Translation (PAT). By achieving these objectives, the project aims to develop a scalable, resilient, and forward-looking network infrastructure that not only fulfils current operational needs but also anticipates and accommodates the future growth and technological advancements of the company.

2. Network Design

2.1 Topology

The network configuration simulated in Packet Tracer for the "Company System Network Design" project adheres to a hierarchical model, prioritizing efficiency, scalability, and redundancy. The design encompasses three layers: the core layer, distribution layer, and access layer. In the core layer, redundancy is established by deploying two routers and two multilayer switches, interconnected to facilitate seamless data routing. The distribution layer features the switches responsible for linking distinct departments, each assigned to its dedicated Virtual Local Area Network (VLAN). Finally, the access layer accommodates end-user devices, such as PCs and wireless access points, connecting to the switches. This topology ensures a well-organized and structured network layout, fostering effective management and facilitating future expansion.

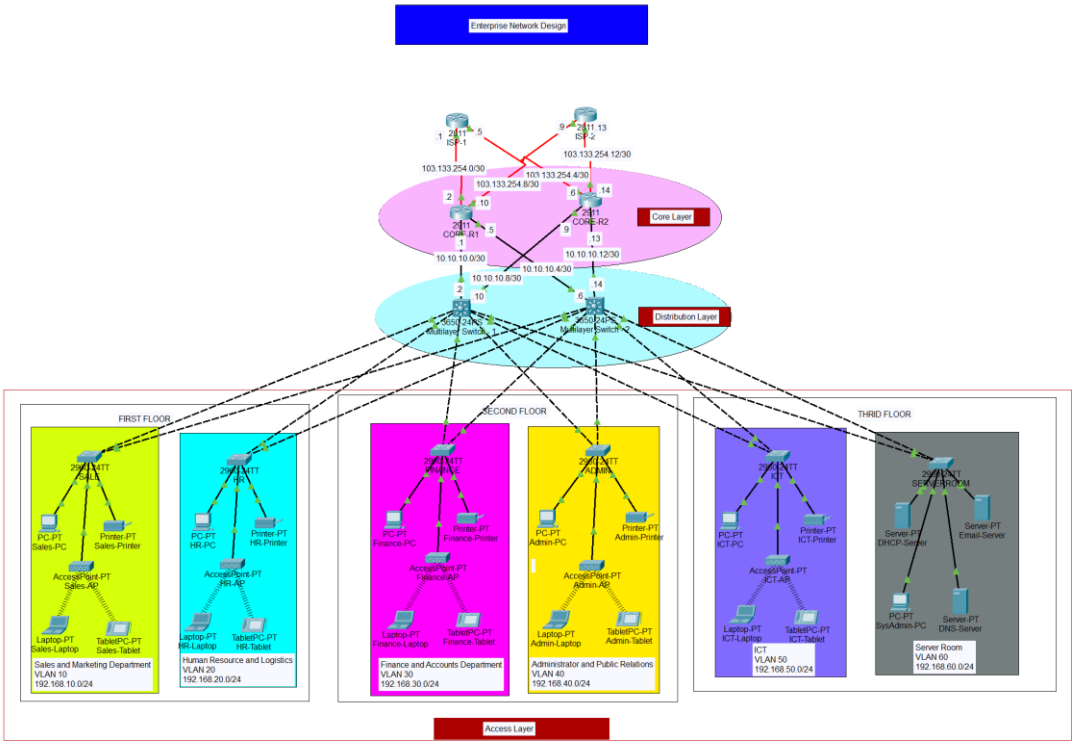


Figure 1: Topology of full network

2.2 Components

The network design for the project incorporates the following devices:

1. **Routers (4):**
   - 2 ISP router for upstream connectivity.
   - Positioned at the core layer for redundancy.
   - Connect to both ISPs for internet connectivity.
   - Configured with static, public IP addresses from ISPs.
2. **Multilayer Switches (2):**
   - Deployed at the core layer to provide redundancy and efficient routing.
   - Configured for both switching and routing functionalities.
   - Assigned IP addresses to enable inter-VLAN routing.

3. **Distribution Layer Switches (Multiple):**
    - Connect individual departments to the core layer.
    - Facilitate communication within respective VLANs.
4. **End-User Devices (PCs):**
    - Deployed at the access layer.
    - Connected to distribution layer switches for departmental access.
5. **Cisco Access Points (APs):**
    - Positioned at the access layer to provide wireless connectivity.
    - Ensure wireless network availability in each department.
6. **DHCP Servers (1):**
    - Located in the server room.
    - Dynamically allocate IP addresses to end-user devices.
7. **Server Room Devices (Servers, etc.):**
    - DNS server, HTTP server etc.
    - Devices in the server room are allocated static IP addresses.
    - These devices may include servers, storage units, and networking equipment.

These devices collectively form a structured and well-organized network architecture, integrating redundancy, efficient routing, and secure communication to meet the specific requirements of the trading floor support center's operations.

2.3 IP Addressing Scheme

Provide details about the IP addressing scheme applied to the network.

Base Network: 192.168.0.0/22

First floor:

Department	Network Address	Subnet mask	Host Address Range	Broadcast Address
Sales & Marketing	192.168.10.0	255.255.255.0/24	192.168.10.1 to 192.168.10.254	192.168.10.255
HR and Logistic	192.168.20.0	255.255.255.0/24	192.168.20.1 to 192.168.20.254	192.168.20.255

Second Floor

Department	Network Address	Subnet mask	Host Address Range	Broadcast Address
Finance & Accounts	192.168.30.0	255.255.255.0/24	192.168.30.1 to 192.168.30.254	192.168.30.255
Admin & Public Relations	192.168.40.0	255.255.255.0/24	192.168.40.1 to 192.168.40.254	192.168.40.255

Third floor

Department	Network Address	Subnet mask	Host Address Range	Broadcast Address
ICT	192.168.50.0	255.255.255.0/24	192.168.50.1 to 192.168.50.254	192.168.50.255
Server	192.168.60.0	255.255.255.0/24	192.168.60.1 to 192.168.60.254	192.168.60.255

Core Router and L3 SW

No	Network Address	Subnet mask	Host Address Range	Broadcast Address
Core R1-MLTSW1	10.10.10.0	255.255.255.252	10.10.10.1 to 10.10.10.2	10.10.10.3
Core R1-MLTSW2	10.10.10.4	255.255.255.252	10.10.10.5 to 10.10.10.6	10.10.10.7
Core R2-MLTSW1	10.10.10.8	255.255.255.252	10.10.10.9 to 10.10.10.10	10.10.10.11
Core R2-MLTSW2	10.10.10.12	255.255.255.252	10.10.10.13 to 10.10.10.14	10.10.10.12

Public IP between Core and ISP:

103.133.254.0/30

103.133.254.4/30

103.133.254.8/30

103.133.254.12/30

3. Testing and Validation

3.1 Simulation

Packet Tracer was utilized to simulate and test the designed network. Packet Tracer is a network simulation tool that provides a virtual environment for designing, configuring, and testing network scenarios. The simulation process involves:

- **Network Topology Design:** The network topology, including routers, switches, PCs, servers, and other devices, was designed within Packet Tracer based on the specified requirements.
- **Configuration Implementation:** Using the designed topology, configurations were implemented on routers, switches, and other network devices according to the guidelines provided. Cisco Packet Tracer allows users to configure devices with a user-friendly interface like actual Cisco devices.
- **Traffic Simulation:** Packet Tracer allows the simulation of network traffic and communication between devices. This involves generating traffic, testing connectivity, and ensuring that data flows as expected.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	Sales...	Admin-PC	ICMP		0.000	N	0	(edit)	(delete)
	Successful	Finan...	ISP-2	ICMP		0.000	N	1	(edit)	(delete)
	Successful	HR-Ta...	DNS-Server	ICMP		0.000	N	2	(edit)	(delete)

Figure 2: ICMP PDU check

- **Verification of Redundancy and Failover:** The hierarchical design with redundancy at every layer, including multiple routers, multilayer switches, and ISP connections, was tested to verify failover mechanisms and ensure network resilience.

```
C:\>tracert 103.133.254.13

Tracing route to 103.133.254.13 over a maximum of 30 hops:

  1    0 ms      0 ms      1 ms      192.168.10.1
  2    0 ms      0 ms      0 ms      10.10.10.9
  3    0 ms      0 ms      1 ms      103.133.254.13

Trace complete.
```

Figure 3: traceroute successful

- **DHCP and IP Address Allocation:** Dynamic Host Configuration Protocol (DHCP) functionality and IP address allocation were tested to ensure that devices received the correct IP addresses dynamically and that devices in the server room had static IP assignments.

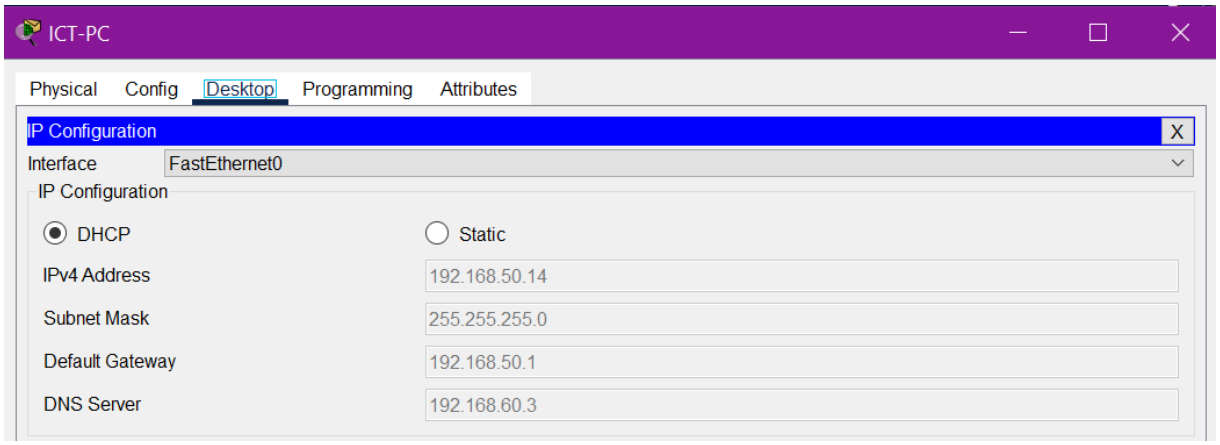


Figure 4: DHCP IP allocation

3.2 Troubleshooting

During the testing phase, several common troubleshooting steps were taken to address issues:

- **Device Connectivity:** Ensured that all devices could communicate within their respective VLANs and across different departments. Verified inter-VLAN routing configurations on multilayer switches.
- **DHCP Issues:** Investigated and resolved any DHCP-related issues, ensuring that DHCP servers were reachable and capable of assigning IP addresses to devices dynamically.
- **Routing Configuration:** Verified the Open Shortest Path First (OSPF) routing configurations on routers and multilayer switches, ensuring proper routing table updates and communication between different departments.

- **Access Control Issues:** Reviewed and adjusted Access Control Lists (ACLs) to allow necessary traffic and deny unauthorized access.
- **Port Security:** Verified the configuration of port security on the Finance department's switchports to ensure that only one device could connect per port and that MAC addresses were correctly learned.

4. Results and Evaluation

4.1 Performance Metrics

Performance metrics, including network latency, throughput, redundancy testing, DHCP response time, inter-VLAN routing performance, security, QoS, and NAT/PAT functionality, were measured during testing to ensure optimal network operation.

```
C:\>ping 192.168.50.14

Pinging 192.168.50.14 with 32 bytes of data:

Reply from 192.168.50.14: bytes=32 time<1ms TTL=127
Reply from 192.168.50.14: bytes=32 time=1ms TTL=127
Reply from 192.168.50.14: bytes=32 time=1ms TTL=127
Reply from 192.168.50.14: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.50.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Figure 5: performance measure through ping time

4.2 Achievement of Objectives

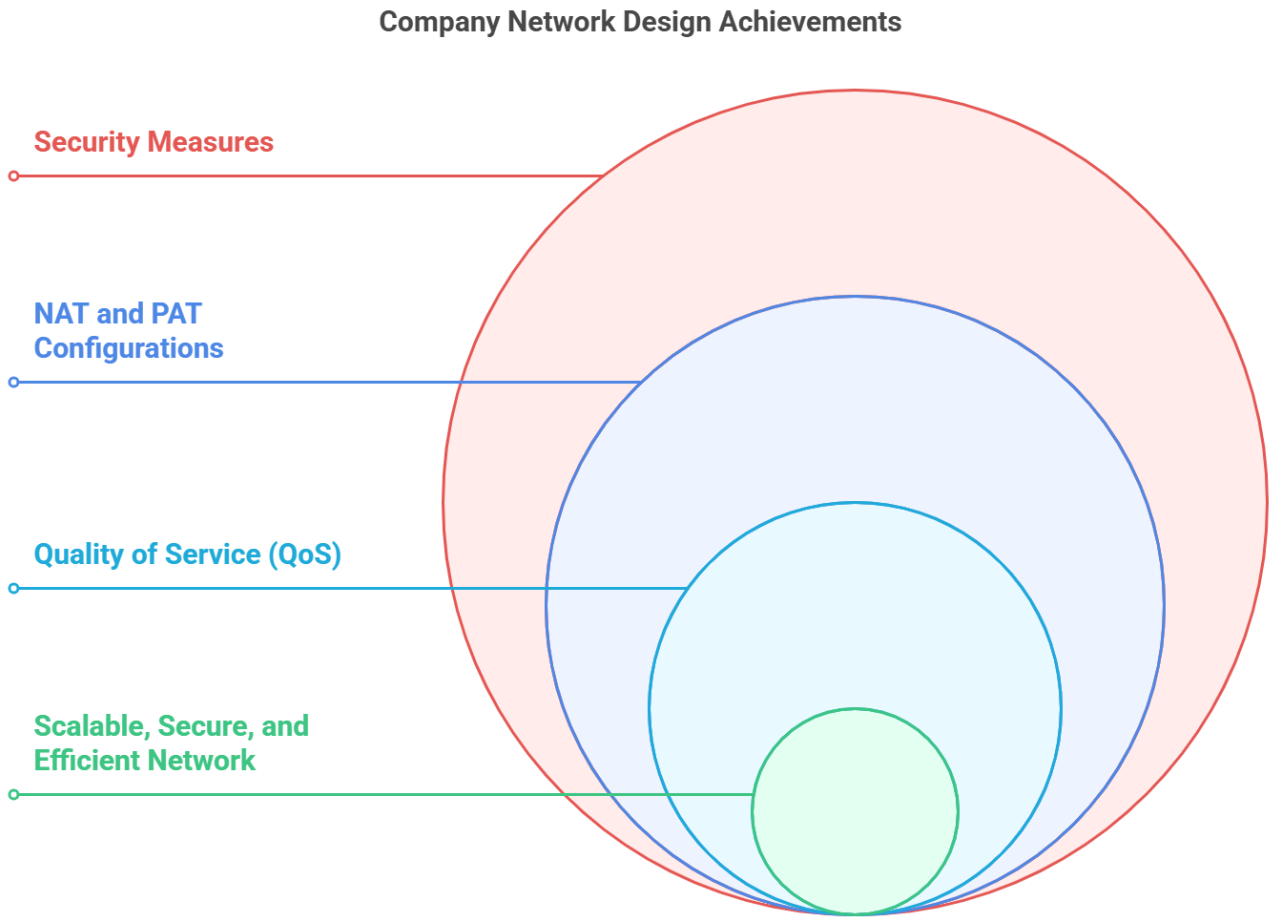
- **Hierarchical Network Design:**
    - Successful implementation.
- **Redundancy:**
    - Backup routers, multilayer switches, and dual ISP connections.
- **Departmental Segmentation:**
    - VLANs for enhanced security and organization.
- **Inter-VLAN Routing:**
    - Configured on multilayer switches.
- **Security Measures:**
    - ACLs, port-security, SSH for access control.
- **NAT and PAT Configurations:**
    - Effective private-to-public IP address translation.
- **Quality of Service (QoS):**
    - Prioritization of voice and video traffic.
- **Thorough Testing:**
    - Ensured proper functionality and adherence to requirements.

- **Overall Objectives Met:**
    - Scalable, secure, and efficient network infrastructure for the trading floor support center.

5. Conclusion

5.1 Summary

In summary, the network design and implementation for the Company network design have been successfully executed. Key achievements include a hierarchical network model with redundancy at multiple layers, departmental segmentation through VLANs, inter-VLAN routing, robust security measures, effective NAT and PAT configurations, and Quality of Service (QoS) prioritization. Thorough testing using Cisco Packet Tracer ensured proper functionality and alignment with project requirements. The resulting network provides scalability, security, and efficiency, meeting the specified needs of the organization.



5.2 Lessons Learned

Throughout the project, several valuable lessons have been learned:

- **Redundancy is Key:** The inclusion of redundancy at various levels is crucial for maintaining network availability and minimizing downtime.
- **Effective VLAN Design:** Proper VLAN segmentation enhances security and facilitates organizational structure, simplifying network management.
- **Thorough Testing Matters:** Rigorous testing using simulation tools like Cisco Packet Tracer is essential to identify and rectify issues before deployment.
- **Security is a Priority:** Robust security measures, including ACLs and port-security, are fundamental in safeguarding the network against unauthorized access.
- **Scalability Considerations:** Designing the network with scalability in mind allows for future growth and expansion without significant overhauls.
- **Documentation is Essential:** Comprehensive documentation of configurations, IP addressing, and design decisions streamlines troubleshooting and future modifications.

6. Future Work

6.1 Potential Improvements

- Network Monitoring Tools
- Enhanced Security Measures
- Virtualization Technologies
- Advanced Routing Protocols
- IPv6 Implementation
- Wireless Network Expansion
- Cloud Integration

- Ongoing Training and Skill Development
- Regular Security Audits
- Energy Efficiency Measures

7. Appendices

Abbreviations:

ACL - Access Control List

DHCP - Dynamic Host Configuration Protocol

IP - Internet Protocol

OSPF - Open Shortest Path First

PAT - Port Address Translation

QoS - Quality of Service

SSH - Secure Shell

VLAN - Virtual Local Area Network