Design and Implementation of a Secure and Redundant Enterprise Network

by

Din Islam
ID: CSE2301028110

Md. Ramzan
ID: CSE2301028019

Kamrul Hasan Sakib
ID: CSE2301028170

Rafayat Kabir Tonoy
ID: CSE2301028043

Aminul Islam Opu
ID: CSE2302029040

Supervised by
Md. Shamim Hossain

Submitted in partial fulfillment of the requirements for the degree of
Bachelor of Science in Computer Science and Engineering



DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SONARGAON UNIVERSITY (SU)

September 2026

APPROVAL

The project titled **"Design and Implementation of a Secure and Redundant Enterprise Network''** submitted by Din Islam (CSE2301028110), Md. Ramzan (CSE2301028019), Kamrul Hasan Sakib (CSE2301028170), Rafayat Kabir Tonoy (CSE2301028043), and Aminul Islam Opu (CSE2302029040) to the Department of Computer Science and Engineering, Sonargaon University (SU), has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of Bachelor of Science in Computer Science and Engineering and approved as to its style and contents.

Board of Examiners

Md. Shamim Hossain
Lecturer
Department of Computer Science and Engineering
Sonargaon University (SU)

Supervisor

(Examiner Name and Signature)
Department of Computer Science and Engineering
Sonargaon University (SU)

Examiner 1

(Examiner Name and Signature)
Department of Computer Science and Engineering
Sonargaon University (SU)

Examiner 2

(Examiner Name and Signature)
Department of Computer Science and Engineering
Sonargaon University (SU)

Examiner 3

DECLARATION

We, hereby, declare that the work presented in this report is the outcome of the investigation performed by us under the supervision of **Md. Shamim Hossain, Lecturer,** Department of Computer Science and Engineering, Sonargaon University, Dhaka, Bangladesh. We reaffirm that no part of this project has been or is being submitted elsewhere for the award of any degree or diploma.

Countersigned

(Md. Shamim Hossain)
Supervisor

Signature

Din Islam
ID: CSE2301028110

Md. Ramzan
ID: CSE2301028019

Kamrul Hasan Sakib
ID: CSE2301028170

Rafayat Kabir Tonoy
ID: CSE2301028043

Aminul Islam Opu
ID: CSE2302029040

ABSTRACT

This project presents a comprehensive study and design of an enterprise network infrastructure for a corporate office located in a newly established three-floor building. The organization is expected to support approximately 600 users distributed among different departments, including Sales and Marketing, Human Resource and Logistics, Finance and Accounts, Administrator and Public Relations, and ICT, along with a dedicated Server Room. Since the new building has no existing network infrastructure, a secure, reliable, scalable, and efficient enterprise network is required to support current business operations and future expansion.

The proposed network infrastructure is designed using a structured approach that includes VLAN segmentation, IP addressing and subnetting, inter-VLAN routing, DHCP, static IP addressing for Server Room devices, OSPF dynamic routing, wireless networking, SSH-based remote management, switchport security, PAT, and Access Control Lists (ACLs). Six VLANs are created to logically separate departmental traffic: SALES (VLAN 10), HR (VLAN 20), FINANCE (VLAN 30), ADMIN (VLAN 40), ICT (VLAN 50), and SERVER-ROOM (VLAN 60). Dedicated DHCP services are used to dynamically assign IP addresses to network devices, while Server Room devices are configured with static IP addresses for reliable access and management.

Special security measures are implemented for the Finance and Accounts Department, including sticky MAC address learning and shutdown violation mode to prevent unauthorized devices from accessing protected switchports. OSPF is configured on routers and Layer 3 switches to provide efficient dynamic route advertisement, while DHCP helper addresses support communication between VLANs and centralized DHCP services. SSH is enabled for secure remote administration of routers and Layer 3 switches. PAT and ACLs are also implemented to provide controlled and secure Internet connectivity.

The complete network design is implemented and tested using appropriate networking technologies and configurations. Connectivity, IP address allocation, VLAN communication, routing, security mechanisms, wireless access, and Internet connectivity are verified through systematic testing. The overall design provides a reliable and manageable enterprise network infrastructure capable of supporting the organization's present requirements while allowing future scalability and expansion.

ACKNOWLEDGEMENT

At the very beginning, we would like to express our deepest gratitude to the Almighty Allah for giving us the ability, strength, patience, and knowledge to successfully complete our project entitled “A Comprehensive Study and Design of Enterprise Network Infrastructure for a 600-User Organization.”

We are truly fortunate to have received the kind guidance and supervision of **Md. Shamim Hossain, Lecturer,** Department of Computer Science and Engineering, Sonargaon University. His heartfelt support, valuable suggestions, continuous encouragement, and proper direction served as essential resources throughout the completion of our project.

We would also like to express our sincere gratitude to all the respected teachers of the Department of Computer Science and Engineering, Sonargaon University, for their valuable teaching, guidance, and support throughout our academic journey. Their dedication and efforts have inspired us and helped us develop the knowledge and skills necessary to complete this project.

Finally, we would like to express our deepest gratitude and love to our parents and family members for their continuous support, encouragement, patience, and endless love throughout our academic journey.

We are sincerely grateful to everyone who directly or indirectly contributed to the successful completion of “A Comprehensive Study and Design of Enterprise Network Infrastructure for an Organization.”

LIST OF ABBREVIATIONS

ACL	Access Control List
AP	Access Point
CLI	Command-Line Interface
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
ICMP	Internet Control Message Protocol
IP	Internet Protocol
ISP	Internet Service Provider
LAN	Local Area Network
MAC	Media Access Control
NAT	Network Address Translation
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PAT	Port Address Translation
RSA	Rivest–Shamir–Adleman
SSH	Secure Shell
STP	Spanning Tree Protocol
SVI	Switch Virtual Interface
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network

VTY	Virtual Terminal Line
WAN	Wide Area Network
WLAN	Wireless Local Area Network

TABLE OF CONTENTS

Title			Page No.
DECLARATION			iii
ABSTRACT			iv
ACKNOWLEDGEMENT			v
LIST OF ABBREVIATIONS			vi-vii
CHAPTER 1			1 – 8
INTRODUCTION			
1.1	Introduction		1-2
1.2	Background of the Project		3
1.3	Problem Statement		4
1.4	Aim of the Project		4
1.5	Objectives of the Project		5
	1.5.1	Scope of the Project	5
	1.5.2	Importance of the Project	6
	1.5.3	Proposed Network Solution	7
	1.5.4	Expected Outcome	7
	1.5.5	Conclusion	8
CHAPTER 2			9 – 12
FUNDAMENTALS OF COMPUTER NETWORKS AND NETWORK DEVICE CONFIGURATION			
2.1	Introduction to Computer Networks ……..		9
2.2	Types of Computer Networks		9
2.3	Network Devices		10
2.4	IP Addressing		10
2.5	Network Protocols		11
2.6	OSI and TCP/IP Models		11
2.7	Basic Device and SSH Configuration		12

Title Page No.

CHAPTER 3 13 – 16

NETWORK REQUIREMENTS AND ANALYSIS

3.1 Introduction..... 13

3.2 Network Architecture, Security Requirements..... 14

3.3 ISP Routers, Core Routers, Multilayer Switches, Access Switches .....…….. 14

3.4 VLAN-Based Architecture, Trunk Connectivity……. 15

3.5 Server Room, Wireless Network…….. 16

CHAPTER 4 17 –23

VLAN ACCESS AND TRUNK PORT CONFIGURATION

4.1 Introduction..... 17

4.2 Subnetting And DHCP Addressing..... 18

4.3 Static Server Addressing and Access and Trunk Ports…… 18

4.4 Inter-VLAN Routing and DHCP Helper Address…… 19

4.5 OSPF Routing and Routing Verification……. 19

4.6 Basic Device Configuration and SSH Configuration…….. 20

4.7 Finance Department Port Security, Sticky MAC Address and Shutdown Violation Mode…… 21

4.8 Blackhole VLAN, Wireless Network Configuration and Network Security……. 22

4.9 Security Testing and Network Verification……. 23

CHAPTER 5 24 – 31

NETWORK CONFIGURATION AND IMPLEMENTATION

5.1 Introduction..... 24

5.2 ISP Router Configuration……. 24

5.3 Core Router Configuration……... 25-26

5.4 Multilayer Switch Configuration……. 27

5.5 Access Switch Configuration……... 28

5.6 Network Redundancy and Configuration Verification…… 30

Title Page No.

5.7 Summary…….. 31

CHAPTER 6 32 –42

RESULTS AND DISCUSSION

6.1 Introduction..... 32

6.2 Expected Results and ACL Testing 32

6.3 Internet Connectivity, NAT and PAT and PAT Configuration……... 33

6.4 Access Control List and PAT and ACL Relationship…….. 34

6.5 Network Implementation Basic Device Configuration and VLAN and Switching Implementation……... 35

6.6 Inter-VLAN Routing, DHCP Implementation and DHCP Helper Address… 36

6.7 Server Room Implementation, OSPF Implementation and SSH Implementation..... 37

6.8 Finance Port Security, Wireless Network Implementation…….. 37

6.9 Testing Communication between All Network Devices…….. 38-42

CHAPTER 7 43

CONCLUSION AND FUTURE SCOPE

7.1 Conclusion……... 43

7.2 Future Scope…… 43

CHAPTER 8

APPENDIX : SERVER CONFIGURATIONS 44-51

8.1 DHCP Server Configuration…… 44

8.2 DHCP Server Configuration for Sales …… 45

8.3 DHCP Server Configuration for HR…… 46

8.4 DHCP Server Configuration for Finance……. 46

8.5 DHCP Server Configuration for Admin……. 47

8.6 DHCP Server Configuration for ICT…….. 48

8.7 DNS Server Configuration Static IP.……... 49

Title Page No.

8.8 DNS Server Configuration……... 50-51

REFERENCES..... 52

LIST OF TABLES

Figure No.	Title	Page No.
Table 3.1	The Building Structure	13
Table 4.1	The departmental VLAN structure	17
Table 4.2	The departmental VLAN structure and IP	18
Table 4.3	Server IP Addressing	18
Table 5.1	The VLAN and IP Gateway	24
Table 6.1	The VLAN and departmental structure	32
Table 6.2	Expected Results and ACL Testing	33

LIST OF FIGURES

Figure No.	Title	Page No.
Fig. 1.1	Complete Enterprise Network Infrastructure Design	2
Fig. 1.2	VLAN Architecture	3
Fig. 8.1	DHCP Server Configuration	44
Fig. 8.2	DHCP Server Configuration for Sales	45
Fig. 8.3	DHCP Server Configuration for HR	46
Fig. 8.4	DHCP Server Configuration for Finance	47
Fig. 8.5	DHCP Server Configuration for Admin	48
Fig. 8.6	DHCP Server Configuration for ICT	49
Fig. 8.7	DNS Server Configuration Static IP	50
Fig 8.8	DNS Server Configuration	51

CHAPTER 1
INTRODUCTION

1.1 Introduction

In the modern business environment, computer networking plays a vital role in ensuring efficient communication, data sharing, Internet connectivity, and resource management within corporate offices and enterprise organizations. A well-designed enterprise network enables employees from different departments to communicate effectively, access shared resources, use centralized services, and perform their daily activities efficiently.

This project focuses on designing and implementing a corporate office network infrastructure for a new three-floor building. The organization is expected to accommodate approximately 600 users across different departments. The first floor will contain the Sales and Marketing Department and the Human Resource and Logistics Department, with approximately 120 users expected in each department. The second floor will contain the Finance and Accounts Department and the Administrator and Public Relations Department, with approximately 120 users expected in each department. The third floor will contain the ICT Department, with approximately 120 users, and a dedicated Server Room containing approximately 12 devices.

To provide logical separation and efficient network management, separate VLANs will be assigned to each department**.** Sales will use VLAN 10, HR will use VLAN 20, Finance will use VLAN 30, Admin will use VLAN 40, ICT will use VLAN 50, and the Server Room will use VLAN 60**.** VLAN segmentation will help control broadcast traffic, improve network performance, and provide better security between different departments.The proposed network infrastructure will use Cisco 2811 routers, Cisco 2911 core routers, Cisco 3650 multilayer switches, and Cisco 2960 access switches. The multilayer switches will provide inter-VLAN routing, while the routers will provide connectivity between the internal enterprise network and the ISP. Access switches will be used to connect end-user devices and assign them to their respective VLANs.

The network will use a dedicated DHCP server located in the Server Room. All end-user devices are expected to obtain their IP addresses dynamically from the DHCP servers. However, devices located in the Server Room will be assigned static IP addresses to ensure consistent connectivity to important network services.

For dynamic routing, Open Shortest Path First (OSPF) will be configured on both routers and multilayer switches. OSPF will advertise routes dynamically throughout the network and provide an efficient routing mechanism for communication between different network segments.

Security is also an important part of the proposed network. SSH will be configured on all routers and Layer 3 switches to provide secure remote login and network device management. In addition, port security will be implemented for the Finance and Accounts Department. Each designated switchport will allow only one device to connect, using the sticky MAC-address method. The violation mode will be configured as shutdown to prevent unauthorized devices from accessing the network.

For Internet connectivity, Port Address Translation (PAT) will be configured using the respective outbound router interface IPv4 address. Appropriate Access Control List (ACL) rules will also be implemented to control and permit the required traffic between the internal network and the external network.

The project will also include appropriate subnetting and IP addressing, VLAN assignment, access and trunk port configuration, DHCP configuration, inter-VLAN routing, wireless network configuration, OSPF routing, network security, and communication testing. These technologies will work together to provide a reliable, secure, scalable, and manageable enterprise network infrastructure. The logical network design is intended not only to satisfy the organization's current business requirements but also to make the network future-proof. The design will allow additional users, devices, and network resources to be added in the future without requiring major changes to the overall network infrastructure.

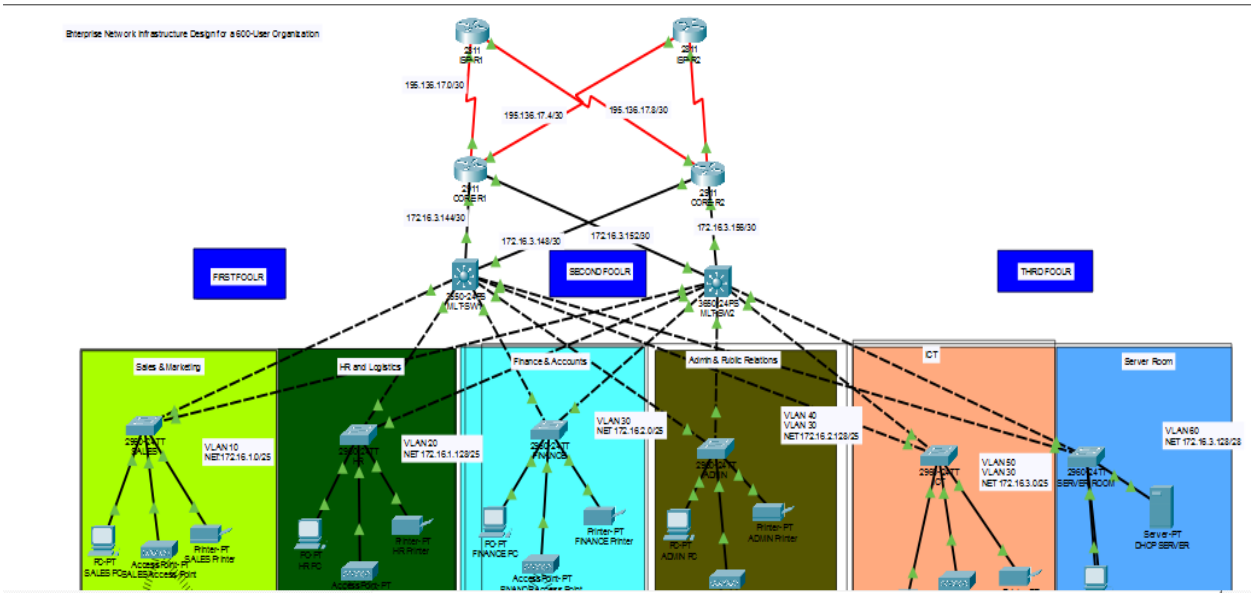


Fig: 1.1 Complete Enterprise Network Infrastructure Design

1.2 Background of the Project

The organization is planning to move into a new three-floor building that currently does not have a network infrastructure. Therefore, a complete enterprise network needs to be designed and implemented before the organization can fully operate from the new building.The organization will have approximately many users distributed across six main network segments and a dedicated Server Room. Due to the large number of users and different departmental requirements, a simple network design would not be sufficient. A structured enterprise network is required to provide reliable communication, efficient resource sharing, secure access, and effective network management.

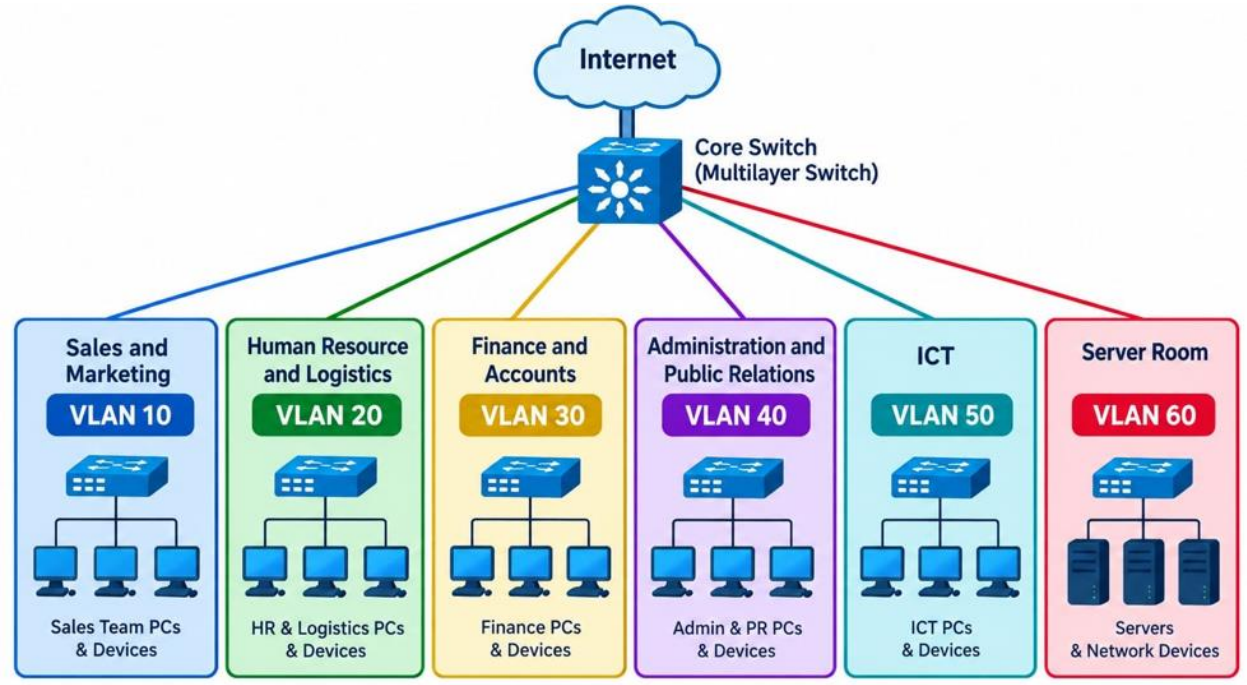


Fig. 1.2 VLAN Architecture

The first floor will accommodate the Sales and Marketing Department and the Human Resource and Logistics Department. The second floor will accommodate the Finance and Accounts Department and the Administrator and Public Relations Department. The third floor will contain the ICT Department and the Server Room.To meet these requirements, VLANs will be used to logically separate the departments. The VLAN structure will consist of VLAN 10 for Sales, VLAN 20 for HR, VLAN 30 for Finance, VLAN 40 for Admin, VLAN 50 for ICT, and VLAN 60 for the Server Room**.** The departmental VLAN structure is shown in **Fig. 1.2**.

1.3 Problem Statement

The new building does not currently have an existing network infrastructure. Therefore, a new enterprise network must be designed to support approximately 600 users distributed across multiple departments and three floors.

The major challenges that need to be addressed are:

- Providing reliable network connectivity for approximately 600 users.
- Connecting multiple departments across three floors.
- Creating separate VLANs for different departments.
- Providing efficient IP addressing and subnetting.
- Providing dynamic IP addresses through centralized DHCP servers.
- Assigning static IP addresses to Server Room devices.
- Providing communication between different VLANs through inter-VLAN routing.
- Implementing OSPF for dynamic route advertisement.
- Providing secure remote management through SSH.
- Protecting Finance department switchports using port security.
- Providing wireless network connectivity.
- Providing Internet access using PAT.
- Controlling required traffic using ACLs.
- Reducing unnecessary network traffic and improving performance.
- Designing a scalable and future-proof network infrastructure.
- Testing all network configurations to ensure proper communication.

Therefore, a well-planned logical enterprise network design is required to meet the current business requirements and support future organizational expansion.

1.4 Aim of the Project

The main aim of this project is to design a secure, reliable, scalable, and efficient corporate enterprise network infrastructure for the new three-floor building. The network will provide connectivity for approximately many users across different departments while supporting VLAN segmentation, centralized DHCP, inter-VLAN routing, OSPF dynamic routing, secure SSH management, wireless connectivity, port security, PAT, and ACL-based traffic control.

1.5 Objectives of the Project

The major objectives of this project are:

- To design a logical enterprise network for the new three-floor corporate building.

- To provide network connectivity for approximately 600 users.
- To create separate VLANs for different departments.
- To implement VLAN 10 for Sales, VLAN 20 for HR, VLAN 30 for Finance, VLAN 40 for Admin, VLAN 50 for ICT, and VLAN 60 for the Server Room**.**
- To perform appropriate subnetting and IP addressing.
- To configure all end-user devices to obtain IP addresses dynamically from dedicated DHCP servers.
- To assign static IP addresses to devices located in the Server Room.
- To configure inter-VLAN routing on multilayer switches.
- To configure DHCP helper addresses for communication with centralized DHCP servers.
- To configure OSPF on routers and multilayer switches for dynamic route advertisement.
- To configure SSH on all routers and Layer 3 switches for secure remote login.
- To implement port security for the Finance and Accounts Department.
- To allow only one device per designated Finance switchport using sticky MAC addresses.
- To configure violation mode as shutdown for Finance department port security.
- To configure wireless network connectivity.
- To configure PAT using the respective outbound router interface IPv4 address.
- To implement the necessary ACL rules for network traffic control.
- To configure access and trunk ports according to the VLAN design.
- To test communication and verify that all network configurations are working as expected.
- To design a scalable and future-proof network infrastructure.

1.5.1 Scope of the Project

The scope of this project covers the complete logical design and implementation requirements of the new corporate enterprise network. The network will cover three floors of the corporate building. The first floor will contain the Sales and Marketing Department and Human Resource and Logistics Department. The second floor will contain the Finance and Accounts Department and Administrator and Public Relations Department. The third floor will contain the ICT Department and Server Room.

The project includes:

- Basic configuration of network devices.
- SSH configuration on routers and Layer 3 switches.
- VLAN creation and departmental VLAN assignment.
- Access and trunk port configuration.
- IP addressing and subnetting.
- Inter-VLAN routing.
- DHCP server configuration.

- DHCP helper-address configuration.
- Static IP configuration for Server Room devices.
- OSPF configuration on routers and multilayer switches.
- Wireless network configuration.
- Finance department switchport security.
- PAT configuration.
- ACL configuration.
- Network connectivity and communication testing.

The network will use 2 Cisco 2811 ISP routers, 2 Cisco 2911 core routers, 2 Cisco 3650-24PS multilayer switches, and 6 Cisco 2960-24TT switches as specified in the proposed infrastructure.

1.5.2 Importance of the Project

The proposed enterprise network is important because it will provide the organization with a reliable communication and resource-sharing infrastructure. A properly designed network will allow employees from different departments to access required resources and communicate efficiently. VLAN segmentation will provide logical separation between departments and help reduce unnecessary broadcast traffic. Inter-VLAN routing will allow controlled communication between different VLANs where required. Centralized DHCP services will simplify IP address management, while static addressing for Server Room devices will ensure that critical servers and network resources remain consistently accessible.

OSPF will provide dynamic route advertisement and make the network easier to manage and expand. SSH will provide secure remote management of network devices, while port security will add an additional layer of protection to the Finance and Accounts Department. PAT will allow internal users to access the Internet using the outbound router interface address, while ACL rules will help control network traffic according to organizational requirements.

Overall, these technologies will improve network reliability, security, performance, manageability, and scalability.

1.5.3 Proposed Network Solution

The proposed network uses a structured enterprise architecture consisting of ISP routers, core routers, multilayer switches, access switches, servers, wireless devices, and end-user devices. End-user devices will connect to access switches through access ports. Trunk links will be used where required to carry multiple VLANs between network devices. The Cisco 3650 multilayer switches will perform inter-VLAN routing and use DHCP helper addresses to forward DHCP requests toward the centralized DHCP servers located in the Server Room.

OSPF will be configured on the routers and multilayer switches to dynamically advertise network routes. SSH will be enabled on routers and Layer 3 switches for secure remote administration. The Finance and Accounts Department will receive additional protection through switch port security. Each designated switch port will allow only one device, with MAC addresses learned using the sticky method. Any violation will result in the port being placed into shutdown mode.

For external connectivity, PAT will be configured on the appropriate outbound router interfaces. ACL rules will be applied to identify and control the required internal traffic before it is translated and forwarded to the Internet. The overall logical communication path can be represented as:

End Users → Access Switches → Multilayer Switches → Core Routers → ISP → Internet

This architecture provides centralized management, departmental segmentation, secure communication, efficient routing, and sufficient flexibility for future expansion.

1.5.4 Expected Outcome

After successful implementation, the proposed network is expected to provide reliable connectivity for approximately 600 users across the three-floor corporate building. The expected outcomes include:

- Successful communication within and between authorized VLANs.
- Automatic IP address allocation through centralized DHCP servers.
- Static IP addressing for Server Room devices.
- Successful OSPF route advertisement between routers and multilayer switches.
- Secure remote management through SSH.
- Successful implementation of Finance department port security.
- Reliable wireless network connectivity.
- Successful Internet connectivity through PAT.
- Appropriate traffic control through ACLs.
- Improved network performance through VLAN segmentation.
- Easier network administration and troubleshooting.
- A scalable network structure capable of supporting future expansion.

All major network configurations will be tested to ensure that communication and services operate according to the specified requirements.

1.5.5 Conclusion

This chapter presented the introduction, background, problem statement, aim, objectives, scope, importance, proposed solution, and expected outcomes of the corporate enterprise networking project. The proposed network is designed for a three-floor corporate building supporting approximately many users. The design incorporates VLANs, subnetting, IP addressing, DHCP, inter-VLAN routing, OSPF, [8]SSH, port security, wireless networking, PAT**,** and ACLs to create a secure, reliable, efficient, and scalable network infrastructure[3]. The network is designed according to the current business requirements while maintaining flexibility for future expansion [5]. The following chapters will discuss the detailed network requirements, logical topology, IP addressing and subnetting scheme, VLAN configuration, routing and switching implementation, security configuration, wireless network, PAT and ACL configuration, testing procedures, results, and future improvements [3].

CHAPTER 2
FUNDAMENTALS OF COMPUTER NETWORKS AND NETWORK DEVICE CONFIGURATION

2.1 Introduction to Computer Networks

A computer network is a system that connects two or more computers, servers, and other digital devices to communicate and exchange information. It allows users to share data, hardware resources, software, internet connections, and other services efficiently. Networks can use wired technologies such as Ethernet and fiber-optic cables or wireless technologies such as Wi-Fi. Computer networks are widely used in homes, educational institutions, businesses, banks, and large organizations. They play an important role in modern communication, information sharing, resource management, and internet connectivity.

2.2 Types of Computer Networks

Computer networks can be classified based on their geographical coverage and purpose. The main types of computer networks are LAN, MAN, and WAN.

- LAN (Local Area Network**):** A LAN connects devices within a small geographical area, such as an office, home, school, or building.
- MAN (Metropolitan Area Network**):** A MAN connects multiple LANs within a city or large metropolitan area.
- WAN (Wide Area Network): A WAN connects networks over large geographical distances, such as between cities, countries, or continents. The Internet is the largest example of a WAN. .

2.3 Network Devices

Network devices are hardware components used to connect computers and other devices, manage network traffic, provide network services, and maintain security. Common network devices include:

- Router**:** Connects different networks and forwards data packets between them.
- Switch**:** Connects multiple devices within a LAN and forwards data to the appropriate device.

- Multilayer Switch**:** A multilayer switch is an advanced network device that performs both switching and routing functions. It can support features such as VLANs, inter-VLAN routing, routing protocols, and network redundancy, making it suitable for enterprise networks.
- Server**:** Provides services and resources such as file sharing, DHCP, DNS, and web services to network users.
- Access Point**:** Provides wireless network connectivity to devices such as laptops, smartphones, and tablets.
- Firewall**:** Monitors and controls incoming and outgoing network traffic to protect the network from unauthorized access and security threats

2.4 IP Addressing

IP Addressing is a fundamental component of computer networking that involves assigning logical addresses to network devices for identification and communication. An IP address uniquely identifies a device within a network and enables the exchange of data between devices on the same network or across different networks. IP addressing also includes the use of subnet masks, default gateways and DNS servers to ensure proper network communication and efficient management of network resources. Proper IP addressing and subnetting are essential for designing a structured, scalable, and reliable network infrastructure.

2.5 Network Protocols

Network protocols are standardized rules and procedures that define how data is transmitted, received, and interpreted between devices over a computer network. They ensure reliable, efficient, secure, and consistent communication between different network devices and systems.

- TCP (Transmission Control Protocol): Provides reliable, connection-oriented, and ordered delivery of data between network devices.
- IP (Internet Protocol): Provides logical addressing and determines how data packets are routed between different networks.
- HTTP/HTTPS: Enables communication between web browsers and web servers. HTTPS provides encrypted and secure communication.
- DNS (Domain Name System): Translates domain names into corresponding IP addresses.
- DHCP (Dynamic Host Configuration Protocol): Automatically assigns IP addresses and other network configuration parameters to devices.
- FTP (File Transfer Protocol): Enables the transfer of files between networked devices.
- SSH (Secure Shell): Provides secure remote access and management of servers and network devices.
- SMTP (Simple Mail Transfer Protocol): Used for sending email messages over a network.

- ARP (Address Resolution Protocol): Resolves IPv4 addresses into corresponding MAC addresses within a local network.
- ICMP (Internet Control Message Protocol): Used for network diagnostics, error reporting, and connectivity testing such as ping.

2.6 OSI and TCP/IP Models

The OSI and TCP/IP models are conceptual frameworks used to understand, design, and troubleshoot network communication. They divide network communication into different layers, with each layer performing specific functions.

OSI Model:

The OSI (Open Systems Interconnection) model consists of seven layers:

- Physical Layer: Transmits raw bits through physical media such as cables, fiber optics, and wireless signals.
- Data Link Layer: Provides node-to-node communication, MAC addressing, and error detection. Switches primarily operate at this layer.
- Network Layer: Handles logical addressing and packet routing between networks. Routers operate mainly at this layer.
- Transport Layer: Provides end-to-end communication, reliability, flow control, and error recovery using protocols such as TCP and UDP.
- Session Layer: Establishes, manages, and terminates communication sessions between applications.
- Presentation Layer: Handles data formatting, encryption, decryption, and compression.
- Application Layer: Provides network services directly to user applications, such as web browsing, email, and file transfer.

TCP/IP Model

The TCP/IP (Transmission Control Protocol/Internet Protocol) model is the practical networking model used on the Internet. It consists of four layers:

- Network Access Layer: Handles physical transmission and data-link functions, including Ethernet and Wi-Fi.
- Internet Layer: Responsible for logical addressing and packet routing using protocols such as IP and ICMP.
- Transport Layer: Provides end-to-end communication using TCP and UDP.
- Application Layer: Provides services for network applications through protocols such as HTTP, HTTPS, DNS, DHCP, FTP, and SMTP.

2.7 Basic Device and SSH Configuration

Basic device configuration includes setting the hostname, passwords, banners, IP addresses, and other required parameters. These configurations prepare routers and switches for secure and proper network operation. Routers are configured with hostnames, passwords, interfaces, IP addresses, and routing settings. Proper router configuration enables communication between different networks and supports reliable network operation. Switches are configured with hostnames, passwords, VLANs, management IP addresses, and other required settings. These configurations allow switches to provide connectivity between devices within the network.

Secure Shell (SSH) provides secure remote access to routers and switches. It encrypts communication between the administrator and the network device, helping protect login credentials and management sessions. SSH is configured on all required routers and 12 switches in the network. This allows administrators to securely access and manage network devices remotely while reducing the security risks associated with unsecured remote access.

CHAPTER 3
NETWORK REQUIREMENTS AND ANALYSIS

3.1 Introduction

Network Requirements and Analysis is an essential stage of network design that identifies the organization's communication, connectivity, security, performance, and scalability requirements. It involves analyzing the existing situation, understanding the needs of users and departments, and determining the hardware, software, IP addressing, routing, security, and redundancy requirements. A proper requirement analysis helps ensure that the proposed enterprise network is reliable, secure, scalable, efficient, and capable of supporting the organization's current and future operational needs**.**

Building Structure and Department VLAN Assignment

The building is divided into three floors: The First Floor, Second Floor and Third Floor.

Table 3.1: Building Structure

Department	Department	VLAN
Sales and Marketing	120	VLAN 10
Human Resource and Logistics	120	VLAN 20
Finance and Accounts	120	VLAN 30
Administrator and Public Relations	120	VLAN 40
ICT	120	VLAN 50
Server Room	12 devices	VLAN 60

Total expected users:

120 × 5 = 600 users

The Server Room contains an additional 12 devices**.** The network will provide Configuration:

- DHCP
- DNS/Server services where required
- Inter-VLAN routing
- OSPF routing

- Wireless connectivity
- Internet connectivity
- Secure SSH management
- NAT/PAT
- ACL-based traffic control

3.2 Network Architecture, Security Requirements

The proposed network follows a hierarchical enterprise architecture consisting of access, distribution/multilayer, core, and ISP connectivity. The basic communication flow is:

End Devices → Access Switches → Multilayer Switches → Core Routers → ISP Routers → Internet

Security requirements include:

- VLAN segmentation
- SSH
- Port security
- Sticky MAC addresses
- Shutdown violation mode
- ACL
- Controlled Internet access

3.3 ISP Routers, Core Routers, Multilayer Switches, Access Switches

The proposed enterprise network uses different types of Cisco networking devices to provide reliable connectivity, routing, switching, inter-VLAN communication, and connectivity for end-user devices. The network infrastructure consists of Cisco 2811 routers for ISP connectivity, Cisco 2911 routers as core routing devices, Cisco 3650-24PS multilayer switches for Layer 3 functionality and inter-VLAN routing, and Cisco 2960-24TT switches for connecting end-user computers and other network devices.

ISP Routers

Two Cisco 2811 routers are used for ISP connectivity. These routers provide external network connectivity and support the required Internet configuration. The use of two ISP routers provides the required ISP connectivity for the enterprise network and supports the Internet connection between the internal network and external networks.

Core Routers

Two Cisco 2911 routers are used as core routing devices. These routers perform the core routing functions within the enterprise network. OSPF is configured on the core routers to dynamically advertise routes. This allows the routing devices to exchange network information dynamically and supports communication between different networks.

Multilayer Switches

Two Cisco 3650-24PS multilayer switches are used in the enterprise network. These switches provide Layer 3 functionality and perform inter-VLAN routing. The multilayer switches allow communication between different departmental VLANs while maintaining logical separation between the departments. The multilayer switches therefore play an important role in connecting the different VLANs and providing routing functionality within the internal enterprise network.

Access Switches

Cisco 2960-24TT switches are used to connect end-user computers and other devices to the enterprise network. These switches provide connectivity for users within their respective departments. Access ports on the switches are assigned to the appropriate VLANs. This allows end-user devices to operate within their designated departmental network and maintains the required VLAN-based network structure.

3.4 VLAN-Based Architecture, Trunk Connectivity

The network is logically divided into six VLANs according to different departments. VLANs are used to separate network traffic, improve security, reduce broadcast traffic, and make the network easier to manage. The VLANs are:

- VLAN 10 – Sales
- VLAN 20 – HR
- VLAN 30 – Finance
- VLAN 40 – Admin
- VLAN 50 – ICT
- VLAN 60 – Server Room

Each VLAN is assigned to a specific department or network section. This logical separation helps prevent unnecessary traffic between departments while allowing communication through Layer 3 routing when required.

Trunk ports are configured between appropriate switches and Layer 3 devices so that multiple VLANs can travel across the same physical link. Trunk connectivity allows VLANs 10, 20, 30, 40, 50, and 60 to share a single connection using VLAN tagging. This reduces the need for separate physical links and provides a more flexible, efficient, and scalable network design.

3.5 Server Room, Wireless Network

The Server Room is assigned to VLAN 60 to provide proper network separation and security for server-related devices. It contains approximately 12 devices, including servers and other network equipment. These devices are configured with static IP addresses to ensure stable and consistent network communication. Using static IP addresses also makes the servers easier to manage and access within the enterprise network.

Wireless Network

Wireless Access Points (APs) are deployed to provide wireless connectivity for authorized users and devices. The wireless network is integrated with the enterprise network so that users can access the required network resources securely. Proper wireless configuration helps provide flexible connectivity while maintaining network security and efficient management.

CHAPTER 4
VLAN ACCESS AND TRUNK PORT CONFIGURATION

4.1 Introduction

This chapter describes the IP addressing, subnetting, VLAN design, routing, switching, network services, wireless connectivity, and security mechanisms implemented in the proposed enterprise network. The design is structured to support approximately 600 users while allowing future expansion.

IP Addressing and VLAN Addressing Plan

A structured IPv4 addressing plan is required to support approximately 600 users and future network expansion. Each department is assigned a separate IP subnet corresponding to its VLAN. This approach provides logical segmentation, easier management, improved security, and efficient use of IP addresses.

The following **Table 4.1** VLAN structure is used to logically separate the departments and network services.

Table 4.1: The departmental VLAN structure

VLAN	Department	Purpose
10	Sales	Sales and Marketing
20	HR	Human Resource and Logistics
30	Finance	Finance and Accounts
40	Admin	Administrator and Public Relations
50	ICT	ICT Department
60	Server Room	Servers and Network Services
99	Black hole	Unused Switch Ports

Each department operates within its own VLAN and subnet. This separation reduces broadcast traffic and provides better control over departmental communication.

4.2 Subnetting and DHCP Addressing

Subnetting divides the available IP address space into smaller logical networks. Since each major department is expected to support approximately 120 users, a /25 subnet is suitable because it

provides 126 usable host addresses**.** The Server Room requires only 12 devices, so a /28 subnet is sufficient and provides 14 usable host addresses**.** A suitable addressing plan is shown **Table 4.2**.

Table 4.2: The departmental VLAN structure and IP

VLAN	Department	Network	Subnet Mask	Default Gateway
10	Sales	172.16.1.0/25	255.255.255.128	172.16.1.1
20	HR	172.16.1.128/25	255.255.255.128	172.16.1.129
30	Finance	172.16.2.0/25	255.255.255.128	172.16.2.1
40	Admin	172.16.2.128/25	255.255.255.128	172.16.2.129
50	ICT	172.16.3.0/25	255.255.255.128	172.16.3.1
60	Server Room	172.16.3.128/28	255.255.255.240	172.16.3.129

DHCP Addressing

All end-user devices are expected to obtain their IP addresses dynamically from dedicated DHCP servers located in the Server Room. DHCP provides the following network parameters:

- IP address
- Subnet mask
- Default gateway
- DNS server information

Centralized DHCP reduces manual configuration and makes IP address management easier for network administrators.

4.3 Static Server Addressing and Access and Trunk Ports

Devices located in the Server Room are assigned static IP addresses. Static addressing ensures that important network services maintain consistent IP addresses and remain easily accessible to users and administrators.

Table 4.3 Server IP Addressing

Server	IP Address
DHCP Server	172.16.3.130
DNS Server	172.16.3.131
Other Servers	172.16.3.132–142

Access and Trunk Ports

Access ports are configured for end-user devices and assigned to their respective departmental VLANs. For example, Finance user ports are assigned to VLAN 30, while Administration and ICT user ports are assigned to VLAN 40 and VLAN 50 respectively. Trunk ports are used for uplinks between access switches and multilayer switches. Trunking allows multiple VLANs to travel through a single physical connection.

4.4 Inter-VLAN Routing and DHCP Helper Address

The Cisco 3650 multilayer switches perform inter-VLAN routing. Each VLAN is configured with a Layer 3 Switch Virtual Interface (SVI), which acts as the default gateway for devices in that VLAN. This allows authorized communication between different departmental networks while maintaining logical VLAN separation.

DHCP Helper Address

Since the DHCP servers are located in VLAN 60 while users are distributed across different VLANs, DHCP helper addresses are configured on the corresponding Layer 3 interfaces. The helper address forwards DHCP requests from departmental VLANs to the centralized DHCP server for example:

```
interface vlan 10
ip helper-address 172.16.3.130
```

The same configuration principle is applied to the other departmental VLAN interfaces.

4.5 OSPF Routing and Routing Verification

Open Shortest Path First (OSPF) is used as the dynamic routing protocol in the enterprise network. OSPF is configured on the routers and multilayer switches to advertise internal network routes dynamically.

OSPF provides:

- Dynamic route advertisement
- Fast convergence
- Scalability
- Efficient route selection
- Reduced manual routing configuration
- Better support for network redundancy

An example OSPF configuration is:

```
router ospf 10
router-id 1.1.1.1
network 172.16.0.0 0.0.255.255 area 0
```

Routing Verification

OSPF operation and routing information can be verified using the following commands:

```
show ip ospf neighbor
show ip route
show ip protocols
```

These commands help confirm OSPF neighbor relationships, learned routes, and routing protocol configuration.

4.6 Basic Device Configuration and SSH Configuration

Basic configurations are applied to all routers and switches to provide consistent device management and security. The configuration includes:

- Hostname
- Console password
- Enable password
- Password encryption
- Banner message
- Disabled IP domain lookup
- SSH remote management

Example:

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname ADMIN-SW
ADMIN-SW(config)#banner motd #No Unauthorised Access!!!#
ADMIN-SW(config)#no ip domain lookup
ADMIN-SW(config)#line console 0
ADMIN-SW(config-line)#password cisco
ADMIN-SW(config-line)#login
ADMIN-SW(config-line)#exit
ADMIN-SW(config)#enable password cisco
ADMIN-SW(config)#service password-encryption
```

SSH Configuration

Secure Shell (SSH) is configured on all routers and Layer 3 switches to provide secure remote access. SSH encrypts communication between the administrator and network devices and provides a more secure alternative to unsecured remote-management protocols.

4.7 Finance Department Port Security, Sticky MAC Address and Shutdown Violation Mode.

Port security is specifically implemented for the Finance and Accounts Department because financial systems and information require additional protection. The Finance switchports are configured to allow only one device per port.

The configuration uses:

- Maximum one MAC address
- Sticky MAC address learning
- Shutdown violation mode

Example:

```
Finance-SW(config)#interface range fa0/3-24
Finance-SW(config-if-range)#switchport port-security
Finance-SW(config-if-range)#switchport port-security maximum 1
Finance-SW(config-if-range)#switchport port-security mac-address sticy
Finance-SW(config-if-range)#switchport port-security violation shut
Finance-SW(config-if-range)#exit
```

Sticky MAC Address

Sticky MAC address learning allows the switch to dynamically learn the MAC address of the device connected to a protected switchport. The learned MAC address is then associated with that port. This reduces the possibility of unauthorized devices connecting to the Finance network.

Shutdown Violation Mode

The shutdown violation mode is configured so that if an unauthorized device attempts to connect to a protected Finance switchport, the switchport is placed into a shutdown or error-disabled state. This provides an additional layer of protection for the Finance department.

4.8 Blackhole VLAN, Wireless Network Configuration and Network Security

VLAN 99 is configured as a Blackhole VLAN for unused switch interfaces. Unused ports are assigned to VLAN 99 rather than remaining in the default VLAN.

Example:

```
interface range gig0/1-2
switchport mode access
switchport access vlan 99
exit
```

This configuration helps reduce the risk of unauthorized access through unused switchports.

Wireless Network Configuration

Each department is provided with a dedicated wireless network to support laptops, mobile devices, and other wireless clients.

The wireless configuration includes:

- SSID configuration
- Wireless security
- IP addressing
- VLAN integration
- Connectivity testing

Wireless users are connected to their appropriate departmental network so that wireless and wired users can access authorized network services.

Network Security

Several security mechanisms are implemented throughout the network, including SSH, VLAN segmentation, Finance port security, Blackhole VLAN configuration, password protection, and ACLs. These mechanisms help protect network devices, users, and organizational resources from unauthorized access.

4.9 Security Testing and Network Verification

The implemented security features are tested to verify proper operation.

The following tests are performed:

- SSH remote login testing
- Finance port-security testing
- Unauthorized-device testing
- Wireless authentication testing
- VLAN isolation testing
- ACL testing
- Network connectivity testing

Network Verification

The final network configuration is verified using different Cisco IOS commands. Important verification commands include:

```
show vlan brief
show interfaces trunk
show ip interface brief
show ip route
show ip ospf neighbor
show port-security
show port-security address
```

These commands are used to confirm VLAN assignments, trunk connections, IP interfaces, routing information, OSPF operation, and port-security status.The multilayer switches provide inter-VLAN routing, while DHCP provides dynamic IP addressing and OSPF provides dynamic route advertisement. SSH, port security, Blackhole VLANs, and other security mechanisms improve the overall security of the infrastructure. The combination of these technologies provides a scalable, manageable, secure, and reliable network suitable for the organization's current requirements and future expansion.

CHAPTER 5
NETWORK CONFIGURATION AND IMPLEMENTATION

5.1 Introduction

This chapter describes the configuration and implementation of the proposed enterprise network using Cisco routers, multilayer switches, and access switches in Cisco Packet Tracer. The configuration includes basic device settings, secure remote access using SSH, IP addressing, VLAN implementation, inter-VLAN routing, OSPF routing, NAT, DHCP relay, trunking, and switch port security. VLANs are configured to enable inter-VLAN routing is shown in **Table 5.1**:

Table 5.1: The VLAN and IP Gateway

VLAN	Gateway IP
VLAN 10	172.16.1.1/25
VLAN 20	172.16.1.129/25
VLAN 30	172.16.2.1/25
VLAN 40	172.16.2.129/25
VLAN 50	172.16.3.1/25
VLAN 60	172.16.3.129/25

5.2 ISP Router Configuration

Two ISP routers, ISP-R1 and ISP-R2, are configured to provide redundant Internet connectivity. Basic security settings, serial interface IP addresses, and OSPF routing are configured on both routers.

ISP-R1 Basic Configuration

The ISP-R1 router is configured with a hostname, console password, enable password, password encryption, domain lookup disabled, and a MOTD banner.

ISP-R1 Interface Configuration

The serial interfaces are assigned IP addresses using /30 subnets for point-to-point communication with the core routers.

- Serial0/3/0: 195.136.17.2/30
- Serial0/3/1: 195.136.17.10/30

ISP-R1 OSPF Configuration

OSPF process 10 is configured with router ID 5.5.5.5**.** The connected /30 networks are advertised in OSPF Area 0 to establish dynamic routing with the core network.

ISP-R2 Configuration

ISP-R2 is configured as the second redundant ISP router. Basic security settings, interface addressing, and OSPF routing are implemented.

ISP-R2 Interface Configuration

The serial interfaces are configured with the following IP addresses:

- Serial0/3/0: 195.136.17.6/30
- Serial0/3/1: 195.136.17.14/30

ISP-R2 OSPF Configuration

OSPF process 10 is configured to advertise the connected networks in Area 0. This enables dynamic routing between ISP-R2 and the core routers.

5.3 Core Router Configuration

Two core routers, CORE-R1 **and** CORE-R2, are configured to provide routing, redundancy, NAT, and connectivity between the enterprise network and the ISP routers.

CORE-R1 Configuration

CORE-R1 is configured with basic security settings, SSH access, Gigabit Ethernet interfaces, serial interfaces, and OSPF routing.

CORE-R1 Basic Configuration

The basic configuration includes:

- Hostname configuration
- Console password
- Enable password
- MOTD banner

- Password encryption
- Domain lookup disabled

CORE-R1 SSH Configuration

SSH is configured to provide secure remote administration. A domain name, local administrator account, RSA key, VTY lines, and SSH version 2 are configured.

CORE-R1 Interface Configuration

The following IP addresses are configured:

- GigabitEthernet0/0: 172.16.3.146/30
- GigabitEthernet0/1: 172.16.3.154/30
- Serial0/2/0: 195.136.17.1/30
- Serial0/2/1: 195.136.17.5/30

Clock rate 64000 is configured on the appropriate serial interfaces.

CORE-R1 OSPF Configuration

OSPF process 10 with router ID **3.3.3.3** is configured. The connected internal and ISP-facing networks are advertised through Area 0.

CORE-R2 Configuration

CORE-R2 provides the second core routing path and supports redundancy, OSPF, NAT, and default routing.

CORE-R2 Basic and SSH Configuration

CORE-R2 is configured with hostname, console password, enable password, MOTD banner, password encryption, domain name, local user account, RSA keys, and SSH version 2.

CORE-R2 Interface Configuration

The following addresses are assigned:

- GigabitEthernet0/0**:** 172.16.3.150/30
- Serial0/2/0: 195.136.17.9/30
- Serial0/2/1: 195.136.17.13/30

The serial interfaces are configured with a clock rate of 64000 where required.

CORE-R2 OSPF Configuration

OSPF process 10 is configured with router ID 4.4.4.4**.** The internal and ISP-facing networks are advertised in Area 0.

NAT Configuration

Network Address Translation (NAT) is configured on the core routers to allow internal private IP addresses to communicate with external networks.

An extended range of internal enterprise networks is permitted through access list 1, including:

- 172.16.1.0/25
- 172.16.1.128/25
- 172.16.2.0/25
- 172.16.2.128/25
- 172.16.3.0/25
- 172.16.3.128/28

NAT overload is configured on the ISP-facing serial interfaces to translate multiple private addresses using the available external interface address.

Default Route Configuration

Default routes are configured on CORE-R2 toward both ISP connections to provide Internet connectivity and redundancy. A primary default route is configured through Serial0/2/0, while a floating static default route with administrative distance **70** is configured through Serial0/2/1.

5.4 Multilayer Switch Configuration and MLT-SW1 Configuration

Two multilayer switches, MLT-SW1 and MLT-SW2, are configured to provide Layer 2 switching and Layer 3 routing functions. These switches provide VLAN segmentation, inter-VLAN routing, DHCP relay, OSPF routing, and redundant uplinks.

MLT-SW1 is configured with basic security settings, SSH, VLANs, routed interfaces, OSPF, and switched virtual interfaces (SVIs).

MLT-SW1 Trunk Configuration

GigabitEthernet1/0/3–1/0/8 are configured as trunk ports to carry multiple VLANs between network devices.

MLT-SW1 Routed Interface Configuration

GigabitEthernet1/0/1 and GigabitEthernet1/0/2 are configured as Layer 3 routed interfaces.

- GigabitEthernet1/0/1: 172.16.3.145/30
- GigabitEthernet1/0/2: 172.16.3.149/30

MLT-SW1 SVI Configuration

The DHCP helper address 172.16.3.130 is configured on the VLAN interfaces to forward DHCP requests to the DHCP server.

MLT-SW2 Configuration

MLT-SW2 is configured similarly to MLT-SW1 to provide Layer 3 switching, VLAN routing, OSPF, DHCP relay, and redundant connectivity.

MLT-SW2 Routed Interface Configuration

The following routed interfaces are configured:

- GigabitEthernet1/0/1: 172.16.3.153/30
- GigabitEthernet1/0/2**:** 172.16.3.157/30

MLT-SW2 VLAN and SVI Configuration

VLANs 10, 20, 30, 40, 50, and 60 are configured for the Sales, HR, Finance, Admin, ICT, and Server-Room departments.

The corresponding SVIs are configured with gateway addresses and DHCP helper address 172.16.3.130**.**

MLT-SW2 OSPF Configuration

OSPF process 10 is configured to advertise the internal VLAN networks and routed /30 networks through Area 0.

MLT-SW2 Default Route

Two default routes are configured toward the core network. The second route is configured with administrative distance **70** to provide a backup path.

5.5 Access Switch Configuration

Access switches are deployed for different departments to provide end-user connectivity. The following switches are configured:

- Sales-SW1
- HR-SW
- Finance-SW
- ADMIN-SW
- ICT-SW
- ServerRoom-SW

Sales Switch Configuration

Sales-SW1 is configured with VLAN 10 for the Sales department. FastEthernet0/1–0/2 are configured as trunk ports, while FastEthernet0/3–0/24 are assigned to VLAN 10. Unused GigabitEthernet ports are assigned to VLAN 99, which is used as a Blackhole VLAN for security purposes.

HR Switch Configuration

HR-SW is configured with VLAN 20 for the HR department. FastEthernet0/1–0/2 are configured as trunk ports, and FastEthernet0/3–0/24 are configured as access ports in VLAN 20.Unused GigabitEthernet ports are assigned to VLAN 99.

Finance Switch Configuration

Finance-SW is configured with VLAN 30 for the Finance department. FastEthernet0/3–0/24 are assigned to VLAN 30, while GigabitEthernet0/1–0/2 are assigned to VLAN 99.

Port Security

Port security is implemented on the Finance department access ports to improve network security. The configuration allows a maximum of one MAC address per port, uses sticky MAC address learning, and shuts down the port when a security violation occurs.

Admin Switch Configuration

ADMIN-SW is configured with VLAN 40 for the Administration department. FastEthernet0/1–0/2 are configured as trunk ports, while FastEthernet0/3–0/24 are assigned to VLAN 40. Unused GigabitEthernet ports are assigned to VLAN 99.

ICT Switch Configuration

ICT-SW is configured with VLAN 50 for the ICT department. FastEthernet0/1–0/2 are configured as trunk ports, and FastEthernet0/3–0/24 are configured as access ports in VLAN 50. Unused GigabitEthernet ports are assigned to VLAN 99.

Server Room Switch Configuration

ServerRoom-SW is configured with VLAN 60 for the Server Room. FastEthernet0/1–0/2 are configured as trunk ports, while FastEthernet0/3–0/24 are assigned to VLAN 60. Unused GigabitEthernet ports are assigned to VLAN 99.

5.6 Network Redundancy and Configuration Verification

Network redundancy is implemented using two ISP routers, two core routers, and two multilayer switches. Multiple network paths are configured to reduce the possibility of network failure. OSPF provides dynamic route learning, while floating static routes provide backup connectivity.

Configuration Verification

After completing the configuration, network connectivity and routing are verified using Cisco IOS commands such as:

```
show ip interface brief

show ip route

show ip ospf neighbor

show ip ospf

show vlan brief

show interfaces trunk

show ip nat translations

show ip nat statistics

show port-security
```

```
show port-security interface

show running-config

ping

traceroute
```

These verification commands are used to confirm interface status, VLAN operation, OSPF neighbor relationships, routing tables, NAT translations, port security, and end-to-end connectivity.

5.7 Summary

This chapter presented the complete configuration and implementation of the enterprise network. The configuration includes ISP and core router setup, multilayer switching, VLAN segmentation, inter-VLAN routing, OSPF, NAT, DHCP relay, SSH, trunking, port security, and redundant network paths. These configurations provide a structured, secure, scalable, and reliable network infrastructure for the organization.

CHAPTER 6
NETWORK DESIGN AND IMPLEMENTATION

6.1 Introduction

This chapter presents the Internet connectivity, network implementation, configuration verification, testing, expected results, discussion, future improvements, and conclusion of the proposed enterprise network. The implementation is based on the logical design described in the previous chapters and is developed using Cisco Packet Tracer. The network incorporates VLANs, subnetting, inter-VLAN routing, DHCP, OSPF, SSH, wireless connectivity, port security, PAT, and ACLs to provide a reliable, secure, scalable, and manageable enterprise network.

These configurations provide basic protection and allow administrators to manage the network devices effectively. Each department is assigned a separate VLAN shown in **Table 6.1**:

Table 6.1: The VLAN and departmental structure

VLAN	Department
10	Sales
20	HR
30	Finance
40	Admin
50	ICT
60	Server Room
99	Blackhole

6.2 Expected Results and ACL Testing

ACL behavior is tested to verify that required traffic is permitted and restricted traffic is appropriately controlled. The configured ACLs can be checked using:

```
show access-lists
```

Successful ACL testing confirms that the required traffic-control rules are functioning correctly and expected results are shown in **Table 6.2**.

Table 6.2: Expected Results

Test	Expected Result
VLAN	Correct VLAN assignment
DHCP	Dynamic IP address received
Server Room	Static IP addresses maintained
Inter-VLAN	Authorized communication successful
OSPF	Routes advertised dynamically
SSH	Secure remote login successful
Port Security	Only authorized device allowed
Wireless	Authorized users connected
PAT	Internet access successful
ACL	Required traffic controlled
VLAN	Correct VLAN assignment

6.3 Internet Connectivity, NAT and PAT and PAT Configuration

The corporate network requires reliable Internet connectivity for users, servers, and organizational services. Two ISP connections are incorporated into the network to provide Internet redundancy.

The enterprise routers provide connectivity between the internal corporate network and the external Internet networks. Each router is connected to the available ISP connections to improve network availability and reduce dependency on a single Internet connection.

The following public IPv4 networks are used for the ISP connections:

- 195.136.17.0/30
- 195.136.17.4/30
- 195.136.17.8/30
- 195.136.17.12/30

NAT and PAT

Private IPv4 addresses used inside the corporate network cannot normally be routed directly over the public Internet. Therefore, Network Address Translation (NAT) is required.

Port Address Translation (PAT) is implemented so that multiple internal devices can share the IPv4 address of the respective outbound router interface. The general communication process is:

Internal Private IP → PAT → Outbound Interface IP → Internet

PAT reduces the requirement for multiple public IPv4 addresses and allows many internal users to access the Internet through the available external interface.

PAT Configuration

PAT is configured to use the respective outbound router interface IPv4 address. An ACL identifies the internal private networks that are allowed to be translated. The general configuration process consists of:

1. Identifying the internal networks.
2. Creating an ACL for the internal addresses.
3. Configuring the appropriate NAT overload rule.
4. Identifying the inside interfaces.
5. Identifying the outside interface.
6. Testing Internet connectivity.

6.4 Access Control List and PAT and ACL Relationship

Access Control Lists (ACLs) are used to identify and control network traffic. In this project, an ACL is used as part of the PAT implementation to identify the internal addresses that are permitted to access the external network. ACLs provide an additional layer of traffic control and can also be extended in the future to restrict unauthorized communication between network segments.

PAT and ACL Relationship

The ACL and PAT work together to provide Internet access. The ACL identifies the internal IP addresses that are permitted to be translated, while PAT translates those private addresses into the public IPv4 address of the appropriate outbound router interface. Therefore, the process can be summarized as:

Private Network → ACL Permission → PAT Translation → Public Interface → Internet

6.5 Network Implementation, Basic Device Configuration and VLAN

The complete network implementation follows the logical design established in the previous chapters. The major implementation activities include:

1. Basic configuration of routers and switches.
2. VLAN creation and assignment.
3. Access port configuration.
4. Trunk port configuration.
5. IP addressing and subnetting.
6. Inter-VLAN routing.
7. DHCP server configuration.
8. DHCP helper address configuration.
9. OSPF configuration.
10. SSH configuration.
11. Finance department port security.
12. Wireless network configuration.
13. PAT configuration.
14. ACL configuration.
15. Network verification and testing.

Basic Device Configuration

Basic configurations are applied to all routers and switches to provide consistent device management and security. The configuration includes:

- Hostname
- Console password
- Enable password
- Password encryption
- Banner message
- Disabled IP domain lookup

- SSH remote management

Access ports are assigned to the appropriate departmental VLAN, while trunk ports are used to carry multiple VLANs between network devices. Unused switchports are assigned to VLAN 99, which is configured as the Blackhole VLAN.

6.6 Inter-VLAN Routing, DHCP Implementation and DHCP Helper Address

The Cisco 3650 multilayer switches provide inter-VLAN routing. Each VLAN is configured with an SVI that acts as the default gateway for the corresponding subnet.

This allows authorized devices in different departments to communicate with each other. For example:

Sales → HR → Finance → Admin → ICT → Server Room

Communication between these networks is controlled through the Layer 3 switching and routing configuration.

DHCP Implementation

Dedicated DHCP servers are located in the Server Room. DHCP automatically provides IP configuration to end-user devices. The DHCP service provides:

- IP address
- Subnet mask
- Default gateway
- DNS server information

DHCP reduces manual configuration and simplifies IP address management for approximately many users.

DHCP Helper Address

Because DHCP servers are located in VLAN 60 while users are located in different VLANs, DHCP helper addresses are configured on the Layer 3 interfaces. The helper address forwards DHCP broadcast requests from each departmental VLAN to the centralized DHCP server.

Example:

```
interface vlan 10
ip helper-address 172.16.3.130
```

The same principle is applied to the other departmental VLAN interfaces.

6.7 Server Room Implementation, OSPF Implementation and SSH Implementation

Server Room devices are configured with static IP addresses to ensure that important network services remain consistently accessible. Static addressing is important for servers because their addresses need to remain consistent for clients and administrators.

OSPF Implementation

OSPF is configured on the enterprise routers and multilayer switches to dynamically advertise network routes.

OSPF provides:

- Dynamic route advertisement
- Fast convergence
- Scalability
- Efficient route selection
- Reduced manual routing configuration
- Support for network redundancy

OSPF operation can be verified using:

```
show ip ospf neighbor
show ip route
show ip protocols
```

SSH Implementation

SSH is configured on all routers and Layer 3 switches for secure remote management. SSH provides encrypted communication between network administrators and network devices. Successful SSH authentication confirms that secure remote management has been configured correctly.

6.8 Finance Port Security, Wireless Network Implementation

Port security is implemented on the Finance department switchports to protect sensitive financial systems and information.

The Finance switchports are configured with:

- Maximum one device per port.
- Sticky MAC address learning.
- Shutdown violation mode.

Example:

```
interface range fa0/3-24
switchport port-security
switchport port-security maximum 1
switchport port-security mac-address sticky
switchport port-security violation shutdown
```

If an unauthorized device attempts to connect to a protected Finance port, the port enters a shutdown or error-disabled state.

Wireless Network Implementation

Each department is provided with wireless connectivity for authorized users. The wireless implementation includes:

- SSID configuration
- Wireless security
- IP addressing
- VLAN integration
- User connectivity
- Internet connectivity

Wireless clients are connected to their appropriate departmental network and receive IP addresses through DHCP.

6.9 Testing Communication between All Network Devices

After completing the configuration, communication between devices and network segments is tested. The basic connectivity test is performed using:

```
Ping <destination-IP>
```

Successful ping responses confirm that the required devices and network segments can communicate.

VLAN Testing

VLAN assignments are verified using:

```
show vlan brief
```

This command confirms whether the required switchports have been assigned to the correct VLANs.

Trunk Testing

Trunk connections are verified using:

```
show interfaces trunk
```

This confirms whether the required VLAN traffic is being carried through the configured trunk links.

DHCP Testing

DHCP functionality is tested by checking whether end-user devices automatically receive:

- IP address
- Subnet mask
- Default gateway
- DNS information

Successful DHCP allocation confirms that the DHCP server, VLAN configuration, and DHCP helper addresses are functioning correctly.

Inter-VLAN Testing

Communication between authorized VLANs is tested using ping.

Examples include:

- Sales VLAN → HR VLAN
- HR VLAN → Finance VLAN
- Finance VLAN → Admin VLAN
- Admin VLAN → ICT VLAN
- ICT VLAN → Server Room VLAN

Successful communication confirms that inter-VLAN routing is functioning correctly.

OSPF Testing

OSPF neighbor relationships are verified using:

```
show ip ospf neighbor
```

The routing table is checked using:

```
show ip route
```

Successful route advertisement confirms that OSPF is operating correctly.

SSH Testing

SSH access is tested from an authorized management device. Successful authentication confirms that secure remote management is functioning correctly on the routers and multilayer switches.

Port Security Testing

The Finance department port-security configuration is tested using both authorized and unauthorized devices.

The authorized device should be permitted to communicate normally. When an unauthorized device is connected, the configured violation action should place the switchport into shutdown/error-disabled mode.

The following command can be used for verification:

```
Show port-security interface fa0/3
```

Wireless Testing

Wireless connectivity is tested for:

- SSID visibility
- Authentication
- IP address assignment
- Internal network connectivity
- Internet connectivity

Successful tests confirm that wireless users can access the required network services.

PAT Testing

Internet access is tested from internal users. PAT translations can be verified using:

```
show ip nat translations
```

PAT statistics can be checked using:

```
show ip nat statistics
```

Successful translation confirms that internal private IP addresses are being translated through the appropriate outbound r outer interface.

Discussion

The proposed enterprise network provides a structured approach to connecting approximately many users across three floors. VLAN segmentation separates departmental traffic, while multilayer switching provides inter-VLAN routing.

Centralized DHCP simplifies IP address management, while static addressing ensures reliable access to Server Room services. OSPF provides dynamic route advertisement and improves the scalability of the network.

Security is strengthened through SSH, VLAN segmentation, Finance department port security, Blackhole VLAN configuration, wireless security, PAT, and ACL-based traffic control.

The use of two routers, two multilayer switches, and two ISP connections also provides redundancy and improves network availability.

Future Improvements

The network can be further improved in the future by implementing:

- Network monitoring systems
- Additional security appliances
- Advanced firewall policies
- Network Access Control (NAC)
- Centralized logging and monitoring
- Backup servers
- Additional wireless access points
- IPv6 support
- Higher-capacity switches

- Additional redundancy mechanisms
- Improved Internet bandwidth

These improvements would further increase the network's scalability, security, availability, and performance.

Future-Proofing

The proposed network is designed with future expansion in mind. The IP addressing scheme provides sufficient flexibility for additional users and devices, while the VLAN structure allows new departments and network segments to be added without major changes to the existing infrastructure.

The hierarchical switching and routing architecture also supports scalability. Additional access switches can be connected when required, and OSPF can dynamically advertise new networks.

The use of centralized DHCP, wireless connectivity, VLAN segmentation, and redundant network devices further ensures that the network can accommodate future growth while maintaining performance, security, and reliability.

Conclusion

This project presented the logical design and implementation of a corporate enterprise network for a new three-floor building supporting approximately 600 users. The proposed infrastructure uses Cisco 2811 ISP routers, Cisco 2911 routers, Cisco 3650-24PS multilayer switches, and Cisco 2960-24TT access switches. Separate VLANs are used to logically isolate Sales, HR, Finance, Admin, ICT, and Server Room resources.

The network incorporates subnetting, DHCP, static Server Room addressing, inter-VLAN routing, OSPF, SSH, Finance department port security, wireless networking, PAT, and ACLs. Two routers, two multilayer switches, and two ISP connections provide network redundancy, while the hierarchical architecture supports scalability and future expansion.

The testing and verification procedures are designed to confirm VLAN operation, DHCP allocation, inter-VLAN communication, OSPF routing, SSH access, port security, wireless connectivity, PAT translation, and ACL functionality.

Overall, the proposed network provides a reliable, secure, scalable, manageable, and future-proof foundation for the organization's communication and business operations.

CHAPTER 7
CONCLUSION AND FUTURE SCOPE

7.1 Conclusion

This project successfully designed and implemented an enterprise network using Cisco Packet Tracer. The network was developed to provide secure, reliable, and efficient communication among different departments and network devices.[1]The project included basic device configuration,[6] SSH for secure remote management, VLAN implementation, access and trunk port configuration, switchport security, subnetting and IP addressing, OSPF dynamic routing, static IP configuration for Server Room devices, DHCP services, Inter-VLAN routing, wireless networking, PAT, and ACL configuration.[5]These technologies were integrated to improve network performance, security, manageability, and connectivity. [8]VLANs provided proper departmental segmentation, while OSPF enabled efficient communication between network segments. DHCP simplified IP address management, and Inter-VLAN routing allowed controlled communication between different departments. PAT provided Internet connectivity, while ACLs and switchport security improved network protection [3].

Overall, the project demonstrates the practical application of enterprise networking concepts and provides a structured network infrastructure suitable for an organizational environment [7].

7.2 Future Scope

The proposed network can be further improved by implementing advanced security and network management technologies. A dedicated firewall, IDS/IPS, and VPN can be added to provide stronger protection and secure remote access.

Network monitoring tools such as SNMP and Syslog can be introduced to monitor device performance and identify network failures. IPv6 can also be implemented to support future network growth. Additional redundancy, load balancing, centralized authentication, and cloud-based services can further improve network reliability, security, and scalability. These enhancements would allow the network to support a larger number of users, devices, and services while maintaining efficient and secure network operations.

CHAPTER 8

APPENDIX: SERVER CONFIGURATIONS

8.1 DHCP Server Configuration

DHCP Server Configuration Steps

1. Open the DHCP Server device.
2. DHCP Server Configuration IP
3. Go to the Services tab.
4. Select DHCP from the available services.
5. Turn the DHCP Service ON**.**
6. Enter the required DHCP pool information:
    - Pool Name
    - Default Gateway
    - DNS Server
    - Start IP Address
    - Subnet Mask
    - Maximum Number of Users
7. Click Add to create the DHCP pool.
8. Configure the client devices to obtain an IP address automatically using DHCP**.**
9. Verify that the client devices receive IP addresses successfully.

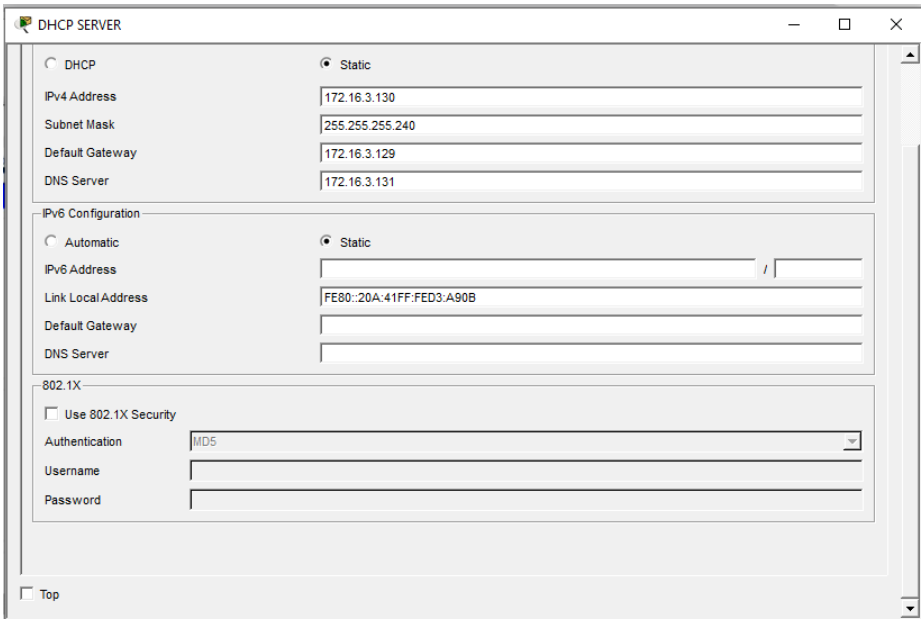


Fig:8.1 DHCP Server Configuration

DHCP Server Configuration for All Departments

- Sales Department
- HR Department
- Finance Department
- Administration Department
- ICT Department

8.2 DHCP Server Configuration for Sales

Pool name Sales Pool

Defult gateway 172.16.1.1

DNS Server: 172.16.1.6

Start IP Address: 172.16.1.126

Subnet Mask: 255.255.255.128

Maximum number of Users: 120

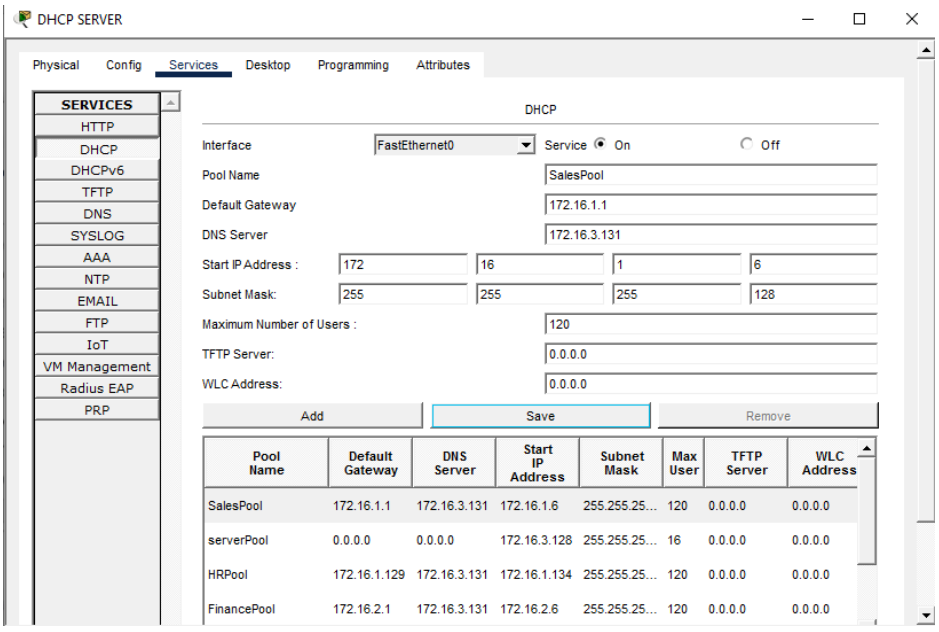


Fig 8.2 DHCP Server Configuration for Sales

8.3 DHCP Server Configuration for HR

Pool name HR Pool

Defult gateway 172.16.1.129

DNS Server: 172.16.3.131

Start IP Address:172.16.1.131

Subnet Mask:255.255.255.128

Maximum number of Users: 120

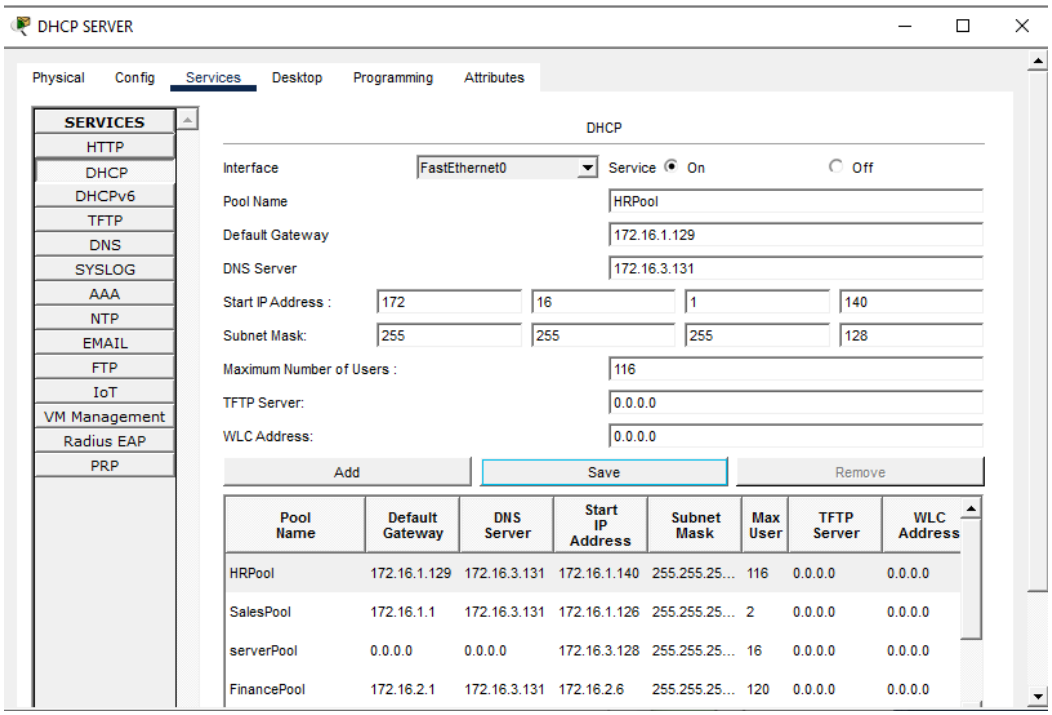


Fig 8.3 DHCP Server Configuration for HR

8.4 DHCP Server Configuration for Finance

Pool name Finance Pool

Defult gateway 172.16.1.129

DNS Server: 172.16.3.131

Start IP Address:172.16.1.131

Subnet Mask:255.255.255.128

Maximum number of Users: 120

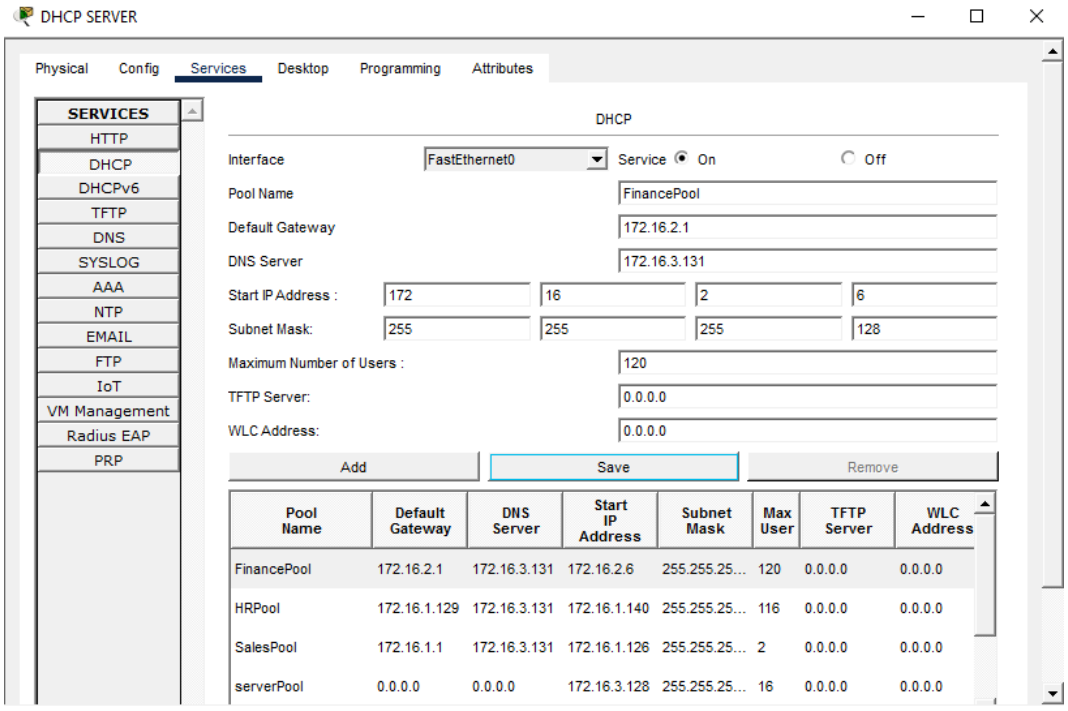


Fig: 8.4 DHCP Server Configuration for Finance

8.5 DHCP Server Configuration for Admin

Pool name Admin Pool

Defult gateway 172.16.1.129

DNS Server: 172.16.3.131

Start IP Address:172.16.1.131

Subnet Mask:255.255.255.128

Maximum number of Users: 120

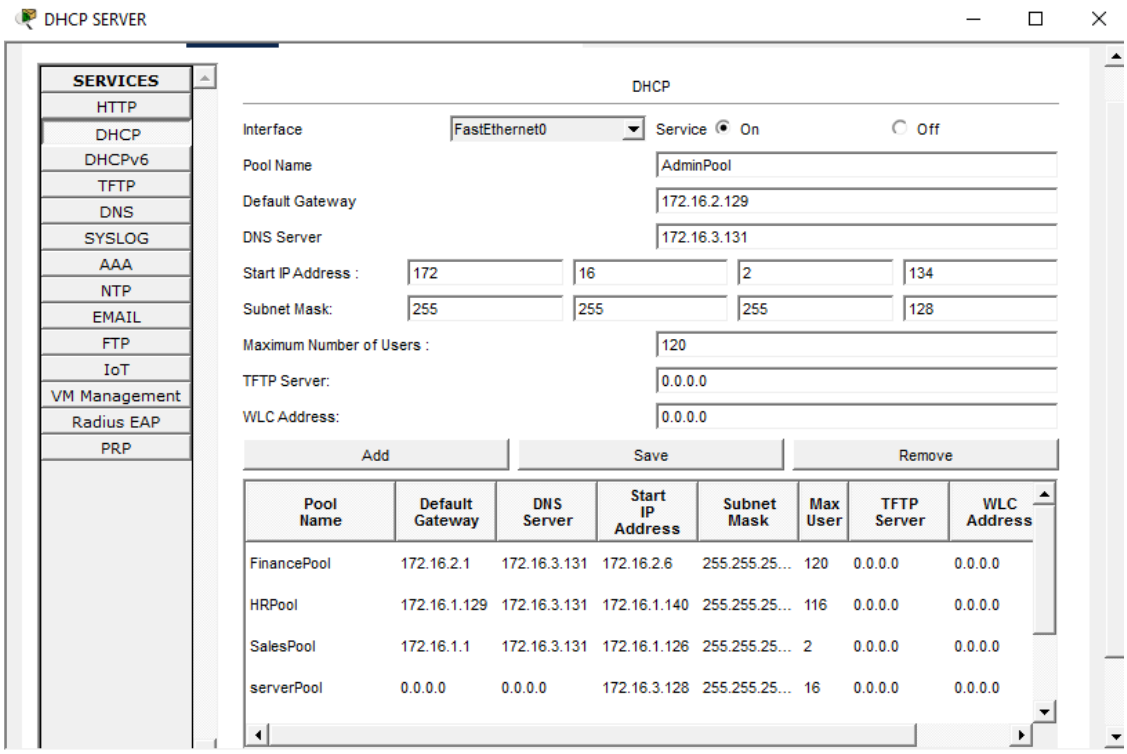


Fig 8.5 DHCP Server Configuration for Admin

8.6 DHCP Server Configuration for ICT

Pool name ICT Pool

Defult gateway 172.16.1.129

DNS Server: 172.16.3.1

Start IP Address: 172.16.3.6

Subnet Mask: 255.255.255.128

Maximum number of Users: 120

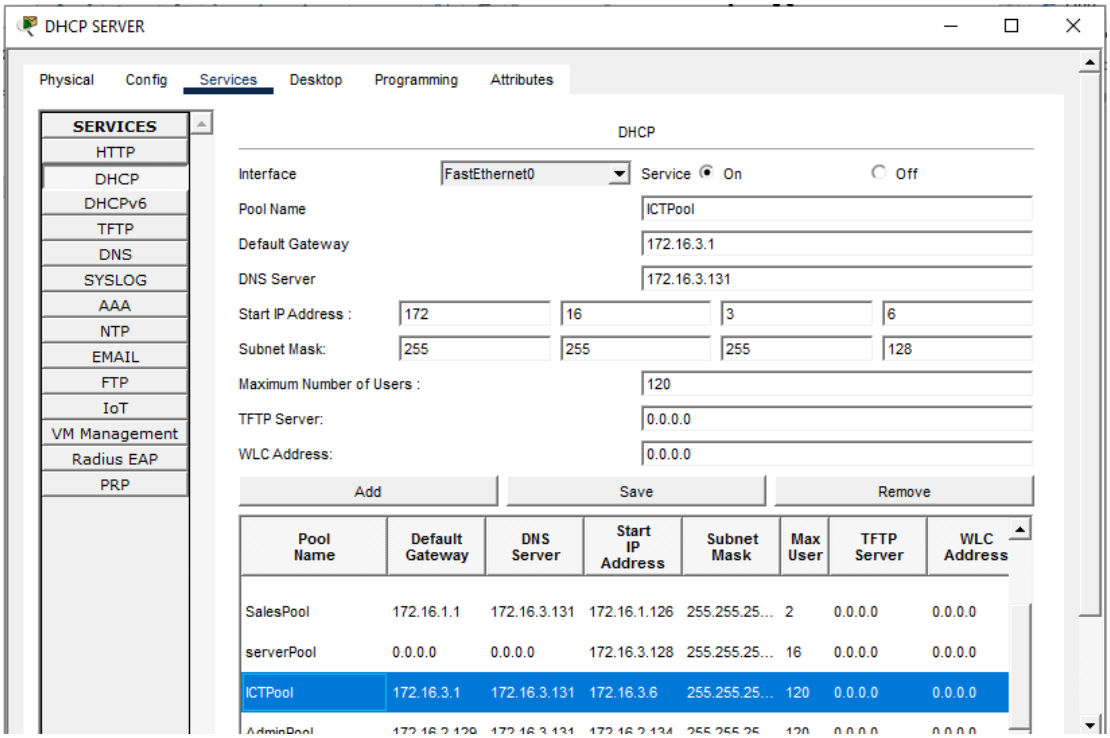


Fig 8.6 DHCP Server Configuration for ICT

8.7 DNS Server Configuration Static IP

To configure the DNS Server, first open the DNS Server device and go to the Desktop tab. Then select IP Configuration and assign a static IP address.

The following IP configuration is used:

IP Address 172.16.3.130

Default Gateway 172.16.3.129

DNS Server 172.16.3.131

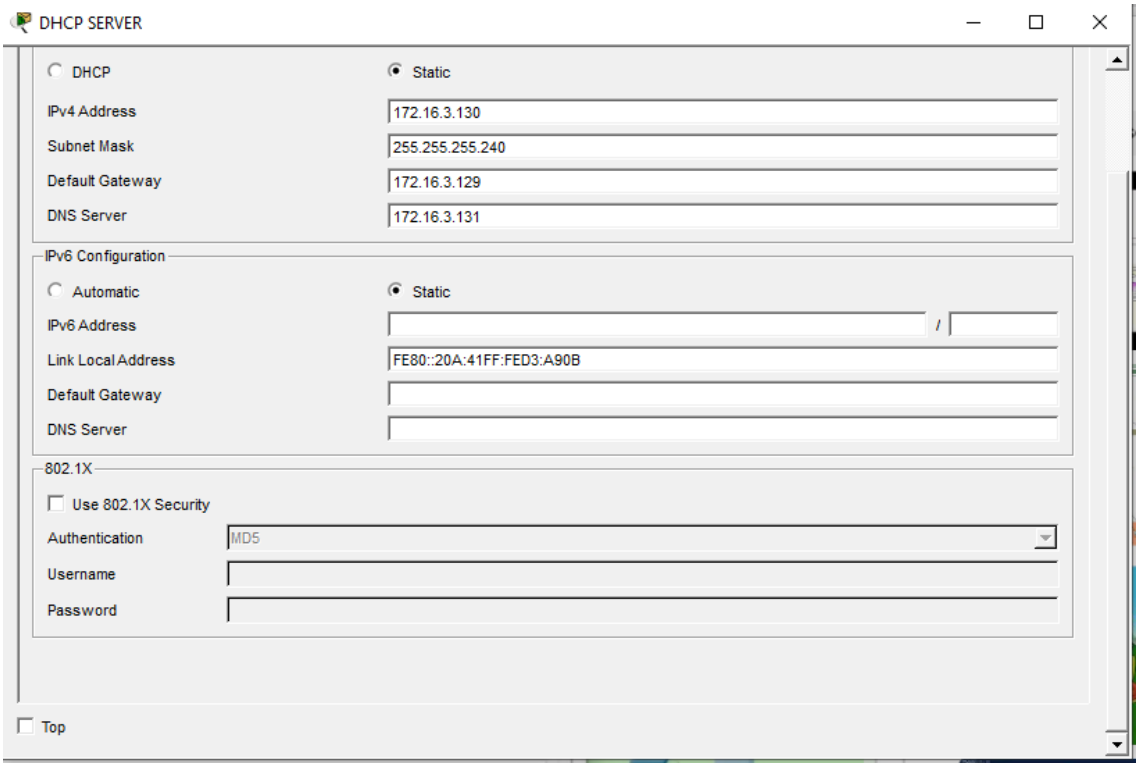


Fig 8.8 DNS Server Configuration

8.8 DNS Server Configuration

IP: 172.16.3.131

Name: www.Gtech.com

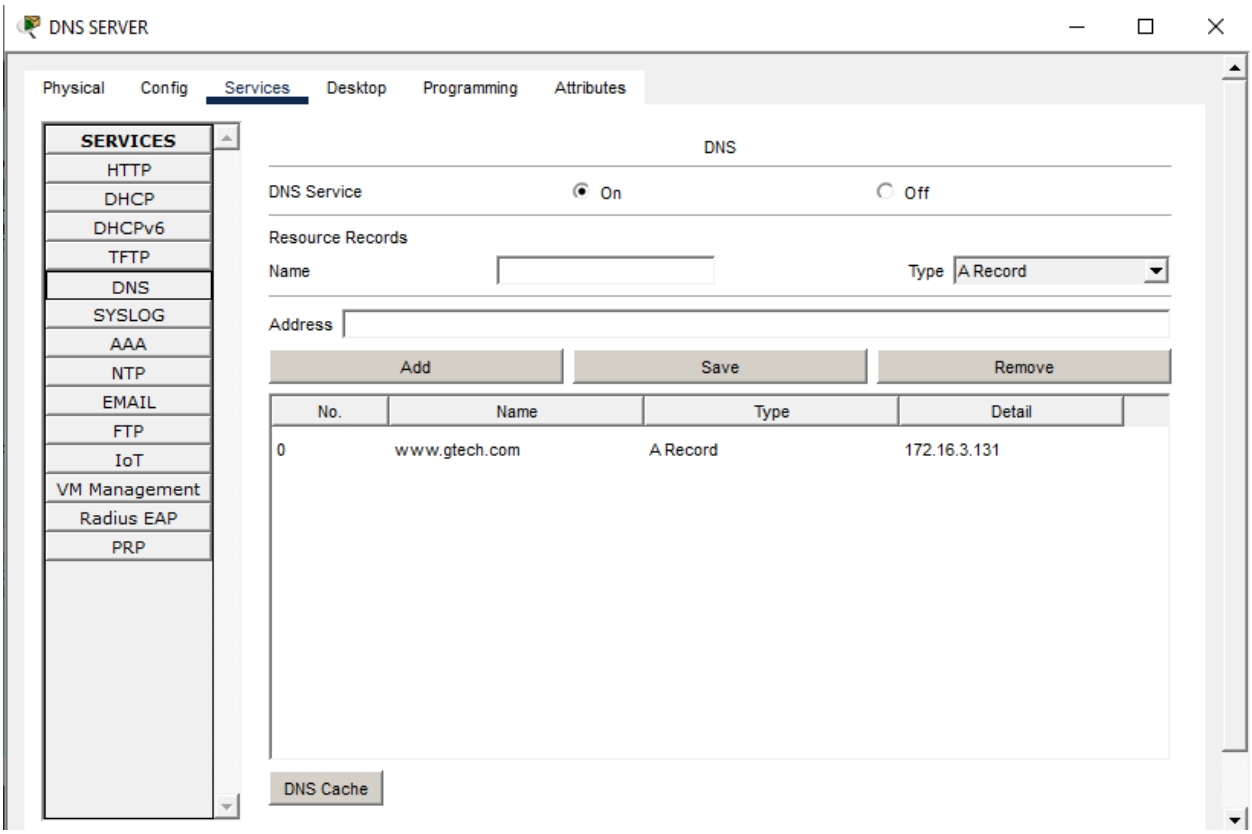


Fig 8.8 DNS Server Configuration

REFERENCES

[1] Cisco Networking Academy, *Cisco CCNA: Introduction to Networks*, Cisco Systems.

[2] Cisco Systems, *Cisco IOS Command Reference*, Cisco Documentation.

[3] Cisco Systems, *Cisco Packet Tracer – Network Simulation Tool*, Cisco Networking Academy.

[4] Andrew S. Tanenbaum and David J. Wetherall, *Computer Networks*, 5th Edition, Pearson

[5] Behrouz A.Forozan,Data Comminutions and Networking,5th Edition, McGraw-Hill.

[6] James F. Kurose and Keith W. Ross, *Computer Networking A Top-Down Approach*.

[7] RFC 1918, *Address Allocation for Private Internets*, Internet Engineering Task Force (IETF)..

[8] T. RFC 2328, *OSPF Version 2*, Internet Engineering Task Force (IETF)