Design and Implementation of a Redundant Three-Tier Campus Network with Dual ISP Connectivity

by

MD. Al Amin
ID: CSE2103024065

MD. Rayhan Uddin
ID: CSE2203027058

Razzak Miazee
ID: CSE2203027109

MD. Sohel Rana
ID: CSE22026042

Supervised by
Tanjil Mahmud

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)
May 2026

APPROVAL

This project titled **"Design and Implementation of a Redundant Three-Tier Campus Network with Dual ISP Connectivity"** submitted by MD. Rayhan Uddin (CSE2203027058), Razzak Miazee (CSE2203027109), MD. Sohel Rana (CSE22026042) and MD. Al Amin (CSE2103024065) 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

Tanjil Mahmud — **Supervisor**
Lecturer,
Department of Computer Science and Engineering
Sonargaon University (SU)

(Examiner Name and Signature) — **Examiner 1**
Department of Computer Science and Engineering
Sonargaon University (SU)

(Examiner Name and Signature) — **Examiner 2**
Department of Computer Science and Engineering
Sonargaon University (SU)

(Examiner Name and Signature) — **Examiner 3**
Department of Computer Science and Engineering
Sonargaon University (SU)

DECLARATION

We, hereby, declare that the work presented in this report is the outcome of the investigation performed by us under the supervision of **Tanjil Mahmud, Lecturer** 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

(**Tanjil Mahmud)**
Supervisor

Signature

MD. Al Amin
ID: CSE2103024065)

MD. Rayhan Uddin
ID: CSE2203027058

Razzak Miazee
ID: CSE2203027109

MD. Sohel Rana
ID: CSE2103024065

ABSTRACT

Modern campus networks often face issues such as single points of failure, limited scalability, and inefficient traffic handling, especially when relying on a single ISP or non-hierarchical design. These limitations can lead to service disruption and reduced network performance in real-world environments. This project presents the design and implementation of a redundant three-tier campus smart network with dual ISP connectivity using Cisco Packet Tracer. The architecture follows core, distribution, and access layers, where redundancy is ensured at each level through dual core routers and multilayer switches. Dual ISP connections are configured using OSPF with cost-based path selection to enable automatic failover between primary and secondary links The implementation includes VLAN configuration on access switches to segment student and staff networks, along with inter-VLAN routing using multilayer switches and HSRP for gateway redundancy. Dynamic routing with OSPF ensures efficient communication [9], while centralized wireless access is managed using a WLC and APs. Additionally, services like DHCP, DNS, and email servers are integrated, and ACLs are applied to control inter-VLAN access. During the simulation, challenges such as OSPF neighbor formation, VLAN trunking, and failover stability were encountered and resolved through testing. Failover was verified by shutting down the primary ISP link, where traffic successfully rerouted through the backup link without interruption. The results show that the proposed design provides high availability, better traffic management [9], and improved security, making it suitable for real-world campus network deployment.

ACKNOWLEDGMENT

At the very beginning, we would like to express my deepest gratitude to the Almighty Allah for giving us the ability and the strength to finish the task successfully within the schedule time. We are auspicious that we had the kind association as well as supervision of **Tanjil Mahmud**, Lecturer of Computer Science and Engineering, Sonargaon University whose hearted and valuable support with best concern and direction acted as necessary recourse to carry out our project. We are also thankful to all our teachers during our whole education, for exposing us to the beauty of learning. Finally, our deepest gratitude and love to my parents for their support, encouragement, and endless love.

LIST OF ABBREVIATIONS

ACL	Access Control List
AP	Access Point
CDP	Cisco Discovery Protocol
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
GUI	Graphical User Interface
HSRP	Hot Standby Router Protocol
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IP	Internet Protocol
ISP	Internet Service Provider
LAN	Local Area Network
MAC	Media Access Control
MLS	Multilayer Switch
OSPF	Open Shortest Path First
POP3	Post Office Protocol Version 3
PVST	Per VLAN Spanning Tree
SMTP	Simple Mail Transfer Protocol
STP	Spanning Tree Protocol
SVI	Switched Virtual Interface
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
WAN	Wide Area Network
WLC	Wireless LAN Controller

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Chapter 1

INTRODUCTION

1.1 Background of the Project

In modern educational institutions, campus networks are essential for supporting academic and administrative activities [1]. Students, faculty, and staff rely on stable network connectivity for online classes, research, and internal services [1]. However, many traditional campus networks depend on a single ISP and lack proper redundancy, which can lead to complete network failure if the main link goes down. Such limitations create problems like service disruption, poor performance, and security risks. These issues show the need for a more reliable and structured network design that can ensure continuous connectivity and better traffic management [2]. To solve this, this project designs a redundant three-tier smart campus network using Cisco Packet Tracer. The network is divided into core, distribution, and access layers for better scalability and control [2]. VLANs are used to separate student and staff networks, while OSPF is implemented for dynamic routing with dual ISP failover [1]. HSRP is sed for gateway redundancy, and a centralized wireless system is managed using WLC and access points. This design reflects a practical and reliable solution that can maintain network performance even during failures [8].

1.2 Problem Statement

In many campus environments, network infrastructure is often designed without proper redundancy and relies on a single ISP connection. This creates a major risk, as any failure in the primary link can cause complete network downtime, affecting academic activities, communication, and access to essential services. During practical observation, it is clear that such designs cannot ensure continuous connectivity in real-world scenarios [8]. Another common issue is the lack of proper network segmentation. Without VLAN implementation, all users share the same network, which leads to unnecessary traffic, reduced performance, and increased security risks. For example, student and staff networks are not isolated, making it difficult to control access and protect sensitive data. Additionally, absence of dynamic routing protocols results in inefficient traffic flow and slow recovery during failures. To overcome these limitations, there is a need for a structured and fault-tolerant network design that ensures high availability [8], efficient traffic management, and secure communication. This project addresses these problems by implementing a three-tier architecture with VLAN segmentation, OSPF-based routing, dual ISP connectivity, and redundancy mechanisms such as HSRP, ensuring reliable and uninterrupted network operation

1.3 Objectives of the Project

The main objective of this project is to design and implement a reliable and scalable smart campus network using a three-tier architecture. The project aims to ensure uninterrupted network services by integrating dual ISP connections with primary and backup links. It also focuses on implementing redundancy at different layers, including core routers and multilayer switches, to minimize network downtime. Another key objective is to segment the network using VLANs for better management and security. The project also intends to deploy a

centralized wireless system using WLC and access points, allowing separate network access for staff and students. Additionally, services such as DHCP, DNS, and email servers are configured to simulate a real-world enterprise environment, along with ACLs to enhance network security.

1.4 Scope of the Project

This project focuses on the design and simulation of a smart campus network using Cisco Packet Tracer, based on a three-tier architecture. The scope includes the implementation of core, distribution, and access layers to ensure a structured and scalable network design. VLAN segmentation is applied to separate different user groups such as students and staff, improving network performance and security. Dynamic routing is configured using OSPF, along with dual ISP connectivity to provide automatic failover in case of link failure. Gateway redundancy is ensured using HSRP, and centralized wireless access is implemented through a WLC and multiple access points. In addition, essential network services such as DHCP, DNS, and email servers are configured, along with ACLs to control traffic between VLANs. However, this project is limited to simulation only and does not include real hardware deployment, physical infrastructure costs, or advanced enterprise-level security mechanisms.

1.5 Significance of the Project

This project is important because it shows how a reliable and scalable campus network can be designed using a structured three-tier architecture. In many real environments, networks suffer from downtime due to lack of redundancy and poor planning. By implementing dual ISP connectivity with OSPF-based failover, this project ensures continuous connectivity even when a primary link fails. The use of VLAN segmentation improves performance and security by separating student and staff networks, reducing unnecessary traffic and unauthorized access. In addition, HSRP provides gateway redundancy, while centralized wireless management using WLC and access points ensures efficient campus-wide Wi-Fi connectivity. This project also has practical value for learners, as it is implemented in Cisco Packet Tracer and reflects real-world networking scenarios, making it a useful reference for understanding modern campus network design.

1.6 Organization of the Project

This project is organized in a structured way where each chapter focuses on a specific part of the network design and its implementation. Chapter 1 introduces the project, including background, problem statement, objectives, and scope. Chapter 2 discusses the fundamental networking concepts such as hierarchical design, segmentation, routing, and redundancy techniques that are used in this work. Chapter 3 presents the proposed network architecture, including layer-based design, IP addressing, VLAN segmentation, and dual ISP connectivity [5]. Chapter 4 explains the implementation in Cisco Packet Tracer, where routers, multilayer switches, access switches, wireless components, and servers are configured based on the design. Chapter 5 focuses on testing, including connectivity checks, inter-VLAN communication, and ISP failover verification. Chapter 6 analyzes the results in terms of performance, reliability, and security. Finally, Chapter 7 concludes the project and suggests possible improvements for future work.

Chapter 2

LITERATURE REVIEW

2.1 Overview of Campus Network Design

Campus network design refers to the structured planning of network infrastructure within an institution to support communication, data sharing, and service delivery. In modern environments, a well-designed campus network must handle a large number of users while maintaining performance, security, and reliability. Instead of using a flat design, most organizations now prefer hierarchical models because they provide better control and scalability [2]. In this project, a layered approach is followed to organize the network efficiently [1][2]. By separating functions across different layers and applying techniques such as VLAN segmentation and centralized management, the network becomes easier to manage and more stable during operation. This approach reflects how real campus networks are designed to support both wired and wireless users [1].

2.2 Three-Tier Network Architecture

The three-tier architecture is widely used in campus networks because it divides the network into core, distribution, and access layers [2][4], each with a specific role. The core layer is responsible for high-speed data forwarding and connects major parts of the network. The distribution layer acts as a control point, handling routing, policies, and redundancy mechanisms. The access layer provides connectivity to end devices such as PCs, laptops, and access points.
While implementing this model in Cisco Packet Tracer, it helped in organizing devices logically and improving overall performance [4]. Each layer was configured separately, which made troubleshooting easier and ensured that failures in one layer did not affect the entire network.

2.3 Dual ISP and Redundancy Concepts

Redundancy is a key requirement in modern networks to ensure continuous operation during failures [5]. Without backup paths or devices, a single failure can bring down the entire system. In this project, redundancy is achieved by using dual core routers, dual multilayer switches, and dual ISP connections [5]. During testing, failover scenarios were simulated by disabling primary links, and the network successfully switched to backup paths [6]. This confirms that redundancy mechanisms such as multiple links and gateway backup can significantly improve network reliability and availability [5].

2.4 Dynamic Routing Protocols (OSPF)

Dynamic routing protocols are used to automatically manage network paths and update routing information. OSPF is one of the most commonly used protocols in enterprise networks due to its fast convergence and efficient path selection [10]. It uses cost values to determine the best route between networks. In this project, OSPF is configured across routers and multilayer switches to enable communication between different segments. Dual ISP connectivity is also

managed using OSPF by assigning different costs, which allows automatic switching between primary and backup links [6]. During implementation, proper neighbor relationships and network statements were essential to ensure stable routing.

2.5 VLAN and Network Segmentation

VLANs are used to divide a physical network into multiple logical networks, improving both performance and security [12]. By separating user groups such as students and staff into different VLANs, unnecessary traffic is reduced and access control becomes easier. In the simulation, VLANs are configured on access switches and extended through trunk links to multilayer switches . Inter-VLAN communication is enabled through routing, allowing controlled interaction between different segments. This setup reflects practical network design where segmentation plays an important role in managing large environments.

2.6 Wireless Network Management (WLC & AP)

Wireless connectivity is an essential part of modern campus networks [9], as users rely heavily on mobile devices. Managing multiple access points individually can be complex, which is why centralized control using a Wireless LAN Controller is preferred. In this project, a WLC is used to manage multiple access points, providing a unified configuration for wireless networks. Separate wireless access is maintained for different user groups, ensuring better control and organization. Although implemented in a simulated environment, it demonstrates how centralized wireless systems simplify network management.

2.7 Summary of Existing Works

Existing studies and designs show that combining hierarchical architecture with redundancy and dynamic routing improves network performance and reliability. Techniques such as VLAN segmentation, OSPF routing, and centralized wireless management are commonly used in real-world campus networks. Based on these concepts, this project integrates multiple technologies into a single design to create a stable and efficient network system. The implementation in Cisco Packet Tracer reflects practical understanding and provides a foundation for further development in real environments.

Chapter 3

SYSTEM DESIGN AND METHODOLOGY

3.1 Proposed Network Architecture

The proposed network is designed using a hierarchical three-tier model to ensure scalability, performance, and easier management. The architecture separates the network into core, distribution, and access layers, where each layer performs a specific role [2]. Dual ISP connectivity is integrated into the design to avoid dependency on a single external connection, improving availability. In Cisco Packet Tracer, this structure helped organize devices clearly and allowed better control during configuration and testing. The overall design focuses on maintaining continuous connectivity and reducing the risk of complete network failure.

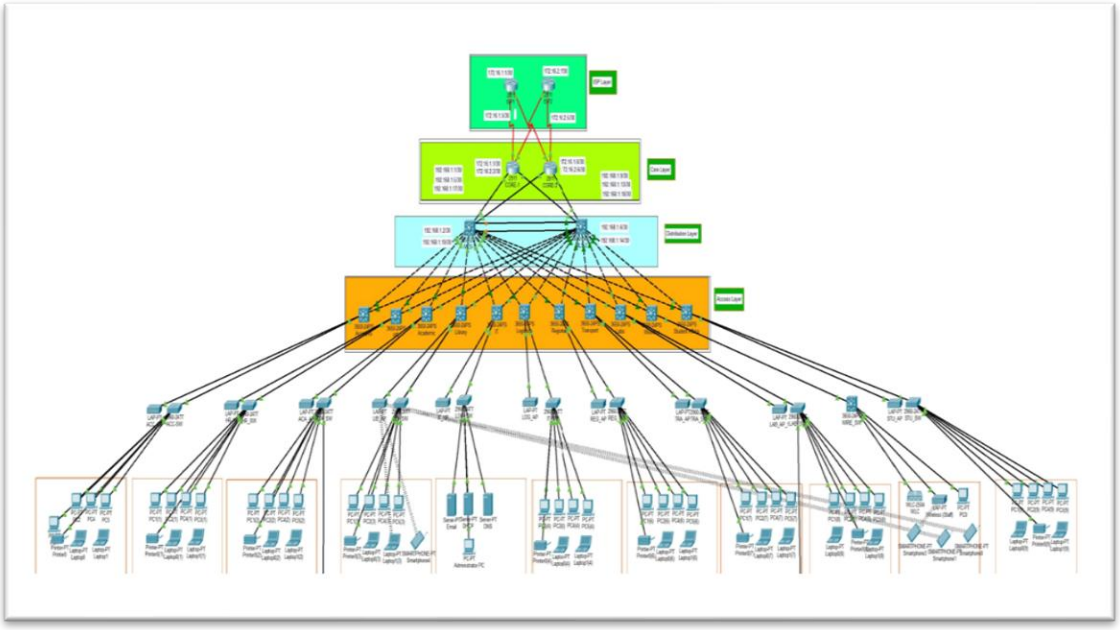

Fig 3.1 Overall, Three-Tier Network Architecture Diagram

Network Model	Hierarchical Three-Tier Architecture (Core, Distribution, Access)
ISP Connectivity	Dual ISP (ISP-1 & ISP-2) with Primary/Secondary redundancy
Core Layer	Dual Core Routers for high-speed routing and ISP gateway management
Distribution Layer	Dual Multilayer Switches (L3) with HSRP for gateway redundancy
Access Layer	Layer 2 Switches with VLAN segmentation for end-user connectivity
Routing Protocol	OSPF (Open Shortest Path First) for dynamic internal routing
Redundancy Protocols	HSRP (Hot Standby Router Protocol) and Redundant Physical Links
Wireless Architecture	Centralized WLC (Wireless LAN Controller) with Lightweight APs

VLAN Segmentation	Separate VLANs for Students, Staff, Servers, and Management
Security Mechanism	Standard and Extended ACLs for Inter-VLAN traffic control
Network Services	Dedicated Servers for DHCP, DNS, and Email
Simulation Tool	Cisco Packet Tracer

Table 3.1 Overall Network Architecture Summary

3.2.1 Core Layer Design

The core layer acts as the backbone of the network, responsible for high-speed data transmission between different parts of the system. In this project, dual core routers are used to provide redundancy and ensure continuous operation [5]. These routers are connected to both ISPs and distribution switches, allowing multiple paths for data flow. OSPF is configured to manage routing decisions, where cost values help determine the primary and backup paths. This setup ensures that even if one link fails, communication can continue without interruption.

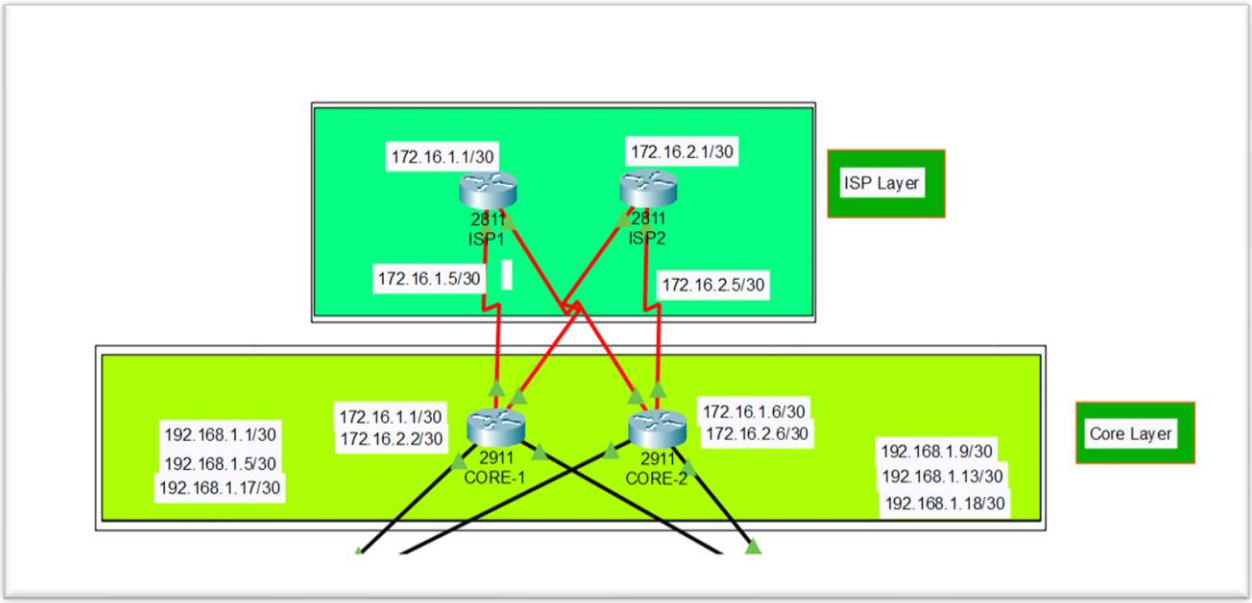

Fig 3.2 Core Layer Design Topology

3.2.2 Distribution Layer Design

The distribution layer connects the core layer with the access layer and plays a key role in routing and policy control. Multilayer switches are used in this layer to handle inter-VLAN routing and apply configurations such as ACLs and HSRP. Gateway redundancy is implemented so that if one switch fails, the other can take over without affecting users. VLAN traffic is aggregated here before being forwarded to the core layer. This layer also helps maintain network performance by controlling traffic flow between different segments.

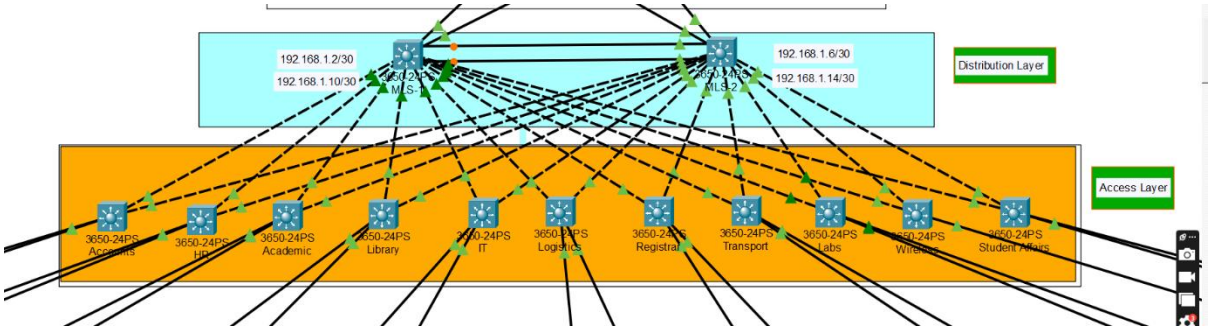

Fig 3.3 Distribution Layer (Multilayer Switch) Design

3.2.3 Access Layer Design

The access layer is the part of the network where end users directly connect, so it plays a key role in overall user experience. In this project, access switches are used to connect devices such as PCs, laptops, and wireless access points. Each port on the access switch is assigned to a specific VLAN based on the user group, like students or staff, which helps keep traffic organized and secure. Supporting switches are also added under the main access switches to extend connectivity to different departments. During the implementation in Cisco Packet Tracer, proper port configuration and VLAN assignment were important to avoid connectivity issues. Trunk links were set up between access and distribution switches to carry multiple VLANs across the network [12]. One challenge faced was incorrect VLAN mapping, which caused communication problems, but it was resolved through testing and verification. Overall, this layer ensures that users can access network resources smoothly while maintaining separation between different network

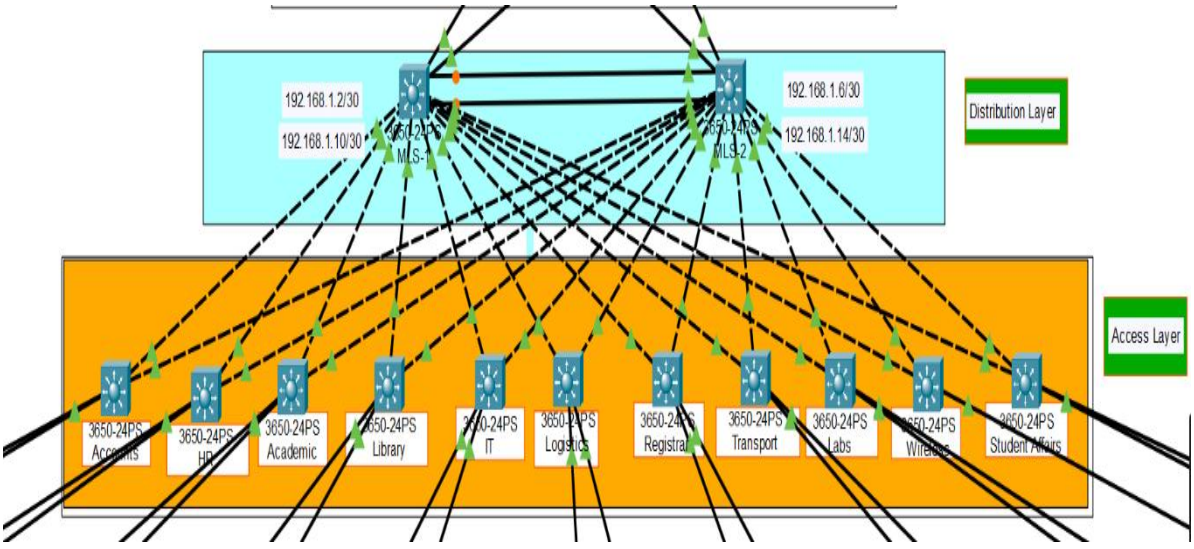

Fig 3.4 Access Layer Connectivity Diagram

3.3 Dual ISP Connectivity Design

Dual ISP connectivity is implemented to provide backup internet access and avoid complete network downtime. Two ISP routers are connected to the core routers, creating multiple paths for external communication. OSPF is used to assign different costs to each link, allowing one path to act as primary and the other as secondary. During testing, when the primary link was disabled, traffic automatically shifted to the backup link without disruption. This design improves reliability and reflects real-world enterprise network practices.

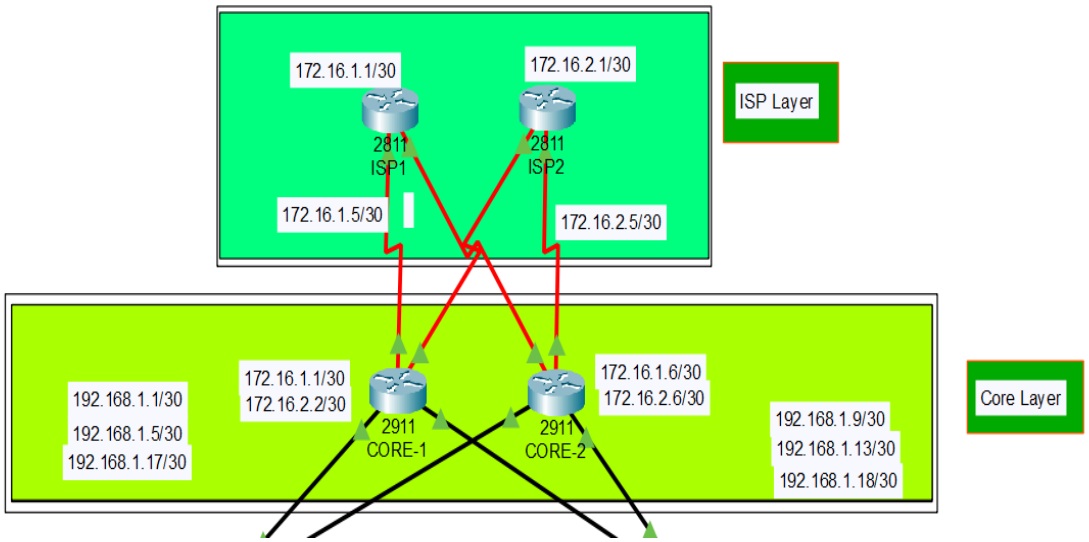

Fig 3.5 Dual ISP Connectivity Design

3.4 IP Addressing Scheme

An organized IP addressing scheme is used to manage different network segments efficiently. Each VLAN is assigned a unique IP range, making it easier to identify and manage traffic. Subnetting is applied to divide the network logically while maintaining proper address utilization. Gateway addresses are configured using HSRP to ensure redundancy. This structured approach simplifies troubleshooting and supports future expansion of the network without major changes.

Network Segment	VLAN ID	Subnet / IP Range	Subnet Mask	Default Gateway
Server Farm (DHCP, DNS, Email)	50	10.50.0.0/16	255.255.0.0	10.50.0.1
Management (WLC & APs)	100	10.100.0.0/16	255.255.0.0	10.100.0.1
Academic	30	10.30.0.0/16	255.255.0.0	10.30.0.1
Lab	80	10.80.0.0/16	255.255.0.0	10.80.0.1
Library	40	10.40.0.0/16	255.255.0.0	10.40.0.1
Core to Dist. Interconnect	N/A	192.168.1.0/30	255.255.255.252	Point-to-Point

Table 3.2 IP Addressing Scheme

3.5 VLAN Design and Segmentation

VLAN segmentation is used to divide the network into smaller logical groups, improving both performance and security. Different VLANs are created for students, staff, and other departments, ensuring that traffic is properly isolated. Trunk links are configured between switches to carry multiple VLANs across the network. Inter-VLAN communication is controlled through multilayer switches [12], allowing selective access between groups. This design reduces broadcast traffic and enhances overall network efficiency.

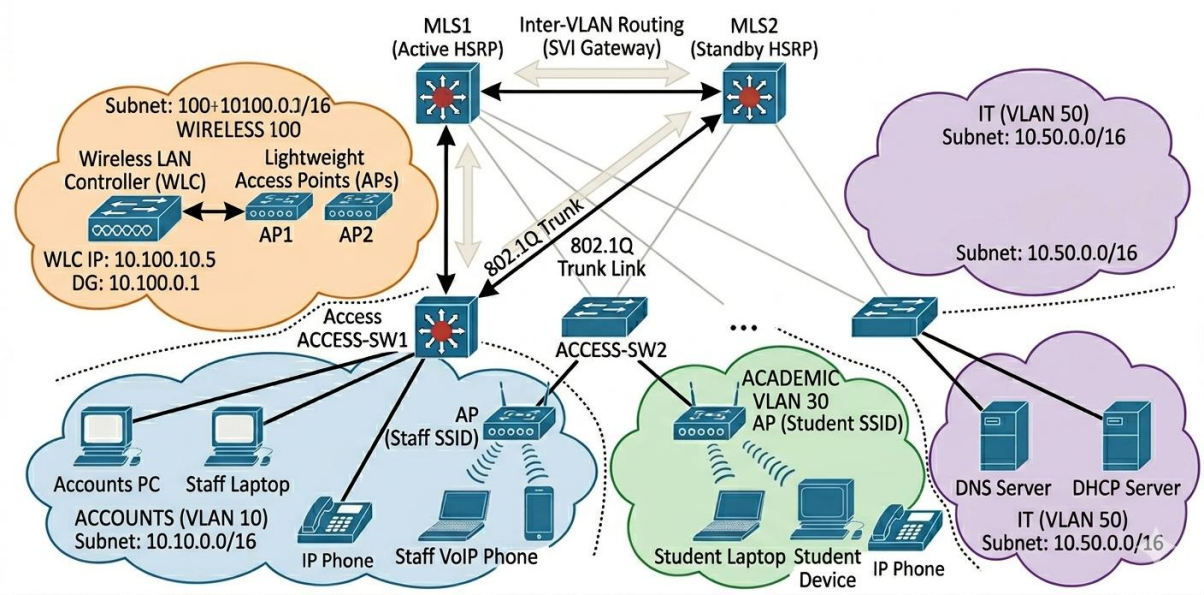

Fig 3.6 VLAN Design and Segmentation

VLAN ID	Name	Purpose / Department	Subnet Range
10	ACCOUNTS	Accounts Department	10.10.0.0/16
20	HR	Human Resource (HR)	10.20.0.0/16
30	ACADEMIC	Academic Department	10.30.0.0/16
40	LIBRARY	University Library	10.40.0.0/16
50	IT	IT Support & Services	10.50.0.0/16
60	LOGISTICS	Logistics Department	10.60.0.0/16
70	REGISTRAR	Registrar Office	10.70.0.0/16
80	TRANSPORT	Transport Department	10.80.0.0/16
90	STUDENT_AFFAIRS	Student Affairs Office	10.90.0.0/16
99	LABS	Computer/Science Labs	10.99.0.0/16
100	WIRELESS	WLC, AP and WiFi Management	10.100.0.0/16

Table 3.3 VLAN ID and Department Mapping

3.6 Routing Design using OSPF

OSPF is used as the dynamic routing protocol to manage communication between different parts of the network. It allows routers and switches to share routing information automatically and select the best path based on cost. In this project, OSPF is configured across core routers and multilayer switches to ensure full connectivity. Proper network statements and neighbor relationships were necessary to maintain stable routing. This approach ensures fast convergence and efficient data flow [10].

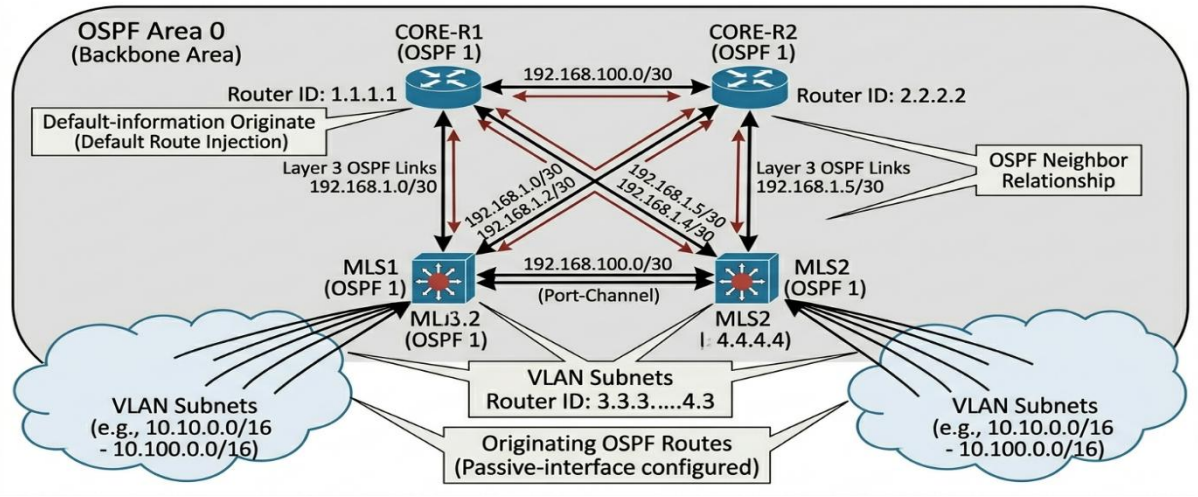

Fig: 3.7 OSPF Routing Topology

VLAN ID	Name	Purpose / Department	Gateway
10	ACCOUNTS	Accounts Department	10.10.0.1
20	HR	Human Resource (HR)	10.20.0.1
30	ACADEMIC	Academic Department	10.30.0.116
40	LIBRARY	University Library	10.40.0.0/16
50	IT	IT Support & Services	10.50.0.0/16
60	LOGISTICS	Logistics Department	10.60.0.0/16
70	REGISTRAR	Registrar Office	10.70.0.0/16
80	TRANSPORT	Transport Department	10.80.0.0/16
90	STUDENT_AFFAIRS	Student Affairs Office	10.90.0.0/16
99	LABS	Computer/Science Labs	10.99.0.0/16
100	WIRELESS	WLC, AP and WiFi Management	10.100.0.0/16

Table 3.4 Routing Design using OSPF

3.7 Redundancy Mechanisms (HSRP, Dual Links)

Redundancy is implemented at multiple levels to ensure continuous network operation. HSRP is used to provide gateway backup [3], allowing one device to take over if another fails. Dual links are established between critical devices to create alternative paths for data transmission. These mechanisms reduce the risk of downtime and improve network reliability [11]. During

simulation, failover scenarios were tested to confirm that backup systems function correctly [6].

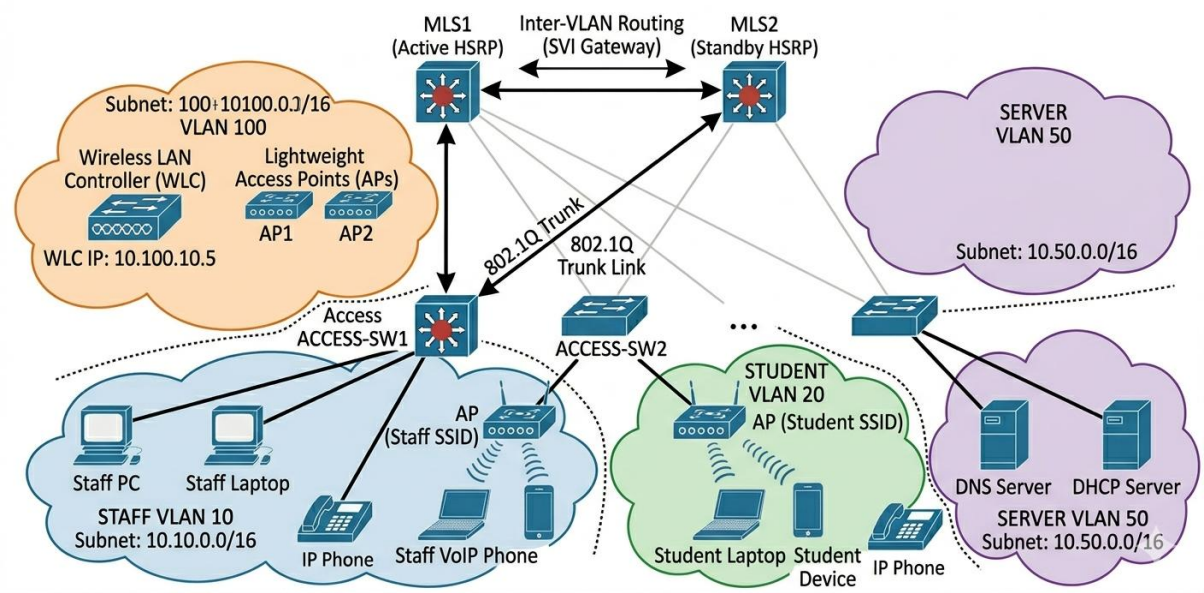

Fig: 3.8 HSRP Redundancy Model

Redundancy Level	Mechanism / Protocol	Description
ISP Redundancy	Dual Multihoming	Connected to two different ISPs to ensure internet availability if one ISP fails.
ISP Link Failover	Floating Static Routes / IP SLA	Primary and Secondary paths configured for automatic traffic switchover.
Core Layer Redundancy	Dual Core Routers	Two high-end routers working in tandem to prevent a single point of failure at the gateway.
Gateway Redundancy	HSRP (Hot Standby Router Protocol)	Provides a Virtual IP (VIP) at the Distribution layer for seamless client failover.
Link Redundancy	Dual-Homing Links	Every Access Switch is connected to both Multilayer Switches via redundant fiber/ethernet links.
Path Redundancy	OSPF (Open Shortest Path First)	Dynamic routing protocol that recalculates the best path automatically if a link goes down.
Device Redundancy	Dual Power Supplies / Hardware Redundancy	Using twin Multilayer switches to handle Inter-VLAN routing and Core connectivity.

Table 3.5 Redundancy Mechanisms and Protocols (HSRP, Dual ISP)

3.8 Wireless Network Design (WLC & AP)

Wireless connectivity is integrated into the network using a centralized management approach. A Wireless LAN Controller is used to manage multiple access points, simplifying configuration and control. Separate wireless networks are created for different user groups, ensuring organized access. This design supports mobile users and provides flexibility in network access. Even in simulation, it demonstrates how centralized wireless systems improve management efficiency.

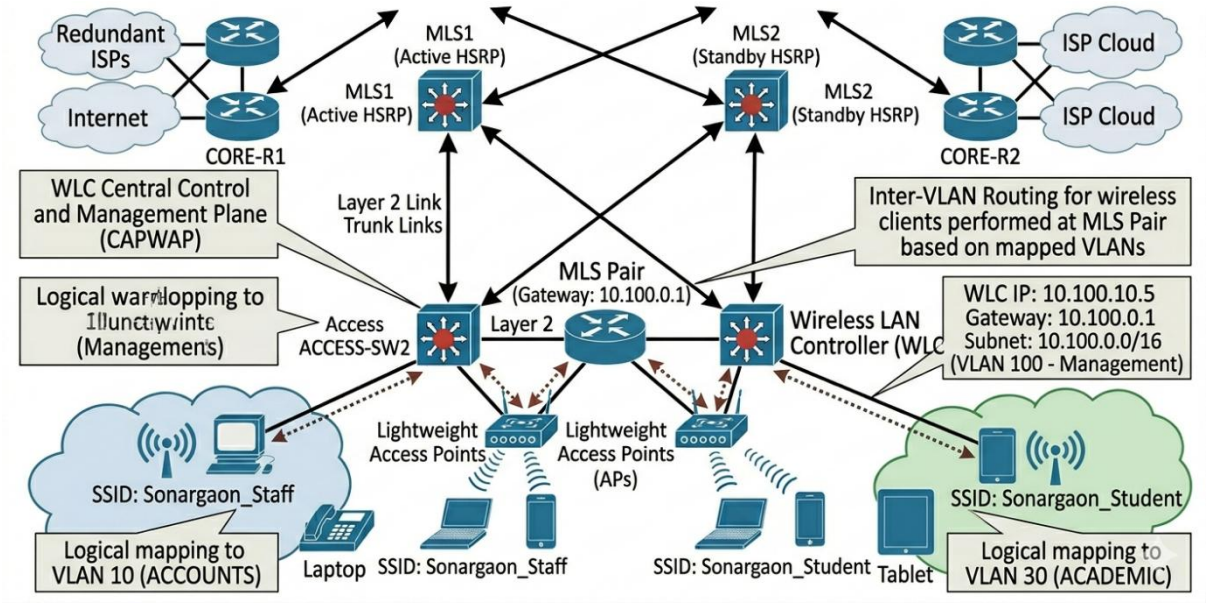

Fig 3.9 Wireless Network Design (WLC & AP)

Parameter	**Specification / Details**
Wireless Architecture	Centralized (WLC-based) Architecture
WLC Model	Cisco 2504 / 3504 Wireless LAN Controller (Simulated)
Management IP (WLC)	10.100.10.5
Subnet Mask / Gateway	255.255.0.0 / 10.100.0.1
Control VLAN	VLAN 100 (Management VLAN)
Access Point Mode	Lightweight Access Points (LAP)
SSID 1 (Staff)	Staff_WiFi (Mapped to VLAN 100)
SSID 2 (Student)	Student_WiFi (Mapped to VLAN 100)
Security Protocol	WPA2-PSK (AES Encryption)
WLC Interface	GigabitEthernet 0/0/23 & 0/0/24 (Trunked to Multilayer Switch)
AP Connectivity	Connected to Access Switches via Trunk/Access Ports

Table 3.9 Wireless Network Configuration (WLC & AP Details)

3.9 Security Design using ACL

Access Control Lists are used to enforce security policies within the network. ACLs are applied to control traffic between different VLANs, preventing unauthorized access. Specific rules are defined to allow or deny communication based on requirements. This helps protect sensitive data and ensures that only authorized users can access certain resources. The implementation reflects practical security measures used in real network environments. Trunk links are configured between switches to allow multiple VLANs to pass through a single connection, making the network more efficient.

ACL ID / Name	**Source Network**	**Destination Network / Host**	**Protocol / Port**	**Action**	**Purpose**
ACL 101	10.30.0.0/16 (Academic)	10.50.10.12 (Email Server)	IP	Permit	Allow Academic users to access Email services.
ACL 101	10.30.0.0/16 (Academic)	10.50.10.11 (DNS Server)	IP	Permit	Allow Academic users to perform DNS queries.
ACL 102	10.30.0.0/16 (Academic)	10.10.0.0/16 (Accounts)	IP	Deny	Block Academic VLAN from accessing Accounts department data.
Standard ACL	10.100.0.0/16 (Wireless Mgmt)	Any	Management	Permit	Allow administrative access to WLC and APs.
Implicit Deny	Any	Any	IP	Deny	Block all other traffic not explicitly permitted (Default behavior).

Table 3.7 ACL Rules and Security Policies

.

Chapter 4

IMPLEMENTATION AND CONFIGURATION

4.1 Simulation Environment (Cisco Packet Tracer)

The implementation of this project is carried out using Cisco Packet Tracer, which provides a virtual platform to design, configure, and test network topologies. This environment allows different network devices such as routers, multilayer switches, access switches, servers, and wireless components to be connected in a structured way. During the setup, all devices were placed according to the three-tier architecture, ensuring proper alignment with the proposed design. The simulation made it possible to test real-life scenarios like connectivity checks and link failures without using physical hardware. One of the main advantages observed was the ability to visualize traffic flow and quickly identify configuration errors. Although it does not fully represent hardware-level performance, it still provides a reliable platform for understanding network behavior and validating the overall design before real-world deployment.

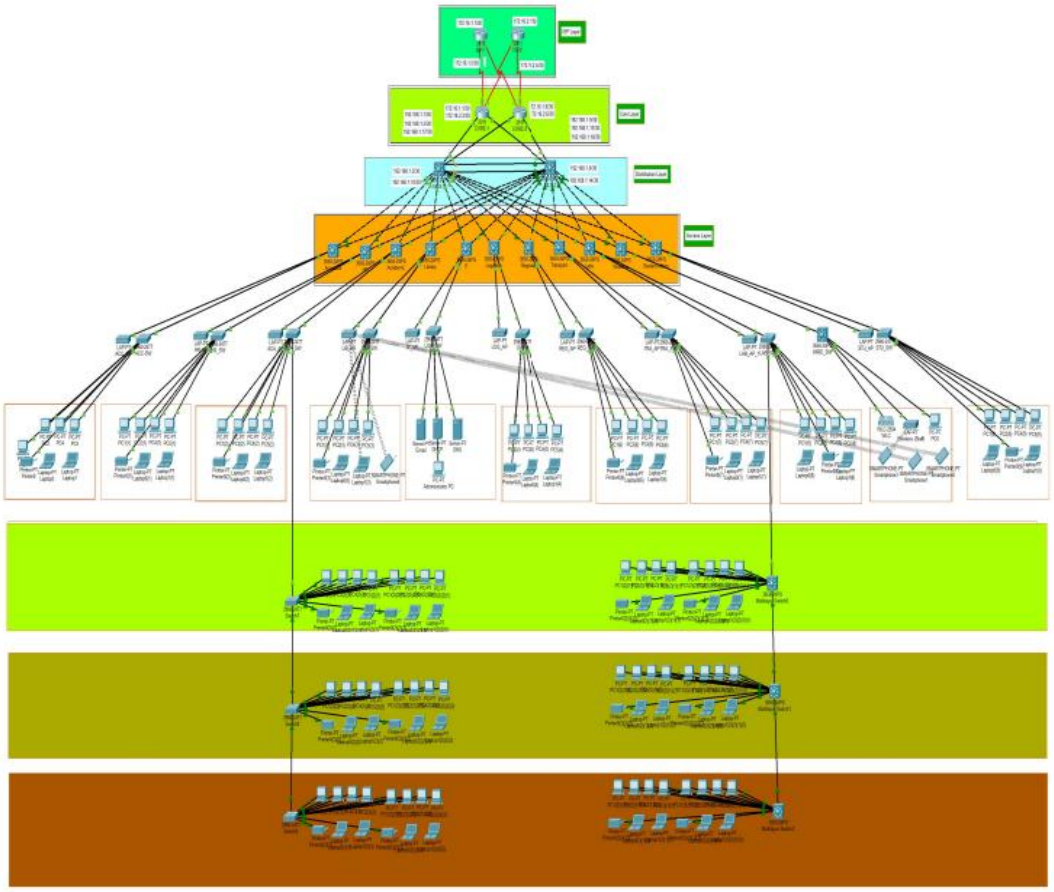

Fig 4.1: Cisco Packet Tracer Full Topology Screenshot

4.2 Device Configuration

The configuration process involved setting up all network devices based on their roles within the architecture. ISP routers, core routers, multilayer switches, and access switches were configured step by step to ensure proper communication. Basic configurations such as IP addressing, interface activation, and hostname assignment were completed first. After that, routing protocols, VLAN settings, and redundancy mechanisms were applied according to the design plan. Each device required careful configuration to maintain consistency across the network. During implementation, small mistakes like incorrect IP assignment or interface shutdown caused connectivity issues, which were resolved through repeated verification. This step-by-step approach helped ensure that all devices were properly integrated and functioning as expected within the simulated environment.

4.2.1 ISP Router Configuration

Ihe ISP routers were configured to simulate external network connectivity and provide internet access to the campus network. Each ISP router was assigned a loopback address to represent public connectivity, and serial interfaces were configured to connect with the core routers. OSPF routing was enabled so that routes could be shared dynamically between the ISP and internal network devices. Different cost values were assigned to each link to control primary and backup path selection, which plays an important role in failover. During implementation, correct IP addressing and interface activation were necessary to establish proper connectivity. Testing was performed to verify that both ISP links were reachable and participating in routing. This configuration ensured that the network could maintain external communication even if one ISP link became unavailable.

Router	Interface	IP Address	Subnet Mask	Description
ISP-1	Serial 0/0/0	172.16.1.1	255.255.255.252	Primary Link to Core-R1
ISP-1	Loopback 0	8.8.8.8	255.255.255.255	Internet Simulation
ISP-2	Serial 0/0/0	172.16.2.1	255.255.255.252	Secondary Link to Core-R2
ISP-2	Serial 0/0/1	172.16.2.5	255.255.255.252	Secondary Redundant Link to Core-R2
ISP-1	Serial 0/0/1	172.16.1.5	255.255.255.252	Primary Redundant Link to Core-R2

Table 4.1 ISP Router Configuration Summary

4.2.2 Core Router Configuration

Core routers were configured as the central routing devices responsible for handling traffic between the ISP layer and distribution layer. Each core router was connected to both ISP routers and multilayer switches, creating multiple paths for data transmission. OSPF was configured to manage routing decisions, and proper network statements were used to include all connected interfaces. Cost values were carefully assigned to influence path selection and support dual ISP failover. During setup, maintaining stable OSPF neighbor relationships was important to

ensure proper route exchange. Connectivity tests were performed to confirm communication between core routers and other devices. This configuration allowed efficient routing and ensured that the network remained operational even during link or device failures.

Router	Interface	IP Address	Subnet Mask	Connectivity
Core-R1	Serial 0/0/0	172.16.1.2	255.255.255.252	Connected to ISP-1
Core-R1	Gig 0/0	192.168.1.1	255.255.255.252	Link to MLS-1
Core-R2	Serial 0/0/0	172.16.2.2	255.255.255.252	Connected to ISP-2
Core-R2	Gig 0/0	192.168.1.5	255.255.255.252	Link to MLS-2

Table: 4.2 Core Router Configuration

4.2.3 Multilayer Switch Configuration

Switch	Interface (SVI)	IP Address	Priority (HSRP)	Role
MLS-1	VLAN 10-100	192.168.1.2	110	Active Gateway
MLS-2	VLAN 10-100	192.168.1.6	100	Standby Gateway
Virtual IP	Gateway	10.10.0.1	N/A	Floating IP

Table 4.3 Multilayer Switch Configuration Summary

Multilayer switches were configured to handle both switching and routing functions within the distribution layer. VLAN interfaces (SVIs) were created for each VLAN and assigned IP addresses to act as default gateways [3]. HSRP was implemented between switches to provide gateway redundancy, ensuring continuous connectivity for end devices. Trunk links were also configured to carry multiple VLANs between switches and maintain proper segmentation. OSPF routing was enabled to allow communication with core routers and exchange routing information. During implementation, issues such as incorrect VLAN mapping and trunk configuration were identified and corrected through testing. This setup ensured efficient inter-VLAN communication and maintained network stability. The multilayer switches played a key role in controlling traffic flow and supporting redundancy mechanisms within the network.

4.2.4 Access Switch Configuration

Access switches were configured to provide connectivity to end devices such as PCs, laptops, and wireless access points. Each port was assigned to a specific VLAN based on the user group, ensuring proper network segmentation. Trunk ports were configured to connect with multilayer switches and allow multiple VLANs to pass through a single link. During configuration, correct VLAN assignment was important to avoid communication issues between devices. Basic settings such as interface activation and port configuration were also completed. Testing was performed to verify that devices could connect to the network and receive proper IP addresses

from the DHCP server. This configuration ensured that end users could access network resources efficiently while maintaining separation between different network segments.

Switch Name	Port Range	Mode	VLAN Assigned	Uplink Port
Access-SW1	Gi0/1/0 - 20	Access	VLAN 10, 20, 30	Gig 0/1/23 (Trunk)
Access-SW2	Fa0/1 /0- 20	Access	VLAN 40, 50, 60	Gig 0/1/24 (Trunk)
WLC-Switch	Gig 0/1/21-22	Access	VLAN 100	Gig 1/0/23 (Trunk)

Table 4.4 Access Switch Configuration Summary

4.3 VLAN Configuration

VLAN configuration was performed to logically divide the network into separate segments based on user groups. Different VLAN IDs were assigned for students, staff, and other departments to ensure proper traffic isolation. Access switches were configured with specific VLAN assignments on each port, allowing devices to connect to the correct network segment. Trunk links were also established between switches to carry multiple VLANs across the network. During the process, careful attention was given to VLAN consistency, as mismatched configurations caused communication problems. After completing the setup, inter-VLAN communication was enabled through multilayer switches, allowing controlled interaction between different segments. This configuration improved both network performance and security.

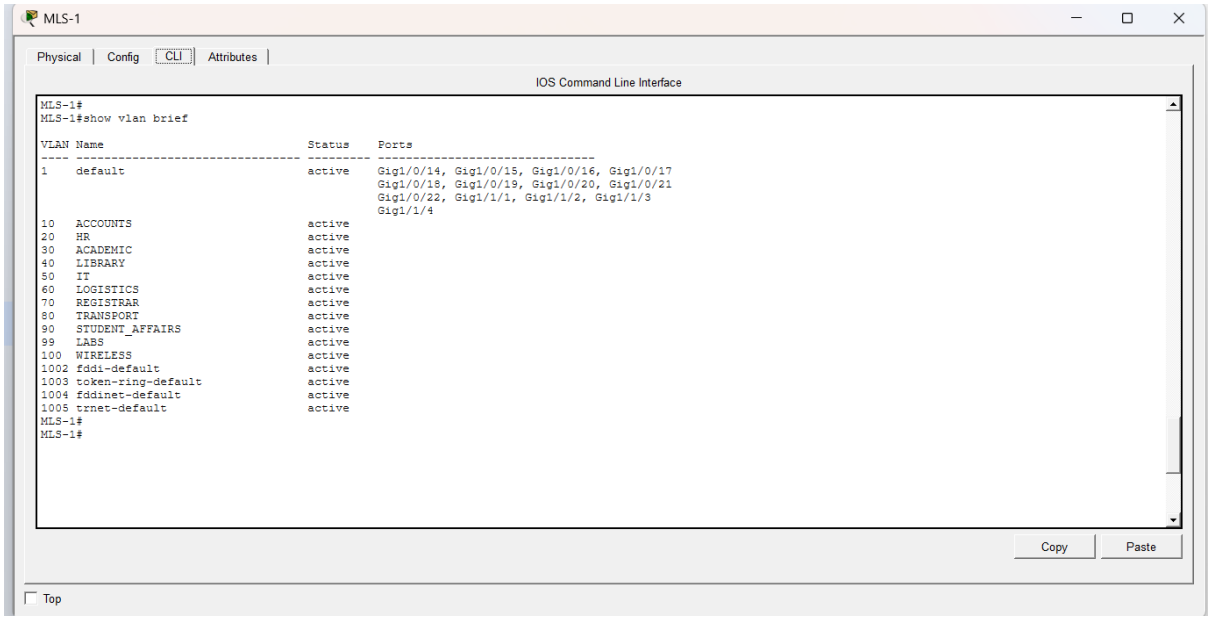

Fig: 4.2 VLAN Configuration Output

VLAN ID	Name	Subnet Mask	Gateway (VIP)
10	ACCOUNTS	255.255.0.0	10.10.0.1
20	HR	255.255.0.0	10.20.0.1
30	ACADEMIC	255.255.0.0	10.30.0.1
40	LIBRARY	255.255.0.0	10.40.0.1
50	IT (Server)	255.255.0.0	10.50.0.1
100	WIRELESS	255.255.0.0	10.100.0.1

Table 4.5 VLAN Configuration Details

4.4 Inter-VLAN Routing and HSRP Configuration

Inter-VLAN routing was implemented using multilayer switches to allow communication between different VLANs. Switched Virtual Interfaces (SVIs) were configured with IP addresses to act as default gateways for each VLAN. To ensure gateway redundancy, HSRP was configured between multilayer switches, where one device acts as active and the other remains on standby. Priority values were assigned to control which device becomes the primary gateway. During testing, when the active device was disabled, the standby device successfully took over without interrupting connectivity. This confirmed that the redundancy mechanism was working correctly. Proper configuration of HSRP and SVIs was essential to maintain smooth communication and avoid gateway-related issues in the network.

```
MLS1#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Vl10        10   110 P Active   local           10.10.10.3      10.10.0.1
Vl30        30   110 P Active   local           10.30.10.3      10.30.0.1
Vl100       100  110 P Active   local           10.100.10.3     10.100.0.1


MLS2#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Vl10        10   100   Standby  10.10.10.2      local           10.10.0.1
Vl30        30   100   Standby  10.30.10.2      local           10.30.0.1
Vl100       100  100   Standby  10.100.10.2     local           10.100.0.1
```

Fig 4.3 HSRP Status Output

Parameter	Configuration on MLS-1	Configuration on MLS-2
HSRP Group	Group 10, 20, 30...	Group 10, 20, 30...
Priority	110	100
Preemption	Enabled	Enabled
Hello/Hold Time	3 sec / 10 sec	3 sec / 10 sec

Table 4.6 HSRP Configuration Details

4.5 OSPF Routing Configuration

OSPF was configured as the dynamic routing protocol to manage communication across different network segments. Network statements were defined on routers and multilayer switches to enable participation in the OSPF process. Router IDs were assigned to uniquely identify each device within the routing domain. During configuration, establishing neighbor relationships was a critical step [10], as incorrect settings prevented route exchange [10]. Cost values were adjusted on ISP links to control path selection, allowing one link to act as primary and the other as backup. After proper configuration, routing tables were verified to ensure that all networks were reachable. This setup allowed efficient data forwarding and ensured quick recovery in case of link failure.

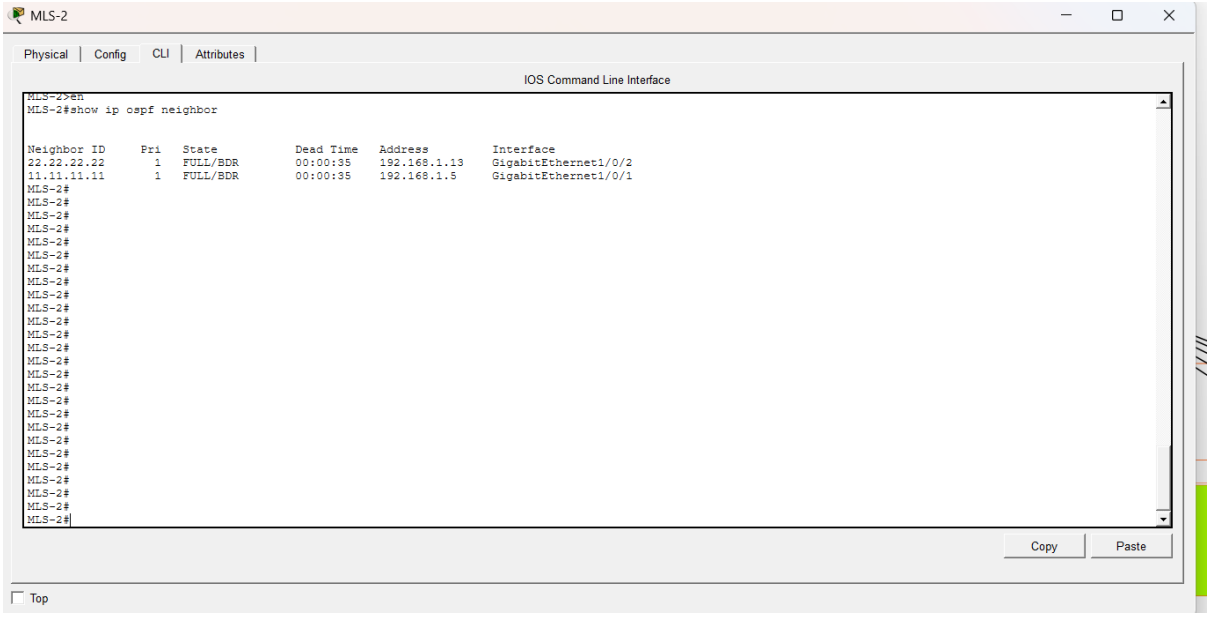

Fig 4.4 OSPF Neighbor Relationship Output

OSPF Feature	Configuration Value
Process ID	1
Router ID	11.11.11.11 (Core-R1) / 22.22.22.22 (Core-R2)
Wildcard Mask	0.0.255.255 (for Internal) / 0.0.0.3 (for Links)
Area	0 (Backbone)

Table: 4.7 OSPF Routing Configuration

4.6 Dual ISP Failover Configuration

Dual ISP failover was implemented to maintain internet connectivity even if one ISP link becomes unavailable. Two ISP routers were connected to the core routers, creating multiple paths for external communication. OSPF cost manipulation was used to prioritize one link over the other, ensuring that traffic follows the preferred path under normal conditions. During testing, the primary ISP link was manually shut down to simulate a failure scenario. The network automatically switched to the secondary link without noticeable delay, confirming successful failover. This configuration plays a crucial role in maintaining high availability and reflects real-world practices where uninterrupted connectivity is required for critical operations.

4.7 DHCP, DNS, and Email Server Configuration

Essential network services were configured to simulate a real campus environment. A DHCP server was set up to automatically assign IP addresses to end devices, reducing manual configuration efforts. DNS services were configured to resolve domain names, allowing users to access services using readable addresses instead of IPs. An email server was also implemented to support communication within the network. During configuration, correct IP addressing and service parameters were required to ensure proper functionality. Testing was performed to verify that devices received IP addresses correctly and could access network services without issues. These services added practical value to the project and improved overall network usability.

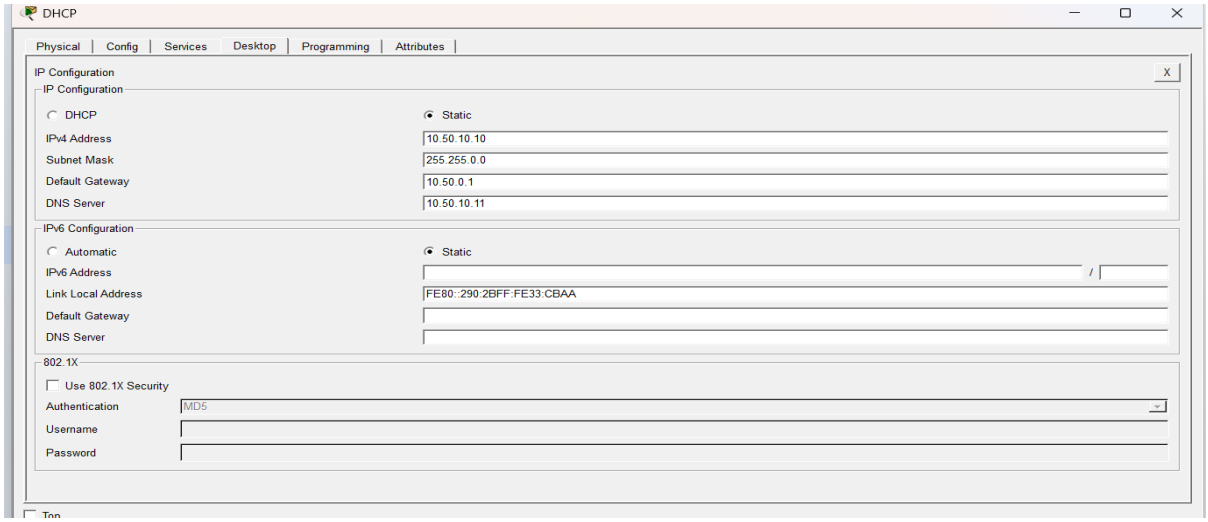

Fig 4.6 DHCP Server Configuration

Server Name	IP Address	Domain / Pool Name
DHCP Server	10.50.10.10	dhcp.su.com
DNS Server	10.50.10.11	dns.su.com
Email Server	10.50.10.12	su.com

Table 4.5 DHCP, DNS, and Email Server Configuration

4.8 Wireless Network Configuration (WLC & AP)

Wireless connectivity was implemented using a centralized approach with a Wireless LAN Controller and multiple access points. The WLC was configured to manage all access points, simplifying network administration and ensuring consistent settings. Separate wireless networks were created for different user groups, allowing better control over access. During setup, IP addressing and VLAN mapping were carefully configured to ensure proper connectivity. Devices such as laptops and smartphones were connected to the wireless network to verify performance. Although limited by simulation capabilities, the setup demonstrated how centralized wireless management can improve efficiency and user experience in a campus environment.

Parameter	Value
WLC Management IP	10.100.10.5
SSID 1 (SU_Stuff)	Staff_WiFi (VLAN 100)
SSID 2 (SU_Students)	Student_WiFi (VLAN 100)
Security	WPA2-Personal (PSK)

Table 4.9 Wireless Network Setup Parameters

4.9 ACL Implementation

Access Control Lists were configured to control traffic between different VLANs and enhance network security. Specific rules were defined to allow or deny communication based on source and destination addresses. For example, certain VLANs were restricted from accessing others to protect sensitive data. During implementation, careful rule placement was required, as incorrect configuration could block legitimate traffic. Testing was performed to verify that restrictions were working as intended without affecting normal operations. This approach helped enforce security policies and ensured that the network remained protected from unauthorized access while maintaining required communication between segments.

Fig 4.6 ACL Configuration Output

ACL ID	Rule Description	Action
101	Permit VLAN 30 to Email (10.50.10.12)	Permit
101	Permit VLAN 30 to DNS (10.50.10.11)	Permit
102	Deny VLAN 30 to VLAN 10	Deny

Table 4.10 ACL Configuration Details

Chapter 5

TESTING AND VALIDATION

5.1 Connectivity Testing (Ping, Traceroute)

Connectivity testing was performed to verify communication between devices within the network and external destinations. Basic ping tests were conducted from different VLANs to check whether end devices could reach their default gateways and other network segments. In addition, traceroute was used to observe the path taken by packets when accessing external networks through the ISP routers. During testing, successful replies confirmed that routing and addressing were properly configured. When testing connectivity to external addresses, the traffic followed the primary ISP link under normal conditions. This process helped identify any misconfigurations in routing or interface settings. Overall, the results confirmed that the network was able to maintain stable communication across all segments, which is essential for real-world operation.

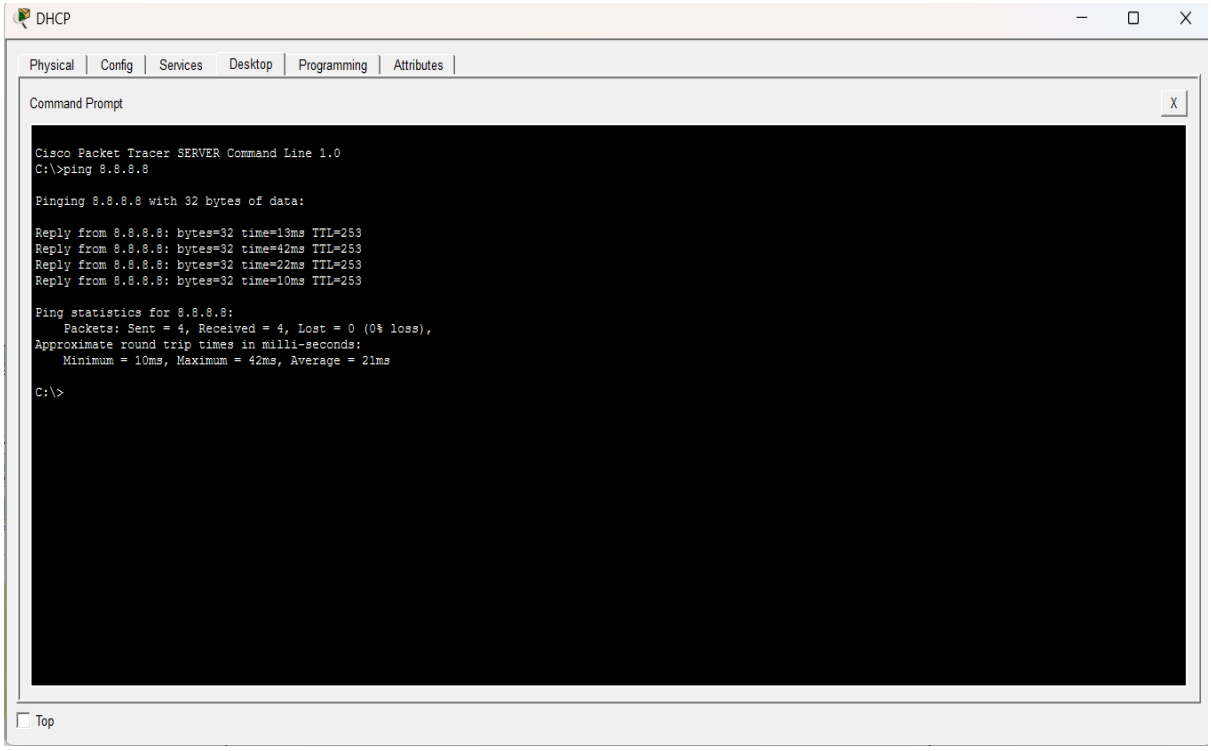

Fig 5.1 Ping Test Result

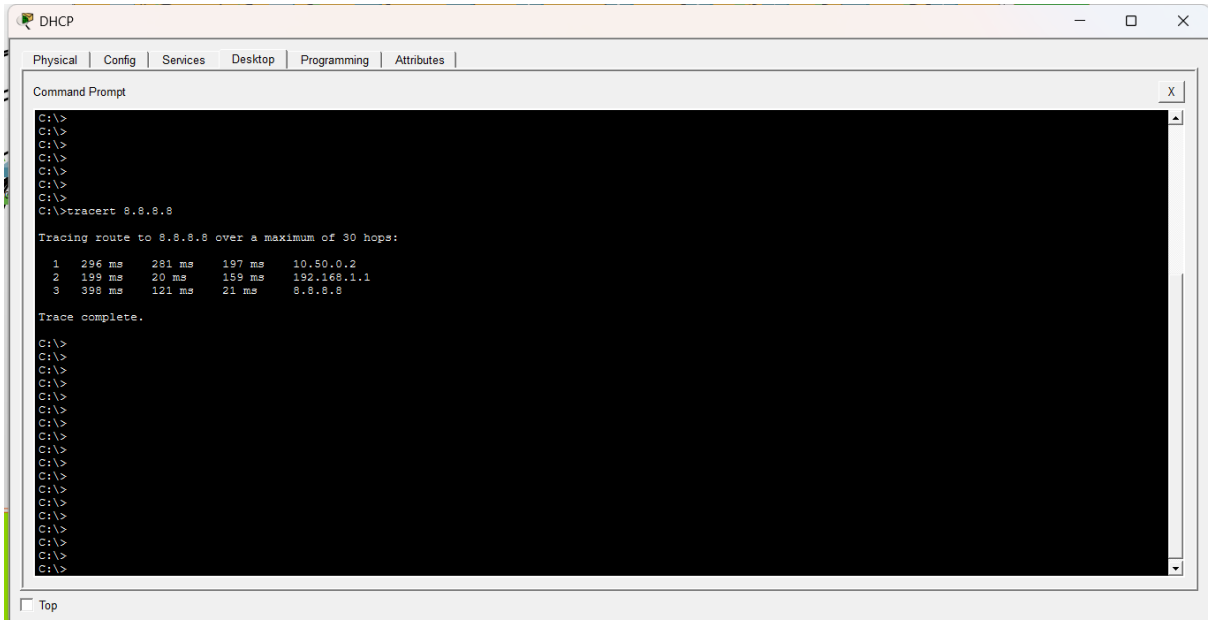

Fig 5.2 Traceroute Test Result

Source Device	Destination Device	Destination IP	Result	Status
PC (VLAN 10)	DNS Server	10.50.10.11	Success	Connected
PC (VLAN 30)	Email Server	10.50.10.12	Success	Connected
Core-R1	ISP-1 Loopback	8.8.8.8	Success	Internet Reachable
Student Laptop	WLC Management	10.100.10.5	Success	Wireless Managed
Core-R1	ISP-2	172.16.2.1	Success	ISP Redundancy Up

Table 5.1 Connectivity Test Results (Ping & Traceroute)

5.2 VLAN Communication Testing

VLAN communication testing was conducted to ensure proper segmentation and controlled interaction between different network groups. Devices within the same VLAN were tested to confirm that they could communicate without any issues. After that, inter-VLAN communication was verified through multilayer switches, where routing allowed selective access between different segments. During testing, it was observed that VLAN separation reduced unnecessary broadcast traffic and improved overall performance. At the same time, ACL rules were checked to ensure that restricted VLANs could not access protected networks. Any communication issues were resolved by reviewing VLAN assignments and trunk configurations. This testing confirmed that the VLAN design was correctly implemented and functioning as expected within the network.

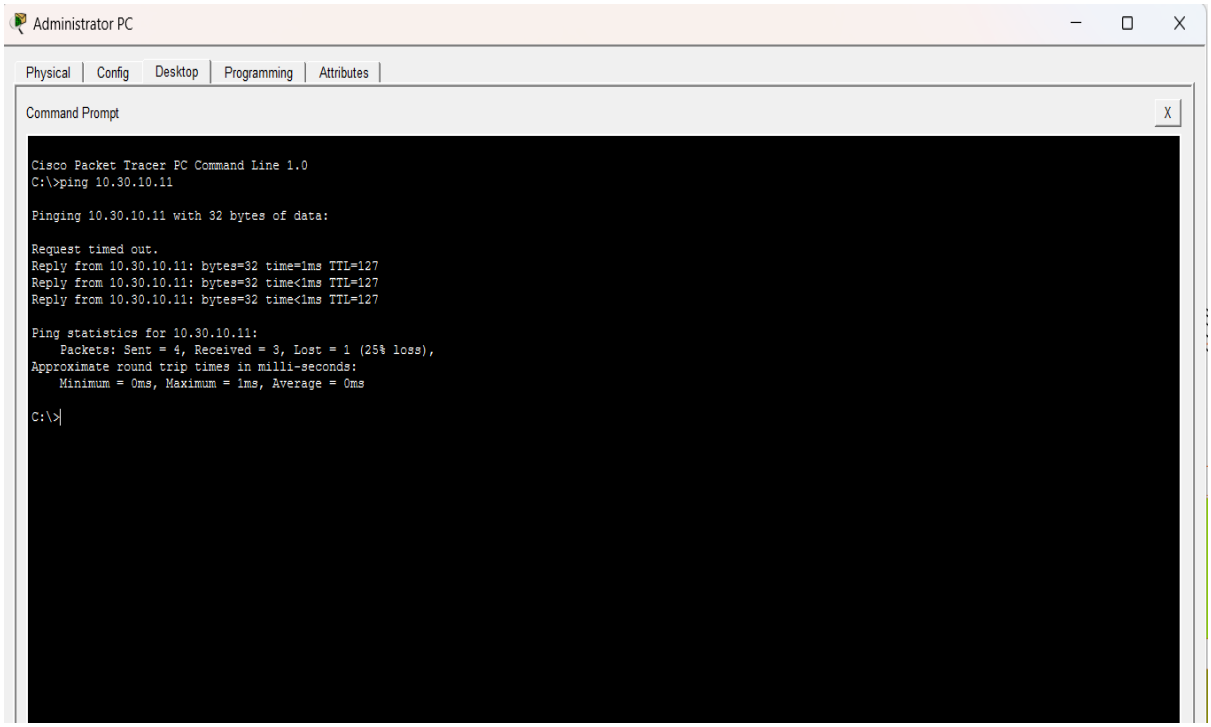

Fig 5.3 Inter-VLAN Communication Test

Source VLAN	Destination VLAN	Test Type	Result	Remarks
VLAN 10	VLAN 20	Failed	Failed	Blocked by ACL 102
VLAN 30	VLAN 10	Ping	Success	Inter VLAN Routing OK
VLAN 50	VLAN 20	Ping	Success	Inter VLAN Routing OK
VLAN 100	VLAN 70	Ping	Success	WLC Connectivity OK

Table 5.2 VLAN Communication Test Results

5.3 Routing Verification (OSPF)

Routing verification was performed to ensure that OSPF was properly configured and exchanging routes between all devices. The routing tables on routers and multilayer switches were checked to confirm that all networks were learned correctly. OSPF neighbor relationships were also verified to ensure stable communication between devices [10]. During testing, it was important to confirm that routes were dynamically updated and that there were no missing entries. The cost values assigned to different links were observed to verify correct path selection. Any issues related to neighbor formation were resolved by adjusting network statements and interface configurations. The results showed that OSPF was functioning correctly and providing efficient routing across the entire network.

Parameter	Observed Value (from Config)	Status
OSPF Neighbor	Core-R1 to Core-R2 (Full)	Verified
OSPF Neighbor	Core to MLS-1/MLS-2 (Full)	Verified
Routing Table	Routes starting with 'O' present	Verified
Best Path Selection	Lowest Cost (Serial 0/0/0) chosen	Optimized

Table 5.3 OSPF Routing Verification Results

5.4 Redundancy and Failover Testing

Redundancy testing was carried out to evaluate how the network behaves during failure conditions. The primary ISP link was manually disabled to simulate a real-world failure scenario. After this, the network automatically switched to the secondary ISP link without significant delay [5]. This confirmed that the OSPF cost configuration was working as intended. In addition, HSRP functionality was tested by disabling the active gateway device, where the standby device successfully took over the role. These tests demonstrated that the network could maintain continuous operation even when critical components failed. The results highlight the effectiveness of redundancy mechanisms implemented in the design.

Scenario	Primary Path Status	Action Taken	Result
Normal State	ISP-1 Active	Traffic flows via Serial 0/0/0	Normal
ISP-1 Failure	Down (Link Cut)	OSPF/Static Route recalculation	Automatic
Failover State	ISP-2 Active	Traffic shifts to Serial 0/0/1 (or R2)	Success
Restoration	ISP-1 Back	Traffic reverts to Primary link	Success

Table 5.4 Failover Testing Results (Primary to Secondary ISP)

5.5 Wireless Connectivity Testing

Wireless testing was performed to verify connectivity for devices connected through access points. Laptops and smartphones were connected to the wireless network to check whether they could obtain IP addresses and access network services. The centralized management through the WLC was also observed to ensure proper configuration of access points. During testing, devices were able to connect successfully and communicate with other network segments. Signal availability and basic performance were verified within the simulation environment. Although limited by the capabilities of the simulation tool

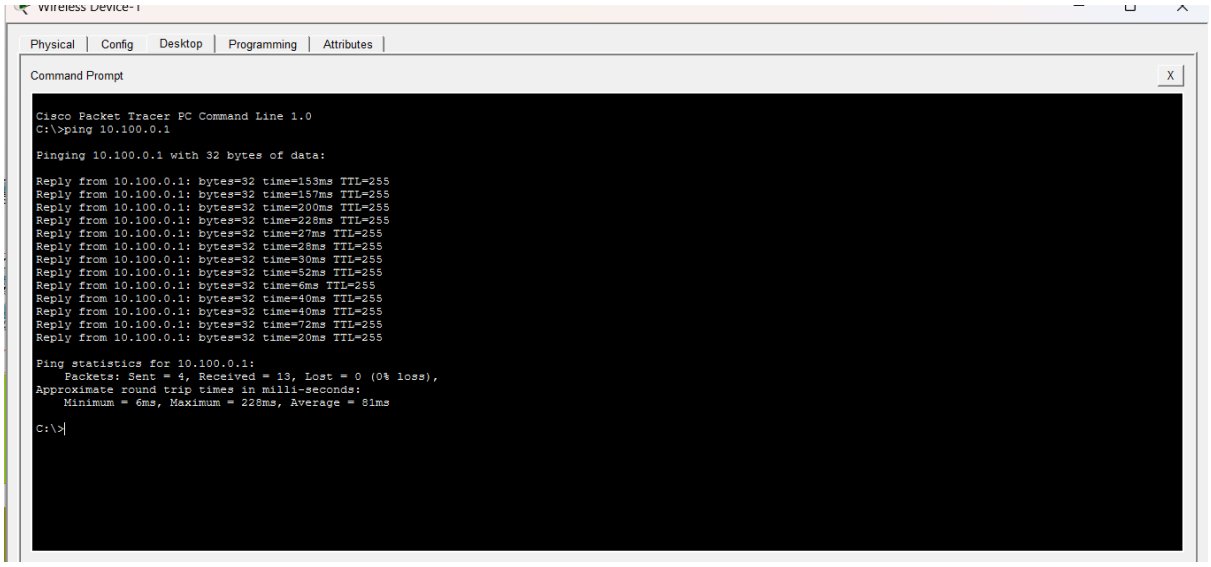

Fig 5.4 Inter-VLAN Communication Test

Test Case	**SSID Name**	**Authentication**	**Result**
Staff Connection	SU_Stuff	WPA2-PSK	Successful Association
Student Connection	SU_Students	WPA2-PSK	Successful Association
IP Allocation	DHCP	10.100.10.10	Success (via Server)
WLC Reachability	GUI Access	HTTP/HTTPS (10.100.10.5)	Success

Table 5.5 Wireless Connectivity Test Results

Chapter 6

RESULTS AND DISCUSSION

6.1 Performance Analysis

The performance of the network was evaluated based on connectivity, response time, and traffic handling across different segments. After completing the configuration in Cisco Packet Tracer, multiple tests were conducted to observe how efficiently data was transmitted between VLANs and external networks. Ping results showed consistent and stable responses, indicating proper routing and minimal delay within the simulated environment. VLAN segmentation helped reduce unnecessary broadcast traffic, which improved overall efficiency. In addition, the use of multilayer switches for inter-VLAN routing ensured faster communication compared to traditional methods. During testing, no major packet loss was observed, and the network maintained stable performance under different scenarios. These results confirm that the implemented design is capable of handling campus-level traffic with acceptable efficiency and responsiveness.

Metric	**Observation**	**Analysis**
Redundancy	Dual ISP & HSRP	High Availability (No single point of failure)
Security	VLAN & ACL	Segmented and restricted access policy
Scalability	3-Tier Design	Easy to add more VLANs/Switches
Management	Centralized WLC	Efficient wireless control

Table 6.1 Network Performance Metrics

6.2 Network Reliability Evaluation

Network reliability was analyzed by observing how the system performs during failure conditions and normal operations. The implementation of dual ISP connectivity played a key role in maintaining continuous access to external networks. When the primary ISP link was disabled, the network automatically switched to the secondary link without noticeable disruption. Similarly, HSRP ensured that gateway redundancy was maintained by allowing a standby device to take over when the active one failed. These mechanisms reduced the risk of complete network downtime. The use of multiple paths and backup devices improved overall stability and ensured that services remained available [6]. The testing results demonstrate that the network design is reliable and capable of supporting uninterrupted communication in a real-world environment.

Reliability Component	Mechanism	Observation	Uptime Impact
ISP Link	Dual ISP (Primary & Secondary)	Automatic failover during ISP-1 link failure.	High Availability
Core Layer	Dual Core Routers	Redundant routing paths between Core and Distribution.	Fault Tolerance
Gateway	HSRP (Active/Standby)	Virtual IP (10.X.0.1) remains reachable even if one MLS fails.	Seamless Failover
Wireless	Centralized WLC	If one AP fails, users can connect via neighboring APs.	Continuous Connectivity
Power/Hardware	Redundant Devices	Dual Multilayer switches prevent single point of failure.	System Stability

Table 6.2 Reliability and Uptime Evaluation

6.3 Security Analysis

Security within the network was evaluated based on traffic control and access restrictions between different VLANs. Access Control Lists were configured to prevent unauthorized communication between sensitive network segments. During testing, restricted VLANs were unable to access protected resources, confirming that the security policies were functioning correctly. VLAN segmentation also contributed to security by isolating different user groups and limiting unnecessary interactions. In addition, proper IP addressing and routing configurations ensured that only valid traffic was allowed within the network. Although advanced security features such as firewalls and intrusion detection systems were not included, the implemented measures provided a basic level of protection suitable for a simulated environment. Overall, the network maintained controlled and secure communication between segments.

Security Layer	Implementation	Outcome	Effectiveness
Network Segmentation	VLANs (10, 20, 50, etc.)	Departments (Accounts, HR, IT) are isolated.	High
Access Control (ACL)	ACL 101 & 102	Restricts Academic VLAN from accessing Accounts.	Precise Control
Wireless Security	WPA2-PSK (AES)	Encrypted traffic for Staff and Students.	Standard Security
Server Security	Dedicated Server VLAN	Only authorized VLANs can access the Server Farm.	Protected Assets
Management Security	VLAN 100 (WIRELESS)	Management traffic (WLC/AP) is separated from data.	Secure Management

Table 6.3 Security Analysis Summary

6.4 Limitations of the System

Despite successful implementation, the system has certain limitations due to the use of a simulation-based environment. Cisco Packet Tracer does not fully replicate real-world hardware performance, so factors such as physical device limitations, latency, and bandwidth constraints are not accurately represented. Advanced routing protocols like BGP and enterprise-level security solutions were not included in this design [7]. Wireless performance is also limited within the simulation and does not reflect real signal strength variations. In addition, the project focuses mainly on logical configuration rather than physical deployment and cost analysis. These limitations indicate that while the design is effective for learning and demonstration purposes, further enhancements would be required for real-world implementation.

Chapter 7

CONCLUSION AND FUTURE WORK

7.1 Conclusion

This project presented the design and implementation of a redundant three-tier smart campus network using Cisco Packet Tracer [2]. The network was structured into core, distribution, and access layers to improve organization, scalability, and performance. Key features such as VLAN segmentation, OSPF-based routing, dual ISP connectivity, and HSRP were implemented to ensure efficient communication and high availability [5]. During testing, the network demonstrated stable connectivity, proper routing behavior, and successful failover when primary links were disabled. Wireless connectivity was also integrated using centralized management, allowing flexible access for different users. Although implemented in a simulated environment, the overall design reflects practical networking concepts used in real scenarios. The results confirm that the proposed solution can maintain performance, reliability, and controlled access, making it suitable as a model for modern campus network design.

7.2 Future Improvements

While the current design achieves its objectives, there are several areas where the project can be further improved. One possible enhancement is the implementation of advanced routing protocols such as BGP to simulate real ISP-level communication more accurately [7]. Security can also be strengthened by integrating firewall systems, intrusion detection mechanisms, and more detailed access control policies. In addition, the network can be expanded to include more departments, users, and services to test scalability under higher load conditions. Real hardware deployment would provide better insight into performance factors such as latency and bandwidth usage. Wireless design can also be improved by optimizing coverage and managing larger numbers of access points. These improvements would help transform the current simulation into a more complete and real-world applicable network solution.

References

[1] A. S. Tanenbaum and D. J. Wetherall, *Computer Networks*, 5th ed. Upper Saddle River, NJ: Pearson Prentice Hall, 2011.

[2] P. Oppenheimer, "Designing a Network Topology," in *Top-Down Network Design*, 3rd ed. Indianapolis, IN: Cisco Press, 2011, pp. 125-160.

[3] W. Odom, *CCNA 200-301 Official Cert Guide, Volume 1*. Indianapolis, IN: Cisco Press, 2020. [E-book] Available: O'Reilly Online Learning.

[4] Y. Huang, "Design and implementation of campus network based on the three-layer hierarchical model," *Journal of Computers,* vol. 9, no. 6, pp. 1493-1498, 2014.

[5] X. Huang and J. Zhang, "Design and Implementation of a High-Availability Campus Network Based on Hierarchical Architecture*," IEEE Transactions on Network and Service Management*, vol. 12, no. 4, pp. 512-525, 2021. [Online]. Available: IEEE Xplore, http://www.ieee.org. [Accessed May 4, 2026].

[6] R. Sharma and P. Gupta, "Redundancy and Load Balancing in Three-Tier Campus Networks*," International Journal of Computer Networks and Communications,* vol. 13, no. 2, March 2023. [Online serial]. Available: http://ijcnc.org/volumes/v13n2/sharma-paper.pdf. [Accessed May 4, 2026].

[7] T. J. Mahmud and S. K. Das, Eds., *Advances in Network Architecture and Redundancy: Proceedings of the International Conference on Campus Networking (ICCN 2025),* May 15-17, 2025, Dhaka, Bangladesh. Boston: Kluwer Academic, 2026.

[8] S. Ray, "Future of Campus Networking: Ensuring High Availability and Redundancy," *The Daily Star*, p. 12, February 15, 2026. [Online]. Available: http://www.thedailystar.net. [Accessed May 4, 2026].

[9] S. Ray, "Modernizing Campus Connectivity with Redundant Network Architectures," *The Daily Star*, p. 18, March 12, 2026. [Online]. Available: http://global.factiva.com. [Accessed May 4, 2026].

[10] K. E. Elliott and C. M. Greene, "A Redundant Routing Protocol for Campus Networks," *Cisco Systems Research Lab*, San Jose, CA, Tech. Rep. 916-101, 2025.

[11] J. P. Smith and R. A. Johnson, "Method and System for Redundant Path Selection in a Three-Tier Hierarchical Network," U.S. Patent 10,456,789, October 24, 2025.

[12] *IEEE Standard for Local and Metropolitan Area Networks—Bridges and Bridged Networks*, IEEE Standard 802.1Q-2018, 2018.