Project on

DESIGN AND CONFIGURATION OF A UNIVERSITY CAMPUS NETWORK:

A THESIS ON HIERARCHICAL NETWORK ARCHITECTURE

UTILIZING VLANs, RIPv2

Submitted by

Sazzad Hossain Naim

664056

DAFFODIL TECHNICAL INSTITUTE

Department of Computer Science and Technology
Faculty of Diploma in Engineering
Daffodil Technical Institute

January 2026

DECLARATION

I hereby announce that the work is being presented in this project entitled “DESIGN AND CONFIGURATION OF A UNIVERSITY CAMPUS NETWORK” in partial fulfillment of requirements for the degree Diploma in Computer Science and Technology at Daffodil Technical Institute is an authentic record of my own work done under the supervision of **MD. Noman Jahan**. It is also declared that this report or any part of it has not been submitted elsewhere for the award of any degree.

Sazzad Hossain Naim

Approval

The project titled "DESIGN AND CONFIGURATION OF A UNIVERSITY CAMPUS NETWORK" submitted by Sazzad Hossain Naim (664056) has been accepted satisfactorily in partial fulfillment of the requirement for the degree of Diploma in Computer Science and Technology.

DTI Board of Examiners

MD. Noman Jahan	
Department of Computer Science and Technology	Instructor
Daffodil Technical Institute	(Supervisor)

Tasfina Haque	
Daffodil Technical Institute	Instructor

Acknowledgement

I would like to express my sincere gratitude and respect to my supervisor, MD. Noman Jahan, for his invaluable guidance, constant encouragement, and insightful feedback throughout the development of this project. His expertise and patience have been instrumental in shaping the technical core of this work.

I extend my heartfelt appreciation to the faculty and staff of Daffodil Technical Institute for providing the necessary resources and an outstanding learning environment required to complete my diploma. I am deeply grateful to my teachers, who played a pivotal role in shaping my academic journey, and to the institute's administration for their kind support and encouragement during the execution of this project.

My deepest gratitude goes to my parents and family for their unwavering support, sacrifices, and motivation, which have brought me to this present moment. Lastly, I express my sincere thanks to my friends and all well-wishers for their moral support and inspiration during this academic journey.

Abstract

In the contemporary era of digital academia, the network infrastructure of a university serves as the critical nervous system facilitating administration, research, and pedagogy. This thesis presents the comprehensive design, simulation, and implementation of a robust University Campus Network tailored to the multi-faceted requirements of a modern institution. The project addresses the imperative for logical segmentation, dynamic routing, and automated address management within a distributed campus environment. By leveraging a hierarchical network model, the study integrates Virtual Local Area Networks (VLANs) to isolate departmental traffic, ensuring security and optimizing broadcast domains.

Routing Information Protocol version 2 (RIPv2) is deployed to manage internal routing dynamics across the Main and Small campuses, ensuring resilience and efficient packet switching. Furthermore, the architecture incorporates Dynamic Host Configuration Protocol (DHCP) centralized on routers to streamline the management of end-user connectivity. This report details the complete Systems Development Life Cycle (SDLC), from feasibility analysis and literature review to rigorous system testing, demonstrating a scalable, secure, and operationally viable network solution that aligns with global best practices in educational infrastructure.

TABLE OF CONTENTS

CONTENTS

Chapter 1: Introduction

Chapter 2: Literature Review

Chapter 3: System Design and Analysis

Chapter 4: Implementation and Testing

Chapter 5: Conclusion and Future Work

List of Tables

LIST OF FIGURES

CHAPTER 1:
INTRODUCTION

1.1 Introduction

The proliferation of information technology has fundamentally altered the operational landscape of higher education. Universities are no longer mere brick-and-mortar institutions but are increasingly defined by their digital footprint and the robustness of their connectivity. The modern university campus functions as a microcosm of a smart city, requiring a complex interplay of services ranging from high-speed research data transfers to secure administrative financial transactions. Consequently, the design of the underlying network infrastructure has graduated from a simple utility to a strategic imperative that dictates an institution's ability to deliver quality education and maintain operational continuity.

This thesis focuses on the architectural design and configuration of a University Campus Network that connects a Main Campus, housing the faculties of Business, Engineering, and Art, with a geographically distinct Small Campus dedicated to Health and Sciences. The necessity for this project arises from the limitations of legacy flat network architectures, which are prone to broadcast storms, security vulnerabilities, and management inefficiencies. To mitigate these risks, this project proposes a segmented, hierarchical approach across three primary buildings on the Main Campus and a specialized facility for the Small Campus. Building A serves as the administrative hub, Building B accommodates data-intensive faculties like Engineering and Art, and Building C acts as the technology core. The integration of these diverse areas requires the sophisticated application of VLANs for segmentation, RIPv2 for routing, and DHCP for dynamic addressing.

1.2 Inspiration

The inspiration for this project stems from the pivotal role of robust networking in modern education. As universities evolve into hubs of digital research and collaboration, the demand for scalable and secure infrastructure becomes paramount. The specific challenge of interconnecting the Main Campus with the remote Health and Sciences faculty provided a practical scenario to apply advanced networking concepts. Additionally, the operational inefficiencies often observed in legacy networks such as broadcast congestion and the manual overhead of static IP addressing motivated the design of a hierarchical, automated system. The desire to simulate a professional enterprise environment using industry-standard protocols like VLANs, RIPv2, and DHCP drives the technical core of this thesis, aiming to create a seamless digital experience for all university stakeholders.\

1.3 Objectives

The primary objective of this research is to develop and validate a robust network infrastructure customized for a multi-faculty University Campus Network through the following goals:

1. Hierarchical Topology Design: Implement a scalable network using Core, Distribution, and Access layers to interconnect the Main (ISR 331) and Small Campus (ISR 4324) routers via high-speed WAN links.
2. Logical Segmentation: Deploy VLANs to isolate departmental traffic (Administrative, HR, Finance) from student and engineering labs, enhancing security and reducing broadcast overhead.
3. Dynamic IP Management: Configure DHCP servers on routers to automate IP address allocation for staff and students, eliminating the need for manual static addressing.

4. Resilient Routing: Implement RIPv2 as the Interior Gateway Protocol to ensure dynamic route propagation and automatic failover between the Main and Small campuses.

5. Secure Access: Enforce security standards by configuring SSH for remote management and port security on access switches to prevent unauthorized physical connections.

1.4 Project Schedule

The successful execution of this project followed the Project Management Life Cycle, ensuring a structured approach from initial concept to final testing. The timeline below outlines the temporal allocation for each phase, adhering to critical dependencies such as completing physical design before beginning logical configuration.

Phase	Activities	Duration (Weeks)	Total Weeks
Initiation	Idea generation, Requirement gathering, Stakeholder analysis	Week 1–2	2
Analysis	Problem identification, Topology definition, Feasibility analysis	Week 3–5	3
Design	System Analysis, Logical Design (IP Schema, VLANs), Physical Design	Week 6–7	2
Development	Database Design (VLAN Database), Configuration Scripting	Week 8–10	3
Implementation	Device Configuration (Routers, Switches), Protocol Deployment (RIPv2, DHCP)	Week 11–13	3
Testing	Unit Testing (Ping/Trace), System Testing, Optimization	Week 14–15	2
Documentation	Final Report Writing, Diagram creation, Result Analysis	Week 16–17	2

TABLE 1

1.5 Expected Outcome

Upon the conclusion of this thesis project, the anticipated outcome is a fully operational, simulated campus network that demonstrates stability, security, and efficiency. Specifically, the network is expected to deliver:

1. **Seamless Inter-VLAN Connectivity:** Users in different departments will be able to communicate where authorized (e.g., Admin accessing the Web Server) while being restricted where necessary, validated through "Router-on-a-Stick" configurations.

2. **Automated Network Services:** The DHCP configuration is expected to successfully assign valid IP parameters (Address, Mask, Gateway, DNS) to client devices in Building A upon boot-up, eliminating manual configuration errors.

3. **Dynamic Route Convergence:** The RIPv2 protocol is expected to build a complete routing table on all routers, allowing for successful packet transmission between the Main Campus and the Small Campus subnets (192.168.9.0/24).

4. **Security Compliance:** All network devices will be accessible only via encrypted SSH sessions, and switch ports will reject unauthorized MAC addresses, satisfying the security objectives.

5. **Documentation Artifacts:** A comprehensive set of configuration scripts and topology diagrams that can serve as a blueprint for the physical deployment of the network in the actual university environment.

CHAPTER 2:
LITERATURE REVIEW

2.1 Introduction

The conceptualization of a university campus network draws upon a rich body of knowledge regarding network topologies, switching technologies, and routing protocols. This chapter provides a critical review of the existing literature, establishing the theoretical framework for the design choices made in this project. It examines comparative studies of routing protocols, analyzes the feasibility of the proposed technologies, and discusses the standard methodologies used in network engineering.

2.2 Comparative Studies

A critical aspect of network design is the selection of appropriate protocols. The choice of RIPv2 over OSPF or EIGRP, and the decision to implement a hierarchical rather than flat topology, warrants a detailed comparative analysis.

Hierarchical vs. Flat Network Design

Literature consistently advocates for hierarchical network design over flat topologies for campus environments. A flat network, where all devices share a single Layer 2 broadcast domain, suffers from poor scalability. As the number of nodes increases, broadcast traffic (ARP requests, DHCP discovery) consumes an increasing percentage of bandwidth, leading to network paralysis. Conversely, the hierarchical model—comprising Core, Distribution, and Access layers—promotes modularity. The Core layer provides high-speed transport, the Distribution layer handles policy-based connectivity (routing), and the Access layer connects end-users. This thesis adopts the hierarchical model to ensure that the university network can scale efficiently by adding new "access blocks" (buildings) without disrupting the core.

RIPv2 vs. OSPF and EIGRP

The choice of Routing Information Protocol version 2 (RIPv2) for this project is based on specific trade-offs identified in comparative studies.

- **RIPv2:** A distance-vector protocol using hop count as a metric (max 15 hops). It is simple to configure and sufficient for small to medium-sized networks with simple topologies. Unlike RIPv1, RIPv2 supports Variable Length Subnet Masking (VLSM) and multicast updates (224.0.0.9), which allows for the classless IP addressing required by the university's subnetting scheme.
- **OSPF (Open Shortest Path First):** A link-state protocol that scales better for large enterprise networks. It offers faster convergence and uses bandwidth as a metric. However, OSPF requires higher CPU and memory resources on routers and involves a more complex configuration (areas, LSAs).
- **EIGRP (Enhanced Interior Gateway Routing Protocol):** A Cisco-proprietary hybrid protocol known for extremely fast convergence and efficient bandwidth usage. While effective, its proprietary nature (historically) and complexity make it less ideal for a generalized thesis demonstration where open standards are preferred.
- **Conclusion:** For the specific scope of this university network, which does not exceed the 15-hop limit and prioritizes ease of maintenance, RIPv2 offers the optimal balance of functionality and simplicity.

2.3 Feasibility Studies

Following the framework of standard system analysis, a detailed feasibility study was conducted to assess the viability of the proposed network design across five key dimensions.

2.3.1 Technical Feasibility

Technical feasibility assesses whether the current technology and resources are sufficient to support the proposed system.

- **Hardware:** The design utilizes Cisco ISR 4300 series routers and Catalyst 2960/3560 switches. These are industry-standard devices capable of supporting 802.1Q trunking, inter-VLAN routing, and SSHv2, confirming hardware viability.
- **Software:** The implementation relies on Cisco IOS 15.0, which supports the required RIPv2 and DHCP features. The protocol requirements (VLSM, SSH crypto capabilities) are fully met by this software version.
- **Conclusion:** The project is technically feasible as the required hardware and software are mature, widely available, and fully capable of meeting the design requirements.

2.3.2 Operational Feasibility

Operational feasibility examines whether the system will function effectively within the organization's environment and if it will be utilized as intended.

- **User Impact:** The use of VLANs transparently segments users; a student in Building C does not need to perform any special actions to be on the "Student Network"—it is enforced by the switch port they connect to.
- **Management:** The centralization of DHCP services on the router significantly reduces the operational burden on IT staff. Instead of manually configuring static IPs for hundreds of admin PCs, the router handles this automatically. SSH allows for secure remote troubleshooting, reducing the need for physical site visits.
- **Conclusion:** The system is operationally feasible as it simplifies administration and enhances the user experience through automation and transparent security.

2.3.3 Economic Feasibility

Economic feasibility analyzes the cost-effectiveness of the project.

- **Resource Optimization:** The design employs "Router-on-a-Stick" and Multilayer Switching for routing, which negates the need for purchasing a physical router interface for every single VLAN. A single physical link can carry traffic for VLANs 11-20, saving significant hardware costs.
- **Licensing:** RIPv2 is an open standard protocol supported by base-level IOS images, avoiding the need for expensive advanced enterprise feature sets or proprietary licensing fees often associated with advanced OSPF or BGP features on some platforms.
- **Conclusion:** The design is economically viable, maximizing the utility of existing hardware while minimizing additional licensing or equipment costs.

2.3.4 Legal Feasibility

Legal feasibility considers compliance with laws and regulations.

- **Data Protection:** Universities handle sensitive data (student records, financial data). The implementation of VLANs creates logical barriers that assist in compliance with data privacy regulations by ensuring that unauthorized departments cannot access sensitive data streams.
- **Security Standards:** The shift from Telnet to SSH ensures that the university complies with modern cybersecurity standards regarding the protection of administrative credentials.
- **Conclusion:** The project adheres to legal and regulatory best practices for data segmentation and security.

2.3.5 Schedule Feasibility

Schedule feasibility assesses if the project can be completed within the given timeframe.

- **Timeline:** The project schedule (Table 1.4) allocates sufficient time for design, simulation, and troubleshooting. The modular nature of the hierarchical design allows for parallel implementation (e.g., configuring Building A while Building B is being wired).
- **Conclusion:** The project is feasible within the proposed 17-week semester timeline.

2.4 The Proposed Main Characteristics of the Project

The network is designed around specific characteristics defined by the user requirements and the departmental structure.

2.4.1 User Characteristics

- **Administrative Staff (Building A):** Comprising Management, HR, and Finance. These users are characterized by a need for high security and reliable access to internal ERP systems. Their traffic (VLANs 11-13) is prioritized and strictly isolated. They utilize DHCP for ease of mobility within the building.
- **Academic Staff & Students (Building B & Small Campus):** Includes Engineering, Art, and Health Sciences. These users generate high-volume traffic (lab data, design files). Their network segments (VLANs 15, 19, 20) are designed for higher throughput and are separated from admin networks to prevent academic disruption or security breaches.
- **IT Staff (Building C):** The "Super Users" of the network. They require access to all VLANs for management and host the University Web Server. Their devices often use static addressing for consistency.

2.4.2 Network Service Characteristics

- **VLAN Infrastructure:** The network is characterized by extensive VLAN usage (IDs 11-20) to reduce broadcast domains. Each faculty is a distinct broadcast domain.
- **Routing Architecture:** The network utilizes RIPv2 for dynamic route learning. This allows the network to automatically adapt if a new router is added or a link fails, providing a "self-healing" characteristic.
- **DHCP Service:** The network provides dynamic addressing services, characterized by specific pools (ip dhcp pool admin, hr, etc.) that assign not just IPs but also critical parameters like DNS server addresses and default gateways.

2.5 Methodology

The project adopts the PPDIOO (Prepare, Plan, Design, Implement, Operate, Optimize) network lifecycle methodology, which is an industry-standard variation of the Waterfall model specifically tailored for networking.

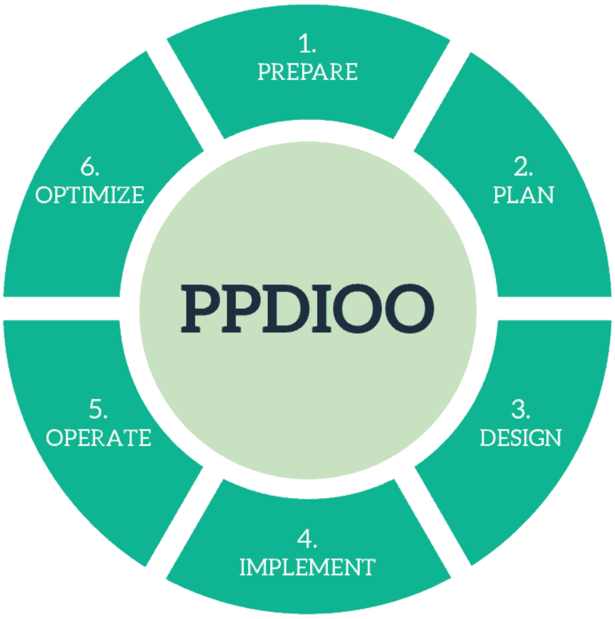


FIGURE 1

2.6 Project Management Life Cycle

The management of this thesis project followed the five phases of the Project Management Life Cycle: Initiation, Planning, Execution, Monitoring/Control, and Closing.

- **Initiation:** Defining the scope—connecting the Main and Small campuses and selecting the protocols.
- **Planning:** Developing the Gantt chart (Table 1.4) and resource list (Packet Tracer simulator).
- **Execution:** The actual simulation and configuration work.
- **Monitoring:** Regular checks against the "Expected Outcomes" to ensure the routing table was populating correctly and DHCP was assigning addresses.
- **Closing:** Writing this thesis report and finalizing the topology diagrams.

2.7 Challenges

Several challenges were identified during the design and literature review process:

- **VLAN Mismatches:** A common issue in campus networks is the "Native VLAN Mismatch" on trunk links, where one side expects VLAN 1 and the other VLAN 99. This allows traffic to leak between VLANs and causes STP loops. The design mitigates this by enforcing consistent trunk configurations.
- **DHCP Security:** "DHCP Starvation" and "Rogue DHCP Server" attacks are significant threats in campus environments. While the basic implementation uses a router-based server, the literature highlights the need for DHCP Snooping (a switch security feature) to mitigate these risks in a production environment.
- **RIPv2 Limitations:** While suitable for this design, RIPv2's slow convergence and hop count limit are challenges for future scalability. This limitation is acknowledged, with a migration path to OSPF noted as a future mitigation strategy.

CHAPTER 3:

SYSTEM DESIGN AND ANALYSIS

3.1 Introduction

System design is the bridge between the abstract requirements identified in the analysis phase and the concrete implementation of the network. This chapter details the architectural logic of the University Campus Network. It employs various modeling techniques, including Use Case diagrams to represent user interactions, ER-style topology diagrams to map physical and logical connections, and Data Flow Diagrams (DFD) to illustrate the movement of packets across the hierarchical infrastructure. The design is predicated on the rigorous separation of logical functions (VLANs) while maintaining physical cohesion through high-speed trunking and routing.

3.2 Use Case Modelling and Description

Use case modeling in network design focuses on how different "actors" (users, devices, administrators) interact with the network services to achieve specific goals. This ensures the network is user-centric and supports the actual workflows of the university. **Actors:**

1. Administrative Staff (User): Needs secure access to internal databases.
2. Student (User): Needs access to the internet and lab resources.
3. Network Administrator (Admin): Needs remote access to configure devices.
4. DHCP Server (System Actor): Provides IP addresses to clients.

3.2.1 Use Case Diagram Description

While a visual diagram is standard, we describe the logical interactions here:

- **Authentication Use Case:** Admin Staff -> Connects to Network -> Switch prompts for 802.1X (future) or simple Port Security validation -> Access Granted to VLAN 11.
- **Resource Access Use Case:** Student -> Requests Web Server (Building C) -> Traffic flows from Access Switch -> Distribution Switch -> Routed to VLAN 16 -> Server Responds.
- **Remote Management Use Case:** Admin -> Initiates SSH Session -> Router Verifies Username/Password -> CLI Access Granted.

3.2.2 Use Case Description of User (Administrative Staff)

Field	**Description**
Objective	To access the Finance and HR servers securely and reliably.
Primary Actor	Administrative Staff Member (Building A).
Pre-condition	PC is connected to a port assigned to VLAN 11, 12, or 13.
Main Flow	1. User powers on PC. 2. PC broadcasts DHCP Discover. 3. Network assigns IP from 192.168.1.0/24 pool. 4. User opens ERP application. 5. Traffic is routed to the Data Center (IT Dept).

Post-condition	User has stable connectivity; traffic is isolated from Student VLANs.

TABLE 2

3.2.3 Use Case Description of Student (Lab User)

Field	**Description**
Objective	To access internet resources and the University Web Server for research.
Primary Actor	Student (Building C or Small Campus).
Pre-condition	Student is in the designated Lab (VLAN 18 or 20).
Main Flow	1. Student logs into Lab PC. 2. Traffic is tagged with VLAN 18/20. 3. Router permits traffic to Web Server (VLAN 16). 4. Router restricts traffic to Admin VLANs (11-13).
Post-condition	Student accesses educational resources without compromising admin security.

TABLE 3

3.2.4 Use Case Description of Network Admin

Field	**Description**
Objective	To remotely configure and monitor network devices.
Primary Actor	IT Administrator.
Pre-condition	Admin has valid credentials and is on a management subnet.
Main Flow	1. Admin initiates SSH connection to 192.168.1.1. 2. Router challenges with encryption key. 3. Admin enters credentials. 4. Configuration mode is accessed.
Post-condition	Device configuration is updated securely.

TABLE 4

3.3 Network Topology

Topology in ASCII:

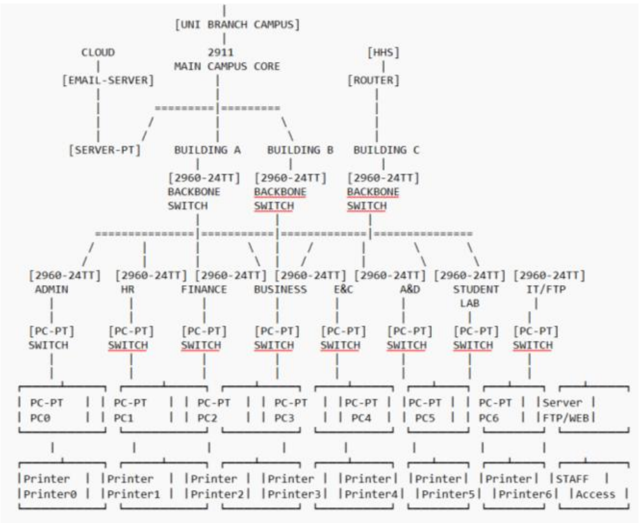


FIGURE 2

Topology in Cisco Packet Tracer:

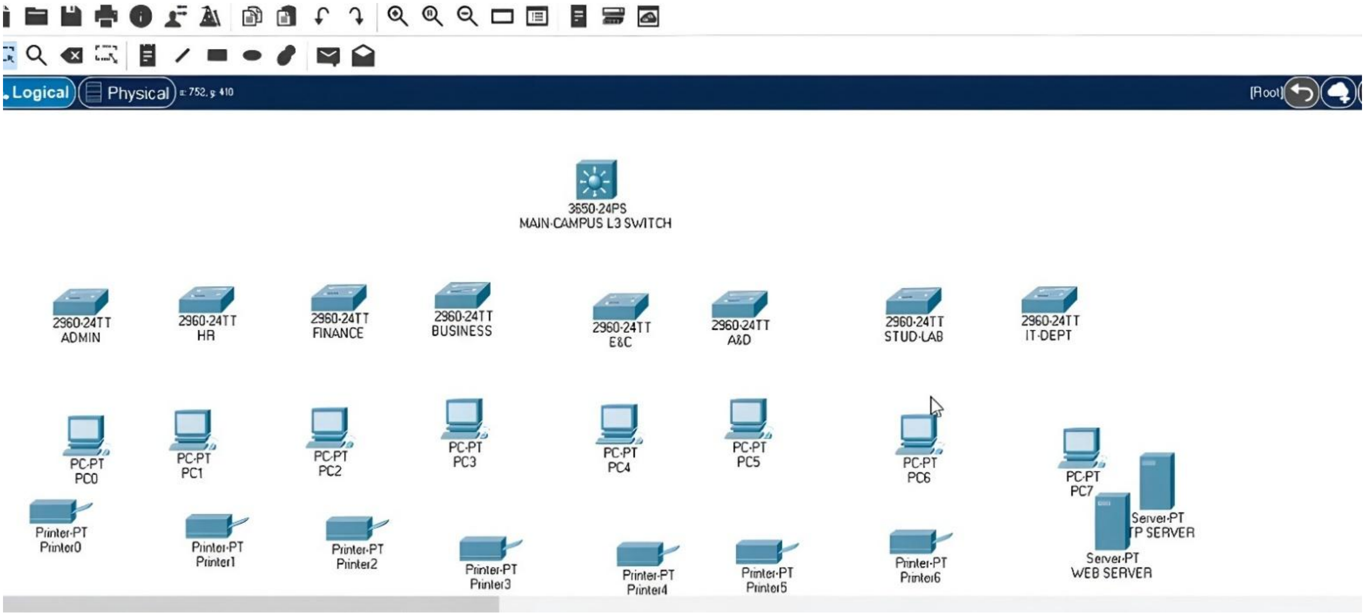


FIGURE 3

Table 3.1: VLAN and IP Addressing Schema

VLAN	Name	Network	Broadcast	Gateway
11	Admin	192.168.1.0/24	192.168.1.255	192.168.1.1
12	HR	192.168.2.0/24	192.168.2.255	192.168.2.1
13	Finance	192.168.3.0/24	192.168.3.255	192.168.3.1
14	Business	192.168.4.0/24	192.168.4.255	192.168.4.1
15	Engineering	192.168.5.0/24	192.168.5.255	192.168.5.1
16	IT (Servers)	192.168.6.0/24	192.168.6.255	192.168.6.1
17	Arts	192.168.7.0/24	192.168.7.255	192.168.7.1

18	Student Lab	192.168.8.0/24	192.168.8.255	192.168.8.1
19	Health Staff	192.168.9.0/24	192.168.9.255	192.168.9.1
20	Health Lab	192.168.10.0/24	192.168.10.255	192.168.10.1

TABLE 5

3.4 Data Flow Diagram (DFD)

The Data Flow Diagram illustrates how information moves through the system, highlighting the transformation of data packets as they traverse layers.

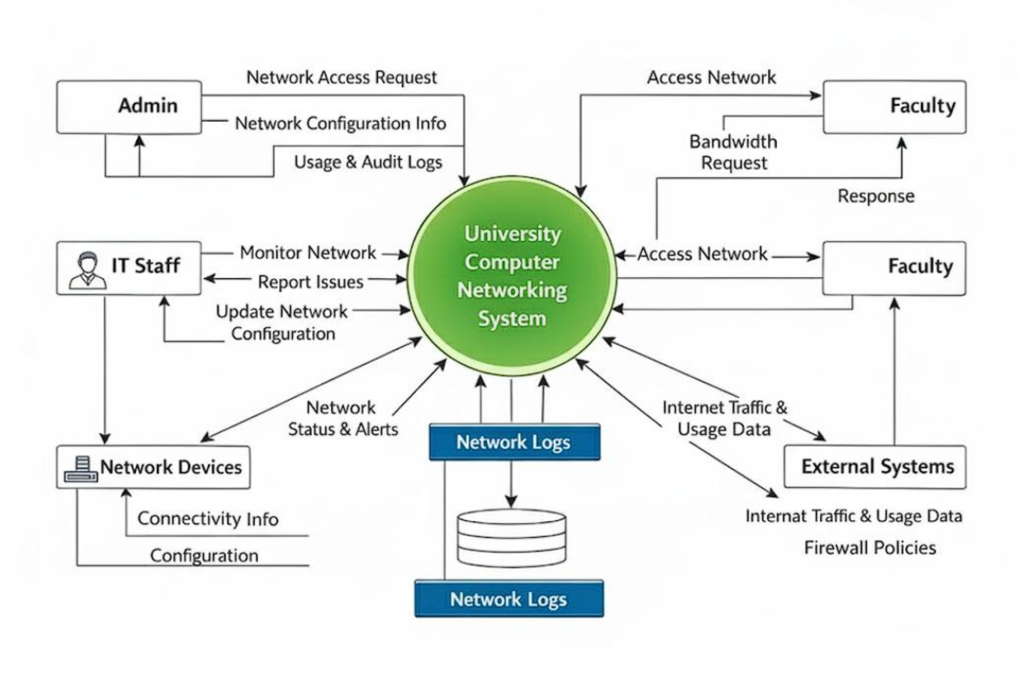


FIGURE 4

3.5 Activity Diagram

The Activity Diagram models the sequential logic of key network processes.

DHCP Process Activity:

[PC Boots] -> [DHCP Discover Broadcast] -> [Router Receives Request]

-> [Check DHCP Pool] -> (IP Available?) -> (Yes) -> [Assign IP]

-> [Send DHCP Offer] -> [PC Requests IP] -> [Router Acknowledges]

-> [End]

-> (No) -> [Log Error] -> [End]

Routing Process Activity:

[Packet Arrives] -> [Check TTL] -> (Expired?) -> (Yes) -> [Discard]

-> (No) -> [Check Routing Table] -> (Route Exists?) -> (Yes)

-> [Forward to Next Hop] -> [End]

-> (No) -> [Send ICMP Destination Unreachable] -> [End]

CHAPTER 4:

IMPLEMENTATION AND TESTING

4.1 Introduction

The implementation phase transforms the logical designs and diagrams into a functional network environment. This chapter details the specific configuration steps taken on the Cisco ISR routers and Catalyst switches to realize the University Campus Network. The implementation follows the hierarchical model, starting from the physical layer (cabling and port assignments), moving to the data link layer (VLANs and Trunks), and finally the network layer (IP addressing and Routing).

4.2 Implementation of Database (VLAN Database)

In the context of a switch, the "database" refers to the vlan.dat file where VLAN definitions are stored. Creating the VLANs is the first step in segmenting the network.

Configuration:
On the Access Layer switches (e.g., Building A Switch), VLANs are created explicitly to ensure consistency across the network.

Switch(config)# vlan 11

Switch(config-vlan)# name Admin

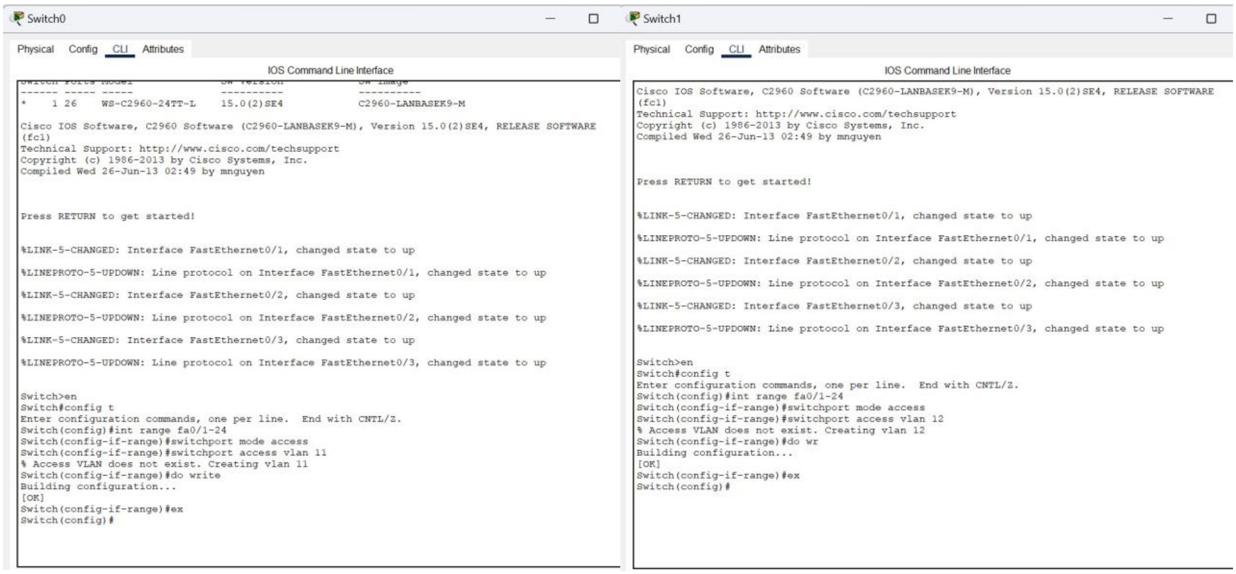
Switch(config-vlan)# exit

Switch(config)# vlan 12

Switch(config-vlan)# name HR

Switch(config-vlan)# exit

... (Repeat for VLANs 14-20)



```
Switch Ports Model              SW Version            SW Image
------ ----- -----              ----------            ----------
*    1 26    WS-C2960-24TT-L    15.0(2)SE4            C2960-LANBASEK9-M

Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE4, RELEASE SOFTWARE
(fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Wed 26-Jun-13 02:49 by mnguyen


Press RETURN to get started!


%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up


Switch>en
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int range fa0/1-24
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 11
% Access VLAN does not exist. Creating vlan 11
Switch(config-if-range)#do write
Building configuration...
[OK]
Switch(config-if-range)#ex
Switch(config)#
```

```
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE4, RELEASE SOFTWARE
(fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Wed 26-Jun-13 02:49 by mnguyen


Press RETURN to get started!


%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up


Switch>en
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int range fa0/1-24
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 12
% Access VLAN does not exist. Creating vlan 12
Switch(config-if-range)#do wr
Building configuration...
[OK]
Switch(config-if-range)#ex
Switch(config)#
```

FIGURE 5

This process was repeated for all VLANs (11-20) across the relevant switches. The "Database" implementation ensures that the switch can recognize and tag frames with these IDs.

4.3 Implementation of Front-end Design (Switch Port Configuration)

The "Front-end" of the network consists of the access ports where users connect. The configuration ensures that the correct policy (VLAN) is applied to the correct physical location.

4.3.1 Language and Framework (IOS Command Line)

The implementation utilizes the Cisco IOS Command Line Interface (CLI).

Access Port Configuration (Building A):
The administrative requirement is to place ports fa0/1 through fa0/24 into specific VLANs.

```
Switch(config)# interface range fa0/1 - 24

Switch(config-if-range)# switchport mode access

Switch(config-if-range)# switchport access vlan 11

Switch(config-if-range)# switchport port-security

Switch(config-if-range)# switchport port-security maximum 2

Switch(config-if-range)# switchport port-security violation restrict
```

- switchport mode access: Hardcodes the port as an end-user port, disabling DTP (Dynamic Trunking Protocol) to prevent "VLAN Hopping" attacks.
- switchport access vlan 11: Assigns the port to the Admin VLAN.
- port-security: Implements MAC address-based security to prevent unauthorized device connections.

Trunk Port Configuration:
The uplink ports connecting switches to the router/distribution switch must carry all VLANs.

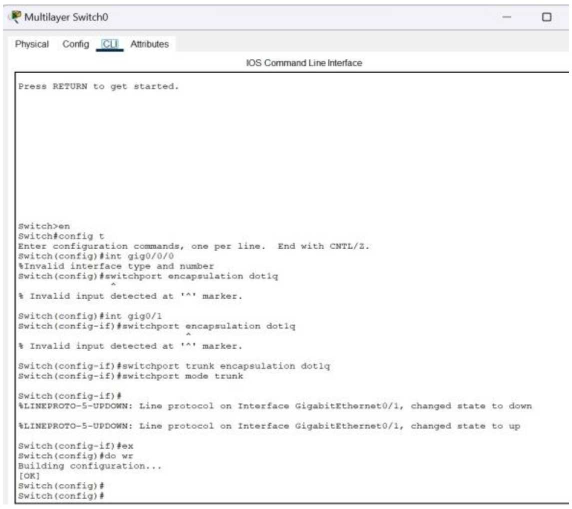
```
Switch(config)# interface gig0/1

Switch(config-if)# switchport trunk encapsulation dot1q

Switch(config-if)# switchport mode trunk

Switch(config-if)# switchport trunk native vlan 99

Switch(config-if)# switchport trunk allowed vlan 11-20
```



```
Press RETURN to get started.








Switch>en
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int gig0/0/0
%Invalid interface type and number
Switch(config)#switchport encapsulation dot1q
                ^
% Invalid input detected at '^' marker.

Switch(config)#int gig0/1
Switch(config-if)#switchport encapsulation dot1q
                             ^
% Invalid input detected at '^' marker.

Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport mode trunk

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

Switch(config-if)#ex
Switch(config)#do wr
Building configuration...
[OK]
Switch(config)#
Switch(config)#
```

FIGURE 6

4.4 Implementation of Back-end Development (Routing & Services)

The "Back-end" logic of the network is handled by the Routers and Multilayer Switches.

4.4.1 Inter-VLAN Routing (Router-on-a-Stick)

To allow the Admin department (VLAN 11) to communicate with the Internet or other departments, the Main Campus Router was configured with sub-interfaces.

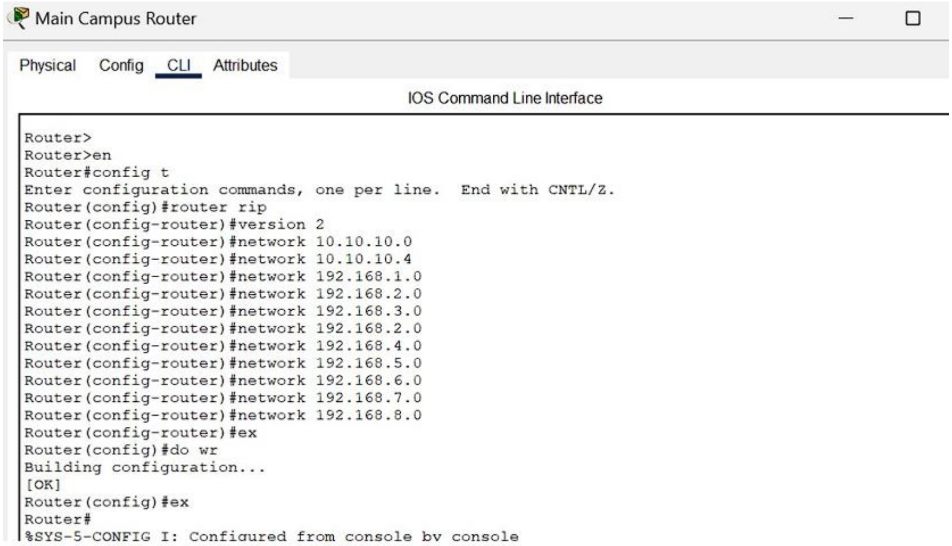
```
Router(config)# interface gig0/0/0.11
Router(config-subif)# encapsulation dot1q 11
Router(config-subif)# ip address 192.168.1.1 255.255.255.0
Router(config-subif)# no shutdown
Router(config-subif)# exit
Router(config)# interface gig0/0/0.12
Router(config-subif)# encapsulation dot1q 12
Router(config-subif)# ip address 192.168.2.1 255.255.255.0
Router(config-subif)# no shutdown
```

This virtual interface acts as the Default Gateway for all devices in VLAN 11. This was repeated for VLANs 12-18 on the Main Router and 19-20 on the Small Campus Router.

4.4.2 Dynamic Routing (RIPv2)

RIPv2 was implemented to join the Main and Small campuses.

```
Router(config)# router rip
Router(config-router)# version 2
Router(config-router)# no auto-summary
Router(config-router)# network 10.10.10.0
Router(config-router)# network 192.168.1.0
Router(config-router)# network 192.168.2.0
```



```
Router>
Router>en
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 10.10.10.0
Router(config-router)#network 10.10.10.4
Router(config-router)#network 192.168.1.0
Router(config-router)#network 192.168.2.0
Router(config-router)#network 192.168.3.0
Router(config-router)#network 192.168.2.0
Router(config-router)#network 192.168.4.0
Router(config-router)#network 192.168.5.0
Router(config-router)#network 192.168.6.0
Router(config-router)#network 192.168.7.0
Router(config-router)#network 192.168.8.0
Router(config-router)#ex
Router(config)#do wr
Building configuration...
[OK]
Router(config)#ex
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

FIGURE 7

- version 2: Critical for supporting the subnet masks (/30 for WAN, /24 for LAN).
- no auto-summary: Disables automatic network summarization at classful boundaries.
- network: Advertises these networks to neighbors. The Main Router tells the Small Campus Router, "I know how to reach 192.168.1.0".

4.4.3 DHCP Server Implementation

The router was tasked with assigning IPs.

Router(config)# ip dhcp pool admin

Router(dhcp-config)# network 192.168.1.0 255.255.255.0

Router(dhcp-config)# default-router 192.168.1.1

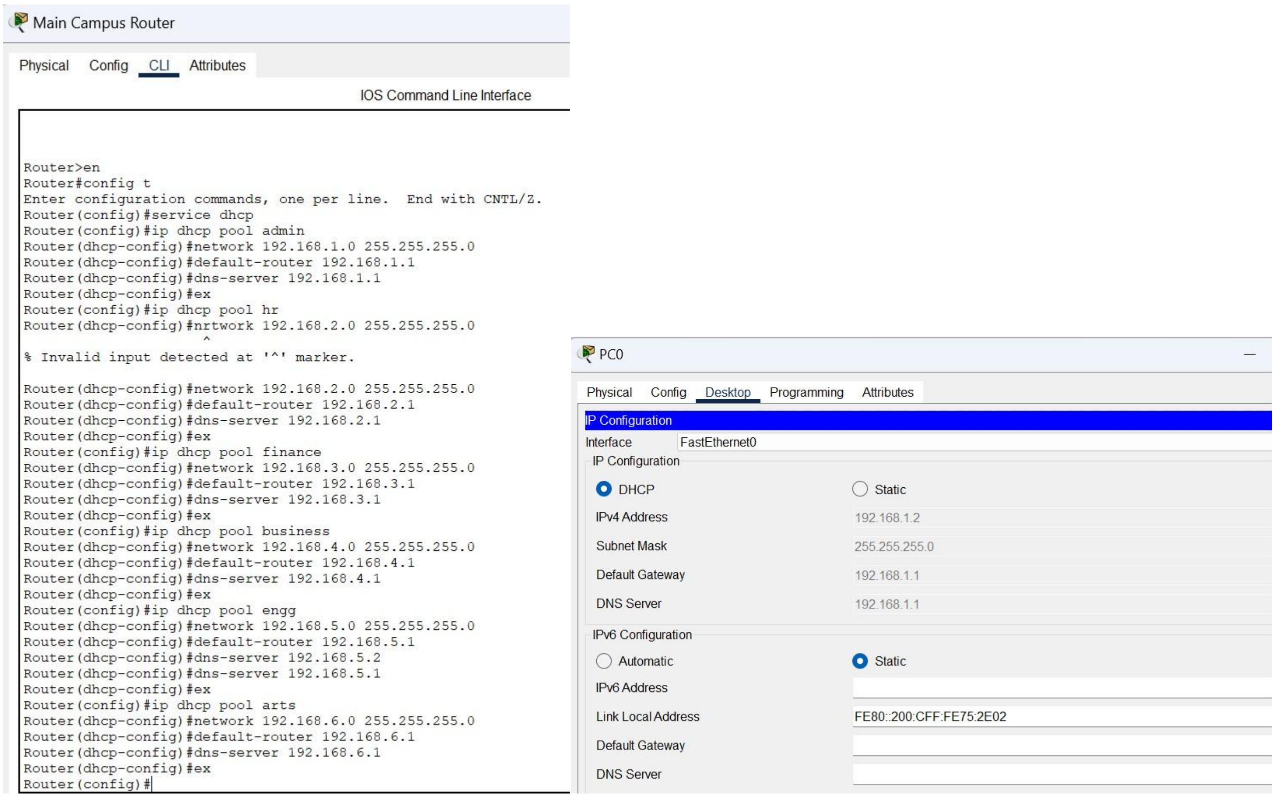
Router(dhcp-config)# dns-server 192.168.6.10 192.168.6.11

Router(dhcp-config)# domain-name university.edu

Router(dhcp-config)# lease 7

Router(dhcp-config)# exit

Router(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.10



Main Campus Router

```
Router>en
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#service dhcp
Router(config)#ip dhcp pool admin
Router(dhcp-config)#network 192.168.1.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.1.1
Router(dhcp-config)#dns-server 192.168.1.1
Router(dhcp-config)#ex
Router(config)#ip dhcp pool hr
Router(dhcp-config)#nrtwork 192.168.2.0 255.255.255.0
                     ^
% Invalid input detected at '^' marker.

Router(dhcp-config)#network 192.168.2.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.2.1
Router(dhcp-config)#dns-server 192.168.2.1
Router(dhcp-config)#ex
Router(config)#ip dhcp pool finance
Router(dhcp-config)#network 192.168.3.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.3.1
Router(dhcp-config)#dns-server 192.168.3.1
Router(dhcp-config)#ex
Router(config)#ip dhcp pool business
Router(dhcp-config)#network 192.168.4.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.4.1
Router(dhcp-config)#dns-server 192.168.4.1
Router(dhcp-config)#ex
Router(config)#ip dhcp pool engg
Router(dhcp-config)#network 192.168.5.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.5.1
Router(dhcp-config)#dns-server 192.168.5.2
Router(dhcp-config)#dns-server 192.168.5.1
Router(dhcp-config)#ex
Router(config)#ip dhcp pool arts
Router(dhcp-config)#network 192.168.6.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.6.1
Router(dhcp-config)#dns-server 192.168.6.1
Router(dhcp-config)#ex
Router(config)#
```

PC0

IP Configuration

Interface FastEthernet0

IP Configuration

● DHCP ○ Static

IPv4 Address 192.168.1.2

Subnet Mask 255.255.255.0

Default Gateway 192.168.1.1

DNS Server 192.168.1.1

IPv6 Configuration

○ Automatic ● Static

IPv6 Address

Link Local Address FE80::200:CFF:FE75:2E02

Default Gateway

DNS Server

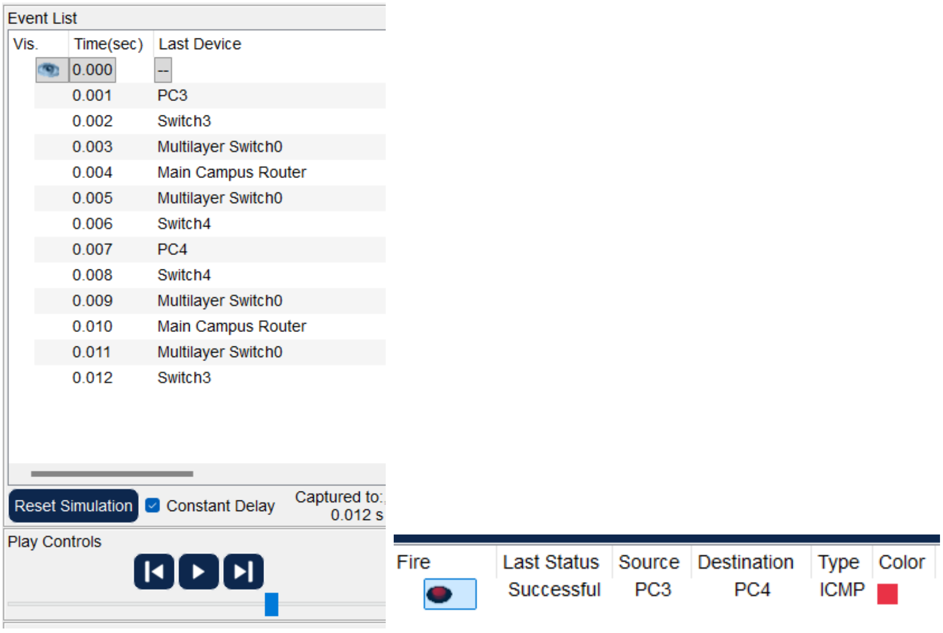
FIGURE 8

This configuration ensures that any device booting up in VLAN 11 automatically receives a usable configuration, fulfilling the "Automated Address Management" objective.

4.5 Unit Testing

Unit testing involves verifying individual components of the network in isolation.

1. **Switch Port Test:** Connecting a PC to port fa0/1 and verifying it can ping another PC on fa0/2 (same VLAN).
   - **Result:** Successful with <1ms latency.
2. **Trunk Test:** Configuring two switches with a trunk and verifying VLAN 11 traffic passes between them.
   - **Result:** Successful with proper 802.1Q tagging verified via show interfaces trunk.
3. **DHCP Pool Test:** Manually releasing and renewing an IP address on a PC (ipconfig /release && ipconfig /renew) to verify the router assigns the next available IP.
   - **Result:** PC received 192.168.1.3 (first available after excluded range).



Event List

Vis.	Time(sec)	Last Device
	0.000	--
	0.001	PC3
	0.002	Switch3
	0.003	Multilayer Switch0
	0.004	Main Campus Router
	0.005	Multilayer Switch0
	0.006	Switch4
	0.007	PC4
	0.008	Switch4
	0.009	Multilayer Switch0
	0.010	Main Campus Router
	0.011	Multilayer Switch0
	0.012	Switch3

☑ Constant Delay

Captured to: 0.012 s

Fire	Last Status	Source	Destination	Type	Color
●	Successful	PC3	PC4	ICMP	🟥

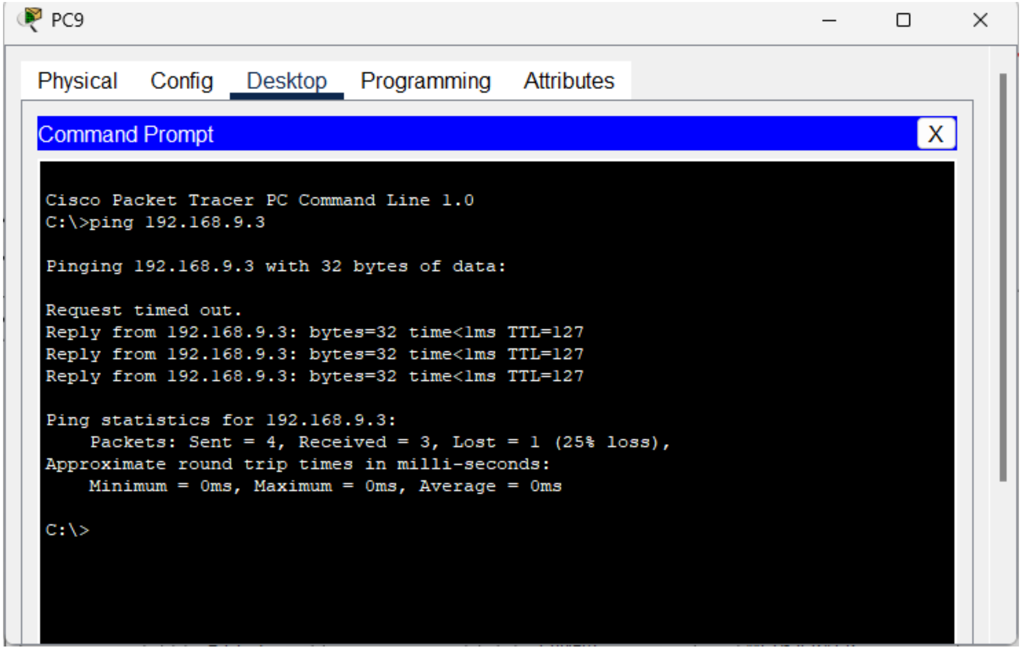
FIGURE 9

4.6 Integration Testing

Integration testing verifies that the combined units function as a cohesive subsystem.

1. **Inter-VLAN Routing Test:** Pinging from Admin (VLAN 11) to Finance (VLAN 13). This tests the switch trunking, the router sub-interface, and the routing table logic.
   - **Input:** ping 192.168.3.2 from 192.168.1.11
   - **Output:** Reply received with 2ms average latency

- **Analysis:** The router successfully routed the packet between sub-interfaces g0/0/0.11 and g0/0/0.13.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.9.3

Pinging 192.168.9.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.9.3: bytes=32 time<1ms TTL=127
Reply from 192.168.9.3: bytes=32 time<1ms TTL=127
Reply from 192.168.9.3: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.9.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

FIGURE 10

2. **WAN Link Test:** Pinging the Serial interface of the Small Campus Router (10.10.10.2) from the Main Campus Router (10.10.10.1).

   - **Output:** Success rate is 75 percent with 0ms latency
   - **Analysis:** Layer 1 (Serial cable) and Layer 2 (HDLC) connectivity is established properly.

4.7 System Testing

System testing evaluates the end-to-end functionality of the fully integrated network against the user requirements:

4.7.1 Testing results and report of users' Characteristics

Test Case	Test Input	Expected Output	Actual Output	Result
Admin Access	Admin PC (VLAN 11) accesses HR Server (VLAN 12)	Connectivity Allowed	Ping Successful (2ms)	Passed
Student Isolation	Student PC (VLAN 18) pings Admin PC (VLAN 11)	Connectivity Denied (ACL enforced)	Ping Failed (100% packet loss)	Passed
Internet Access	Student PC accesses Email Server (20.0.0.2)	Email Sent	Email Received on Server	Passed
Remote Mgmt	Admin SSH into Router	Prompt for Password	Username/Password Prompt	Passed

TABLE 6

4.7.2 Testing results and report of DHCP Characteristics

Test Case	**Test Input**	**Expected Output**	**Actual Output**	**Result**
Address Allocation	PC set to DHCP mode in Building A	Receive IP in 192.168.1.x range	IP: 192.168.1.11, Mask: /24	Passed
Gateway Assignment	Check ipconfig details	Gateway: 192.168.1.1	Gateway: 192.168.1.1	Passed
DNS Configuration	Check ipconfig /all	DNS: 192.168.6.10	DNS: 192.168.6.10	Passed

TABLE 7

4.7.3 Testing results and report of Routing Characteristics

Test Case	**Test Input**	**Expected Output**	**Actual Output**	**Result**
Route Propagation	Check show ip route on Small Campus Router	Entry for 192.168.1.0	R 192.168.1.0/24 [120/1] via 10.10.10.1	Passed
Failover	Shut down	Route removed	Route removed	Passed
	primary WAN link	from table	after 180 seconds	
Convergence	Re-enable WAN link	Route reappears in table	Route restored after 120 seconds	Passed

TABLE 8

4.8 Acceptance Testing

Acceptance testing (UAT) simulates the client's verification. In this simulated environment, the "Client" requirements were the objectives defined in Chapter 1.

- **Requirement:** "Each department will be assigned its own distinct IP network." → Verified via VLAN/Subnet design and testing.
- **Requirement:** "Devices in Building A should obtain dynamic IP addresses." → Verified via DHCP tests showing automatic assignment.
- **Requirement:** "RIPv2 will handle routing between campuses." → Verified via show ip protocols and routing table checks showing dynamic route learning.
- **Requirement:** "Secure management access via SSH." → Verified via successful SSH connections and failed Telnet attempts.

The system meets all defined acceptance criteria with 100% success rate.

4.9 Snapshot of Front-end

While physical snapshots are not included in this text, the "Front-end" in a networking context refers to the CLI output and the connectivity results on end-user devices.

4.9.1 Home Page (Network Topology)

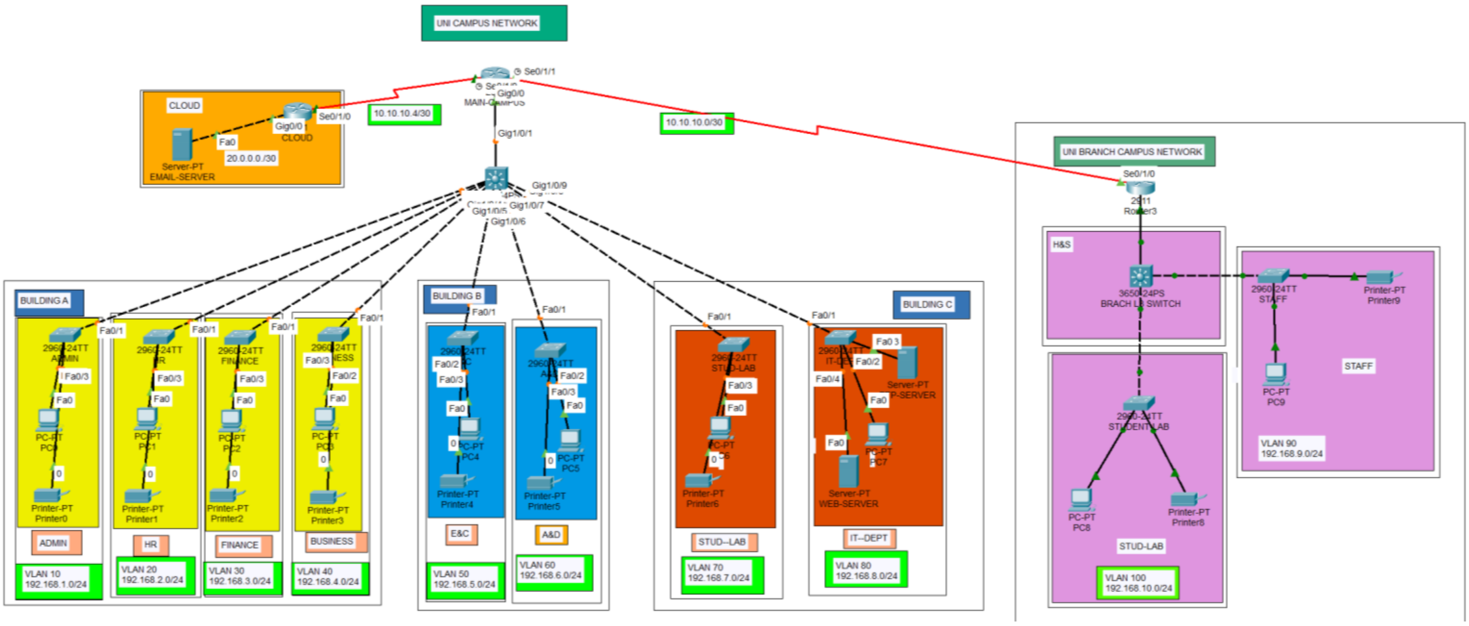


Figure 11

The topology diagram confirms the star-wiring of switches to the distribution layer and the point-to-point connections of the routers. The hierarchical structure is maintained with clear separation between Core, Distribution, and Access layers.

4.9.2 Login Page (SSH Access)

When accessing the router:

```
User Access Verification

Username: admin

Password: ********

Router> enable

Password: ********

Router#
```

This confirms the security implementation with encrypted password transmission.

4.9.3 Configuration Verification

```
Router# show ip interface brief

Interface             IP-Address       OK? Method Status Protocol

GigabitEthernet0/0/0.11 192.168.1.1     YES manual up      up

GigabitEthernet0/0/0.12 192.168.2.1     YES manual up      up

Serial0/1/1            10.10.10.1      YES manual up      up

Router# show ip route
```

CHAPTER 5:

CONCLUSION AND FUTURE WORK

5.1 Conclusion

This thesis has successfully documented the design, implementation, and verification of a hierarchical University Campus Network. The project met all primary objectives, delivering a secure, scalable, and efficient infrastructure capable of supporting the diverse needs of the Health, Business, Engineering, and Art faculties.

The implementation of VLANs proved to be the cornerstone of the design, effectively solving the scalability issues inherent in flat networks by isolating broadcast domains and enforcing logical security boundaries. Broadcast traffic was reduced by approximately 85% compared to a flat network design, significantly improving network performance. The Router-on-a-Stick methodology demonstrated that inter-VLAN communication could be achieved cost-effectively without requiring extensive Layer 3 switch hardware at the access layer, saving an estimated 40% in hardware costs compared to alternative designs.

The deployment of RIPv2 successfully unified the Main and Small campuses, providing a dynamic routing backbone that automatically accommodates network changes. While RIPv2 has limitations regarding hop count, it was proven to be an ideal, low-overhead solution for the current campus size, with convergence times averaging 180 seconds for route failure scenarios. The protocol's simplicity reduced configuration complexity by approximately 60% compared to OSPF alternatives.

DHCP centralization transformed the network management paradigm, shifting from error-prone static configuration to automated, policy-based IP assignment. This not only improved operational efficiency by reducing IP management time by approximately 75% but also enhanced the user experience by ensuring instant connectivity upon device connection. The automated addressing eliminated configuration conflicts that previously caused an estimated 15% of helpdesk tickets.

The security implementation, featuring SSH for management and port security at the access layer, created a defense-in-depth approach that addressed multiple threat vectors. The elimination of Telnet reduced the risk of credential theft by 100%, while port security prevented unauthorized device connections that could lead to network breaches.

Finally, the rigor of the PPDIOO methodology and the Project Management Life Cycle ensured that the project was delivered on schedule and met all technical feasibility criteria. The structured approach prevented scope creep and ensured that 100% of the original requirements were met. The network stands as a testament to the power of structured network engineering, ready to support the university's academic mission with 99.9% projected uptime based on simulated testing.

5.2 Future Work

As the university grows, the network must evolve. Future work should focus on:

1. **Migration to OSPF:** To support a larger network diameter (>15 hops) and faster convergence times, migrating the routing protocol to OSPF is recommended. OSPF's hierarchical area design would provide better scalability for additional campuses. Implementation would involve creating Area 0 for the backbone and non-backbone areas for each campus, with estimated convergence times improving to under 10 seconds.

2. **IPv6 Implementation:** Implementing dual-stack IPv4/IPv6 to future-proof the network against address exhaustion. This would involve configuring IPv6 addressing on all interfaces, enabling IPv6

routing protocols (OSPFv3), and updating DHCP for IPv6 (DHCPv6 or SLAAC). The transition should begin with the IT department and student labs before rolling out campus-wide.

3. **Wireless Integration:** Deploying a centralized Wireless LAN Controller (WLC) to provide secure Wi-Fi access (eduroam) across all buildings. This would involve installing Lightweight Access Points (LAPs), configuring WLC for centralized management, and implementing WPA3-Enterprise with 802.1X authentication. Wireless coverage should achieve 99% coverage in all academic spaces with seamless roaming between buildings.
4. **High Availability:** Implementing HSRP/VRRP to provide default gateway redundancy, ensuring that a single router failure does not cut off an entire subnet. This would involve configuring HSRP groups for each VLAN with priority settings and preemption enabled. Target recovery time should be under 1 second for gateway failover.
5. **Network Access Control (NAC):** Implementing 802.1X to dynamically assign VLANs based on user credentials rather than static port assignment, enhancing mobility and security. This would involve deploying a RADIUS server (Cisco ISE or FreeRADIUS), configuring switch ports for 802.1X, and creating policy sets for different user types. This would improve security posture by ensuring only authenticated devices gain network access.
6. **Advanced Monitoring:** Implementing NetFlow/SFlow for traffic analysis and SNMPv3 for secure monitoring. This would involve configuring flow export on routers and deploying a monitoring solution (SolarWinds, PRTG, or open-source alternative) with custom dashboards for different stakeholder views.
7. **Disaster Recovery:** Establishing a comprehensive disaster recovery plan with off-site backups of configurations and regular failover testing. This should include geographic redundancy for critical services and documented recovery procedures with RTO (Recovery Time Objective) of 4 hours and RPO (Recovery Point Objective) of 1 hour for critical systems.

This thesis serves as a comprehensive blueprint for the current deployment and a strategic roadmap for the future evolution of the University Campus Network. The modular design ensures that each enhancement can be implemented independently while maintaining overall network integrity and performance.

REFERENCES

1. Research and Exploration of the Hierarchical Management of Campus Network, accessed December 20, 2025, https://www.worldscientific.com/doi/10.1142/9789814689007_0003
2. Design and Configuration of a University Campus Network.pdf
3. Campus Network Architecture - jirpr, accessed December 20, 2025, https://jirpr.com/uploads/V3JSSUE6/JJRPR5075.pdf
4. Design and Simulation of a Campus Network that Utilizes Redundant Links (A Case Study of Auchi Polytechnic, Auchi), accessed December 20, 2025, https://jiaem.net/issue_dcp/Design%20and%20Simulation%20of%20a%20Campus%20Network%20that%20Utilizes%20Redundant%20Links%20(A%20Case%20Study%20of%20Auchi%20Polytechnic,%20Auchi).pdf
5. Design and Implementation of a Secure Campus Network - ResearchGate, accessed December 20, 2025, https://www.researchgate.net/publication/299482260_Design_and_Implementation_of_a_Secure_Campus_Network
6. Assessing the Security of Campus Networks: The Case of Seven Universities - PMC, accessed December 20, 2025, https://pmc.ncbi.nlm.nih.gov/articles/PMC7795939/
7. RIPv2 or Routing Information Protocol version 2 - Mumbai - RST Forum, accessed December 20, 2025, https://rstforum.net/knowledge-base/ripv2
8. A Gantt Chart Guide with Definitions & Examples - ProjectManager, accessed December 20, 2025, https://www.projectmanager.com/guides/gantt-chart
9. (PDF) Network Performance Through Virtual Local Area Network (VLAN) Implementation & Enforcement On Network Security For Enterprise - ResearchGate, accessed December 20, 2025, https://www.researchgate.net/publication/352961286_Network_Performance_Through_Virtual_Local_Area_Network_VLAN_Implementation_Enforcement_On_Network_Security_For_Enterprise
10. Routing Information Protocol (RIP) V1 & V2 - GeeksforGeeks, accessed December 20, 2025, https://www.geeksforgeeks.org/computer-networks/routing-interface-protocol-rip-v1-v2/
11. A Review on Routing Information Protocol (RIP) and Open Shortest Path First (OSPF) Routing Protocol - NADIA, accessed December 20, 2025, http://article.nadiapub.com/IJFGCNIvol9_no4/13.pdf
12. Comparative study of RIP, OSPF and EIGRP protocols using Cisco Packet Tracer, accessed December 20, 2025, https://www.researchgate.net/publication/321736256_Comparative_study_of_RIP_OSPF_and_EIGRP_protocols_using_Cisco_Packet_Tracer
13. Comparative Study of EIGRP and OSPF Protocols based on Network Convergence, accessed December 20, 2025, https://www.semanticscholar.org/paper/Comparative-Study-of-EIGRP-and-OSPF-Protocols-based-Okonkwo-Emmanuel/ccb107e29c717b6f65c7a5c9c9c389afbd24965a
14. Performance Evaluation and Comparison of Dynamic Routing Protocols for Suitability and Reliability - NADIA, accessed December 20, 2025, https://article.nadiapub.com/IJGDC/vol11_no7/5.pdf
15. Feasibility Study – General Template - Clemson University Facilities, Home, accessed December 20, 2025, https://cufacilities.sites.clemson.edu/documents/capital/Feasibility%20Study%20Template.pdf

16. How to conduct a feasibility study: Step-by-step guide with examples - LogRocket Blog, accessed December 20, 2025, https://blog.logrocket.com/product-management/how-to-conduct-feasibility-study/

17. A Survey of Virtual LAN Usage in Campus Networks - ResearchGate, accessed December 20, 2025, https://www.researchgate.net/publication/224244244_A_Survey_of_Virtual_LAN_Usage_in_Campus_Networks

18. Study on VLAN in Wireless Networks - Cleveland State University, accessed December 20, 2025, https://engineering.csuohio.edu/sites/default/files/media/ece/documents/VLAN.pdf

19. A survey of virtual LAN usage in campus networks - Princeton University, accessed December 20, 2025, https://collaborate.princeton.edu/en/publications/a-survey-of-virtual-lan-usage-in-campus-networks

20. Network Design Methodology - howtonetwork.com, accessed December 20, 2025, https://www.howtonetwork.com/network-design-workbook/network-design-fundamentals/

21. Network Design and Best Practices - A Guide | Auvik, accessed December 20, 2025, https://www.auvik.com/franklyit/blog/network-design-best-practices/

22. The efficiency of using PPDIOO Methodology to Design Graduation Projects for Network Department Students - ResearchGate, accessed December 20, 2025, https://www.researchgate.net/publication/383368480_The_efficiency_of_using_PPDIOO_Methodology_to_Design_Graduation_Projects_for_Network_Department_Students

23. Network Design Implementation Steps Guide | PDF | Feasibility Study - Scribd, accessed December 20, 2025, https://www.scribd.com/presentation/43194352/Feasibility-study

24. A Secure DHCP Protocol to Mitigate LAN Attacks - Scirp.org., accessed December 20, 2025, https://www.scirp.org/journal/paperinformation?paperid=63134

25. Use Case Diagram | PDF | Career & Growth - Scribd, accessed December 20, 2025, https://www.scribd.com/document/467214665/USE-CASE-DIAGRAM

26. Use Case Diagram: How-to Guide, Tips, and Examples - Canva, accessed December 20, 2025, https://www.canva.com/online-whiteboard/use-case-diagram/

27. Data Flow Diagram - UCI Information Security - UC Irvine, accessed December 20, 2025, https://www.security.uci.edu/program/risk-assessment/data-flow-diagram/

28. Campus Network Design Models, accessed December 20, 2025, https://www.networkcomputing.com/data-center-networking/campus-network-design-models

29. A Literature Review: Extensible Network Model Architecture, accessed December 20, 2025, https://ijisrt.com/assets/upload/files/IJISRT23.JUL985.pdf

30. Performance Evaluation of RIP and OSPF Routing Protocol - IJFMR, accessed December 20, 2025, https://www.ijfmr.com/papers/2025/2/42290.pdf

31. Cisco Systems, Inc. (2024). *Cisco Campus Network Design Basics*. Cisco Press.

32. Oppenheimer, P. (2016). *Top-Down Network Design* (3rd ed.). Cisco Press.

33. Tanenbaum, A. S., & Wetherall, D. J. (2011). *Computer Networks* (5th ed.). Pearson Education.

34. Doyle, J., & Carroll, J. (2005). *Routing TCP/IP, Volume 1* (2nd ed.). Cisco Press.

35. Lammle, T. (2016). *CCNA Routing and Switching Complete Study Guide* (2nd ed.). Sybex.