**UNIVERSITY NETWORK ARCHITECTURE**

A project report submitted

in partial fulfillment of requirement for the award of degree

**BACHELOR OF TECHNOLOGY**

in

**COMPUTER SCIENCE ENGINEERING**

by

**CHANDAN RAJ 2203A53020**

Under the guidance of

## Dr. T Sampath Kumar

Assistant Professor, Department of CSE.

**Department of CS&AI**

****

Ananthasagar, Warangal.

**SR UNIVERSITY**

Ananthasagar, Warangal-506371.



**CERTIFICATE**

This is to certify that this project entitled **“UNIVERSITY NETWORK ARCHITECTURE**" is the bonafide work carried out by **Chandan Raj** as a project for the partial fulfillment to award the degree **BACHELOR OF TECHNOLOGY** in **CS&AI** during the academic year 2024-2025 under our guidance and Supervision.

## Dr. T Sampath Kumar Dr. Sheshikala Martha

Assistant Professor Prof. & HOD (CS&AI),

SR University, SR University,

Ananthasagar, Warangal. Ananthasagar, Warangal.

**ACKNOWLEDGEMENT**

We wish to take this opportunity to express our sincere gratitude and deep sense of respect to our beloved Vice Chancellor, **Prof. DEEPAK GARG,** for his continuous support and guidance to complete this project in the institute.

We would like to extend our gratitude to **Dr. Indrajeet Gupta**, **Professor,** the Dean of the School of Engineering, and **Dr. Sheshikala Martha**, **Professor** and Head of the CS&AI Department, for their encouragement and support.

We owe an enormous debt of gratitude to our project guide **Dr. T. Sampath Kumar, Asst. Prof.,** for guiding me from the beginning through the end of the project with his intellectual advices and insightful suggestions. I truly value his consistent feedback on my progress, which was always constructive, encouraging and ultimately drove us to the right direction.

Finally, I express my thanks to all the teaching and non-teaching staff of the department for their suggestions and timely support.

**ABSTRACT**

In modern educational institutions, reliable and secure networking infrastructure is critical for academic operations, research, administration, and wireless access. This project implements a university-wide network architecture in Cisco Packet Tracer, integrating VLANs, inter-VLAN routing, DHCP services, ACLs, and wireless connectivity to create a segmented and secure network environment. The design ensures optimized communication between departments and controlled access to sensitive resources, aligned with best practices in network security and management.

**CONTENTS**

|  |  |
| --- | --- |
| ***ACKNOWLEDGEMENT ABSTRACT*** | ***i ii*** |
| **Chapter No. Title** | **Page No.** |
| **1. INTRODUCTION** | **04** |
| 1.1 OVERVIEW OF PROJECT | 04 |
| **2. LITERATURE SURVEY** | **05** |
| 2.1 EXISTING METHODS | 05 |
| 2.2 MOTIVATION AND SCOPE OF THE WORK | 05 |
| 2.3 PROBLEM STATEMENT | 06 |
| **3. PROPOSED METHODOLOGY** | **07** |
| 3.1 INTRODUCTION TO METHODOLOGY | 07 |
| 3.2 THEORETICAL FRAMEWORK | 07 |
| 3.3 COMMAND SET | 07 |
| 3.4 DESIGN | 11 |
| 3.5 EXPERIMENTAL SETUP | 13 |
| 3.6 ANALYSIS OF RESULTS | 13 |
| **4. CONCLUSION** | **15** |
| 4.1 CONCLUSION | 15 |
| 4.2 FUTURE SCOPE | 15 |

1. **INTRODUCTION**

# OVERVIEW

Universities are complex institutions that consist of multiple departments, faculties, administrative units, libraries, laboratories, and common areas. Each of these entities has distinct access needs, security policies, and communication patterns. To ensure smooth and secure operation across such a diverse environment, a well-designed network architecture is essential. This project aims to develop a scalable, secure, and logically segmented network infrastructure for a university using Cisco Packet Tracer. The core idea is to divide the university network into multiple Virtual LANs (VLANs) — including Admin, Students, Library, and Wireless — to isolate broadcast domains, reduce network congestion, and enhance security. Each VLAN represents a functional department or user group, allowing for independent traffic management and policy enforcement.

To enable communication between VLANs, inter-VLAN routing is implemented using a Layer 3 switch or router. This ensures that only authorized traffic passes between different departments, enhancing control and data integrity. Additionally, Dynamic Host Configuration Protocol (DHCP) is configured to automate IP address assignment within each VLAN, minimizing manual errors and improving scalability. Access Control Lists (ACLs) are integrated to enforce security by defining which devices or VLANs are permitted to access specific resources. For instance, student VLANs can be restricted from accessing administrative or confidential segments of the network.

The network also simulates wireless connectivity, allowing mobile or BYOD (Bring Your Own Device) users — such as students and staff — to connect seamlessly. These wireless clients are assigned dynamic IPs and logically integrated into the network while still maintaining appropriate security boundaries. This architecture mirrors the requirements of a real-world university: scalable, efficient, secure, and easy to manage. The project highlights practical networking skills, network segmentation strategies, and the importance of network simulation tools in academic environments.

1. **LITERATURE SURVEY**

# EXISTING METHODS

Traditional campus networks often followed a flat or unsegmented design, where all devices operated within a single broadcast domain. This approach led to frequent broadcast storms, performance degradation, and a lack of control over internal traffic flow. As universities expanded their digital infrastructure, this model proved inefficient and insecure. Unauthorized access, inefficient bandwidth use, and insufficient traffic isolation became significant concerns. With the introduction of Virtual LANs (VLANs) and Layer 3 switching, a new paradigm emerged — one where departments could be virtually separated within the same physical infrastructure. VLANs enabled logical segmentation, reducing congestion and improving security. Inter-VLAN routing further facilitated controlled communication between these segments. These technologies became essential in environments requiring role-based access, such as academic institutions, where administration, faculty, students, and guests require varying levels of access.

# MOTIVATION AND SCOPE OF THE WORK

The primary motivation for this project lies in the need to develop a scalable and secure network infrastructure tailored to a university environment. Modern campuses handle thousands of concurrent users with diverse needs, and manual IP allocation or lack of segmentation is not feasible. This project focuses on creating a realistic network simulation using Cisco Packet Tracer, integrating enterprise-level techniques such as VLAN-based segmentation, dynamic IP allocation using DHCP, traffic control through ACLs, and wireless access points. The scope extends to simulating a working model of this network, validating its reliability, security, and ease of management — key goals for any educational institution’s digital infrastructure.

# PROBLEM STATEMENT

To design and simulate a logically segmented and secure university network that ensures efficient communication and resource access using VLANs, inter-VLAN routing, DHCP, ACL-based traffic control, and wireless access. The entire architecture will be implemented within Cisco Packet Tracer, mirroring real-world network deployment scenarios in academic environments.

1. **PROPOSED METHODOLOGY**

# INTRODUCTION TO METHODOLOGY

The proposed university network is built by segmenting various user groups into dedicated VLANs, representing Admin, Students, Library, and Wireless devices. These VLANs logically isolate departments, ensuring that unnecessary traffic doesn't propagate across unrelated domains. Each VLAN has its own subnet and DHCP scope. To enable communication between VLANs when necessary, inter-VLAN routing is configured using a Layer 3 switch or router. For security, Access Control Lists (ACLs) are applied on routing interfaces to allow or deny traffic between VLANs based on organizational policies. A wireless router is included to support mobile users, especially students, who rely on wireless connectivity. The configuration is entirely simulated in Cisco Packet Tracer, allowing for rigorous testing and validation without requiring real hardware.

# THEORETICAL FRAMEWORK

Below are the core concepts and technologies utilized in the proposed design:

VLANs (Virtual LANs): Logically divide the network into segments, each with a specific purpose or user group.

Inter-VLAN Routing: Facilitates communication between VLANs via Layer 3 routing.

DHCP (Dynamic Host Configuration Protocol): Automatically assigns IP addresses to devices within each VLAN to streamline device onboarding.

ACLs (Access Control Lists): Enforce traffic restrictions to prevent unauthorized access between VLANs.

RIP v2 (Routing Information Protocol version 2): Provides dynamic routing updates across the router's interfaces.

**COMMAND SET:**

**VLAN Configuration on Switch**

enable

configure terminal

vlan 10

name ADMIN

exit

vlan 20

name STUDENT

exit

vlan 30

name LIBRARY

exit

vlan 40

name WIRELESS

exit

interface range fa0/1 - 3

switchport mode access

switchport access vlan 10

exit

interface range fa0/4 - 6

switchport mode access

switchport access vlan 20

exit

interface range fa0/7 - 8

switchport mode access

switchport access vlan 30

exit

interface range fa0/9 - 10

switchport mode access

switchport access vlan 40

exit

interface gig0/1

switchport mode trunk

exit

**Router Interface Configuration for Inter-VLAN Routing (Router-on-a-Stick)**

enable

configure terminal

interface gig0/0.10

encapsulation dot1Q 10

ip address 192.168.10.254 255.255.255.0

exit

interface gig0/0.20

encapsulation dot1Q 20

ip address 192.168.20.254 255.255.255.0

exit

interface gig0/0.30

encapsulation dot1Q 30

ip address 192.168.30.254 255.255.255.0

exit

interface gig0/0.40

encapsulation dot1Q 40

ip address 192.168.40.254 255.255.255.0

exit

interface gig0/0

no shutdown

exit

**RIP v2 Configuration**

enable

configure terminal

router rip

version 2

no auto-summary

network 192.168.10.0

network 192.168.20.0

network 192.168.30.0

network 192.168.40.0

**DHCP Configuration**

enable

configure terminal

ip dhcp pool ADMIN

network 192.168.10.0 255.255.255.0

default-router 192.168.10.254

dns-server 8.8.8.8

exit

ip dhcp pool STUDENT

network 192.168.20.0 255.255.255.0

default-router 192.168.20.254

dns-server 8.8.8.8

exit

ip dhcp pool LIBRARY

network 192.168.30.0 255.255.255.0

default-router 192.168.30.254

dns-server 8.8.8.8

exit

ip dhcp pool WIRELESS

network 192.168.40.0 255.255.255.0

default-router 192.168.40.254

dns-server 8.8.8.8

exit

ip dhcp excluded-address 192.168.10.1 192.168.10.10

ip dhcp excluded-address 192.168.20.1 192.168.20.10

ip dhcp excluded-address 192.168.30.1 192.168.30.10

ip dhcp excluded-address 192.168.40.1 192.168.40.10

**Wireless Router Configuration (GUI Steps in Packet Tracer)**

Go to the **GUI** tab of the wireless router.

Set **SSID** to UniversityWiFi

Set **Wireless Security**:

Mode: WPA2-PSK

Passphrase: university123

LAN IP Address: 192.168.40.1

Enable **DHCP**:

Start IP: 192.168.40.11

End IP: 192.168.40.100

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.40.1

# DESIGN

* **VLAN 10**: Admin Department
* **VLAN 20**: HR Department
* **VLAN 30**: Finance
* **VLAN 40**: Bussiness
* **Layer 3 Switch / Router**: Enables inter-VLAN routing and hosts ACLs
* **DHCP Server**: Provides IP addresses dynamically per VLAN
* **VLAN 50 – Electronics and Computer Department.**
* **VLAN 60 – Arts and Design**
* **VLAN 70 – Student Lab**
* **VLAN 80 – IT department**
* **VLAN 90 – Staff.**
* **VLAN 100 – Student library**

In this proposed model or architecture, the university network is structured to reflect a real-world institutional setup, emphasizing logical segmentation, security, scalability, and ease of management. The entire network is distributed across two physical campuses: the Main Campus and the Branch Campus. These campuses are interconnected and internally divided using VLANs (Virtual Local Area Networks), which play a vital role in isolating network traffic by department or function, reducing unnecessary broadcast traffic, and enforcing access control policies.

The Main Campus is composed of three primary buildings—A, B, and C—each hosting specific departments assigned to unique VLANs. Building A is dedicated to the administrative core of the university. Here, VLAN 10 is allocated to the Admin Department, which requires full network access across various segments for managing overall university operations. VLAN 20 is designated for the HR Department, which handles employee records and internal policies, necessitating secure and restricted access to internal systems. VLAN 30 is for the Finance Department, where sensitive financial data and transaction systems reside, making security and isolation a top priority. VLAN 40 supports the Business Department, where academic and business-related activities take place. This department needs reliable access to both internal learning resources and external educational platforms.

Building B focuses more on the academic and creative aspects of the university. VLAN 50 is reserved for the Electronics and Computer Department, which demands high-performance networking to accommodate practical sessions, software development, and testing environments. Next, VLAN 60 supports the Arts and Design Department, where users engage in multimedia production, design projects, and creative work that require stable connectivity and access to design tools while maintaining controlled internet usage.

Building C is oriented toward student-centric and IT support functions. VLAN 70 is assigned to the Student Lab, where students work on academic projects. It is configured to allow access to essential resources while maintaining strict access control to avoid interference with other VLANs. VLAN 80 is dedicated to the IT Department, which acts as the backbone of the entire network. This department requires elevated access to every VLAN for support, troubleshooting, and monitoring, making it a critical part of the infrastructure.

The Branch Campus, though smaller, is equally important. It consists of a single building named Honors and Science, which includes two key departments. VLAN 90 is for the Staff Department, which is responsible for administrative and academic operations at the branch level. It is configured to communicate securely with the main campus while being protected from unauthorized access. VLAN 100 is dedicated to the Student Library, a common access zone where students can explore digital resources, academic databases, and limited internet content in a secure environment.

The entire network architecture relies on a Layer 3 Switch or Router to handle inter-VLAN routing. This enables different VLANs to communicate when necessary while enforcing strict access policies. For example, the IT VLAN may need to interact with the Admin or Lab VLANs, but such access is tightly controlled using Access Control Lists (ACLs). These ACLs help in defining which VLANs can interact with others, thereby ensuring the security of sensitive departments like Finance and HR.

A centralized DHCP server is used to assign IP addresses dynamically to each device connected to the network. This reduces administrative overhead and simplifies device configuration. Each VLAN is associated with a specific DHCP pool, ensuring that devices receive appropriate IP configurations automatically based on their VLAN assignment.

Overall, this university network architecture is not only practical but also mirrors real-world campus networking scenarios. It supports security by isolating departments, improves manageability through logical segmentation, and allows for future scalability. The use of VLANs, inter-VLAN routing, ACLs, and dynamic IP addressing via DHCP ensures a robust and efficient network, capable of supporting the diverse needs of a modern educational institution.

# EXPERIMENTAL SETUP

**Simulation Tool**: Cisco Packet Tracer (version supporting L3 switches)

**Devices Used**:

Layer 2 and Layer 3 Switches

Routers with RIP support

Wireless Router

End-user devices (PCs, printer)

**Cable Types**:

Copper straight-through for switch to device

Copper cross-over for switch to router

**Configuration Mode**: CLI and GUI hybrid approach

**Validation Tools**:

ping: Test connectivity

tracert: Check route path

ipconfig: Verify IP assignment

show vlan, show ip route, show access-lists: Check setup status

# ANALYSIS OF RESULTS

* VLAN Segmentation: Verified that devices in different VLANs cannot communicate unless permitted.
* DHCP Functionality: Devices in all VLANs obtained correct IP addresses automatically.
* ACL Enforcement: Student VLANs were successfully denied access to Admin VLANs, while communication to Library was permitted.
* Wireless Integration: Wireless clients were able to obtain IPs and access both the internet and intranet as per rules.
* Routing: RIP v2 correctly propagated networks among routing devices, ensuring consistent connectivity.
* Network Efficiency: Reduced broadcast domains, improved performance, and easier troubleshooting.

1. **CONCLUSION**

# CONCLUSION

This project successfully simulated a comprehensive university network using industry-standard networking principles and simulation tools. The use of VLANs provided effective segmentation, while DHCP automation reduced manual IP management overhead. With ACLs, fine-grained access control was achieved, ensuring security between departments. Wireless connectivity extended the usability of the network to mobile users, simulating a modern university environment. The design is modular, scalable, and secure, aligning with best practices in enterprise networking.

# FUTURE SCOPE

**Real Server Integration**: Adding DNS, Web, or FTP servers for service simulation.

**IPv6 Adoption**: Future-proofing the network for next-gen internet protocols.

**Load Balancing and Redundancy**: Ensuring high availability and fault tolerance.

**Firewall Deployment**: Enabling more advanced packet filtering and deep packet inspection.

**QoS and Bandwidth Control**: Prioritizing traffic and managing network load during high usage