Project Report
On
Computer Networking: Concepts
(CSE3751)

University Network Design & Implementation

Submitted by:

Name:	Regd. No.:
Name:	Regd. No.:
Name:	Regd. No.:
Name:	Regd. No.:
Name:	Regd. No.:

B. Tech. CSE 5th Semester (Section)

INSTITUTE OF TECHNICAL EDUCATION AND RESEARCH
(FACULTY OF ENGINEERING)
SIKSHA 'O' ANUSANDHAN (DEEMED TO BE UNIVERSITY),
BHUBANESWAR, ODISHA

Declaration

We, the undersigned students of B. Tech. of **(CSE)** Department hereby declare that we own the full responsibility for the information, results etc. provided in this PROJECT titled "**(University Network Design & Implementation)**" submitted to **Siksha 'O' Anusandhan (Deemed to be University), Bhubaneswar** for the partial fulfillment of the subject **Computer Networking: Concepts (CSE 3751)**. We have taken care in all respect to honor the intellectual property right and have acknowledged the contribution of others for using them in academic purpose and further declare that in case of any violation of intellectual property right or copyright we, as the candidate(s), will be fully responsible for the same.

Name: Regd. No.:

Name: Regd. No.:

Name: Regd. No.:

Name: Regd. No.:

Name: Regd. No.:

Date: 26/12/2025

Place: Bhubaneswar

Abstract

In modern educational institutions, efficient and secure communication between departments is critical for academic and administrative operations. This project focuses on the design and implementation of a scalable and secure university campus network using Cisco Packet Tracer. The network follows a three-tier hierarchical architecture consisting of core, distribution, and access layers. VLANs are implemented to logically separate departments such as CSE, ECE, Mechanical, Civil, Administration, Library, and Server Farm. Inter-VLAN routing is achieved using a multilayer core switch. Centralized services including DHCP, DNS, Web, FTP, and Mail servers are deployed to provide essential network services. OSPF is implemented as a dynamic routing protocol to ensure efficient route exchange, while NAT is configured to provide internet access. Security is enhanced through the use of Access Control Lists (ACLs) and Spanning Tree Protocol (STP). The project successfully demonstrates a real-world enterprise campus network design with reliability, scalability, and security.

Contents

1. Introduction

Computer networks form the backbone of modern educational institutions by enabling seamless communication, data sharing, and centralized resource management. A university campus typically consists of multiple departments, administrative offices, libraries, and server rooms, all requiring secure and reliable connectivity.
This project presents the design and implementation of a university campus network using Cisco Packet Tracer. The network is structured using a three-tier hierarchical architecture to ensure scalability and performance. Logical segmentation is achieved using VLANs, while routing and centralized services ensure efficient communication. The project reflects real-world enterprise networking practices.

2. Problem Statement

I. Design and implement a fully functional campus-wide network for a university that spans multiple academic buildings and administrative blocks. The network should support segmentation, inter department routing, essential services, and internet access for all authorised users.

II. • Logical separation of departments
III. • Secure inter-department communication
IV. • Centralized server infrastructure
V. • Internet access for all users
VI. • Prevention of network loops
VII. • Access control to sensitive resources
VIII. • Implementation limited to Cisco Packet Tracer
IX. • Simulated internet connectivity
X. • No physical hardware deployment

3. Methodology

Topology Design
A three-tier hierarchical topology was designed consisting of:

- Edge Router (Internet access and NAT)
- Core Router (Backbone routing)
- Core Switch (Inter-VLAN routing)
- Distribution and Access switches

VLAN Implementation
Separate VLANs were created for each department to reduce broadcast traffic and enhance security.

IP Addressing
Each VLAN was assigned a unique /24 subnet. /30 subnetting was used for point-to-point WAN links.

Routing Configuration

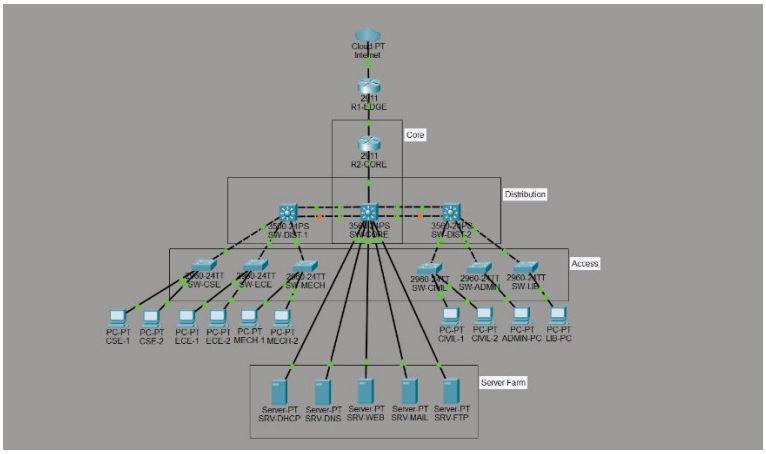
- Inter-VLAN routing using SVIs
- OSPF dynamic routing protocol
- Static routes replaced with OSPF for scalability

Server Configuration

- DHCP for dynamic IP assignment
- DNS for name resolution
- Web, FTP, and Mail servers for application services

Security Implementation

- STP for loop prevention
- PortFast on access ports
- Extended ACLs to restrict unauthorized access




```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface g0/1
Router(config-if)# ip address 10.0.0.1 255.255.255.252
Router(config-if)# no shutdown

Router(config-if)#exit
Router(config)#end
Router#wr
Building configuration...
[OK]
Router#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

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

%SYS-5-CONFIG_I: Configured from console by console
```

```
R2-CORE#enable
R2-CORE#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2-CORE(config)#interface g0/1
R2-CORE(config-if)# ip address 192.168.99.2 255.255.255.0
R2-CORE(config-if)# no shutdown

R2-CORE(config-if)#exit
R2-CORE(config)#end
R2-CORE#wr
Building configuration...
[OK]
R2-CORE#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

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

4. Results and Interpretation

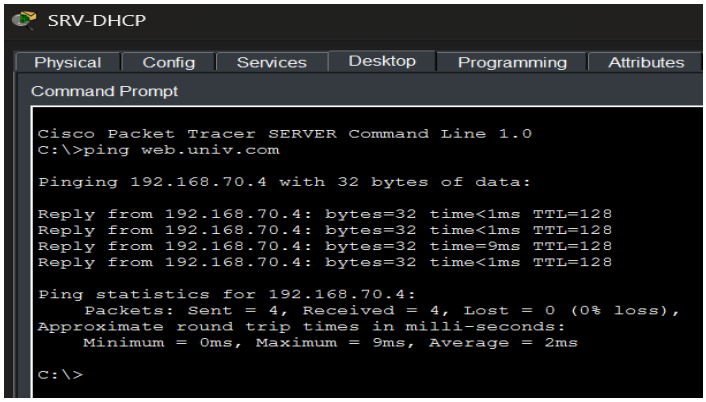
VLAN ID	VLAN Name	Network Address	Subnet Mask	CIDR	Default Gateway	Usable IP Range	Broadcast Address
10	CSE	192.168.10.0	255.255.255.0	/24	192.168.10.1	192.168.10.2 – 192.168.10.254	192.168.10.255
20	ECE	192.168.20.0	255.255.255.0	/24	192.168.20.1	192.168.20.2 – 192.168.20.254	192.168.20.255
30	MECH	192.168.30.0	255.255.255.0	/24	192.168.30.1	192.168.30.2 – 192.168.30.254	192.168.30.255
40	CIVIL	192.168.40.0	255.255.255.0	/24	192.168.40.1	192.168.40.2 – 192.168.40.254	192.168.40.255
50	ADMIN	192.168.50.0	255.255.255.0	/24	192.168.50.1	192.168.50.2 – 192.168.50.254	192.168.50.255
60	LIB	192.168.60.0	255.255.255.0	/24	192.168.60.1	192.168.60.2 – 192.168.60.254	192.168.60.255
70	SERVER	192.168.70.0	255.255.255.0	/24	192.168.70.1	192.168.70.2 – 192.168.70.254	192.168.70.255

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server
LIB	192.168.60.1	192.168.70.3	192.168.60.10	255.255.255.0	50	0.0.0.0
ADMIN	192.168.50.1	192.168.70.3	192.168.50.10	255.255.255.0	50	0.0.0.0
CIVIL	192.168.40.1	192.168.70.3	192.168.40.10	255.255.255.0	100	0.0.0.0
MECH	192.168.30.1	192.168.70.3	192.168.30.10	255.255.255.0	100	0.0.0.0
ECE	192.168.20.1	192.168.70.3	192.168.20.10	255.255.255.0	100	0.0.0.0
CSE	192.168.10.1	192.168.70.3	192.168.10.10	255.255.255.0	100	0.0.0.0

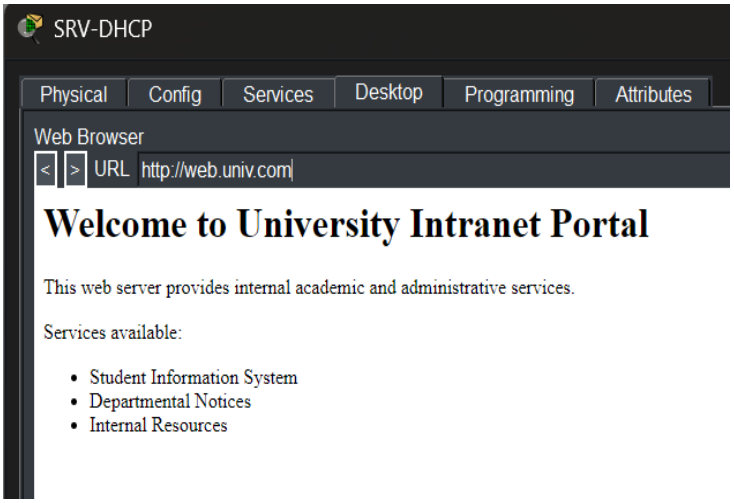
DHCP Pools

No.	Name	Type	Detail
0	dhcp.univ.com	A Record	192.168.70.2
1	dns.univ.com	A Record	192.168.70.3
2	ftp.univ.com	A Record	192.168.70.6
3	mail.univ.com	A Record	192.168.70.5
4	web.univ.com	A Record	192.168.70.4

DNS Records

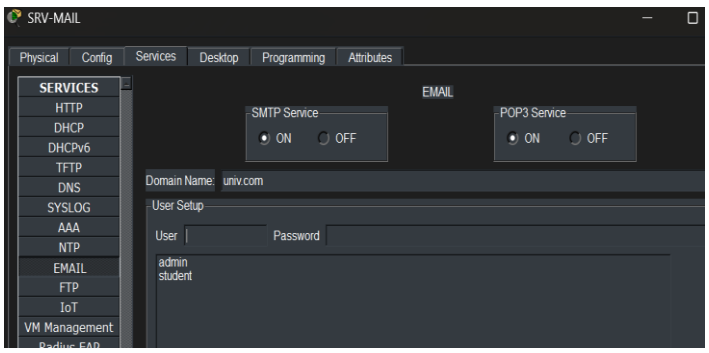


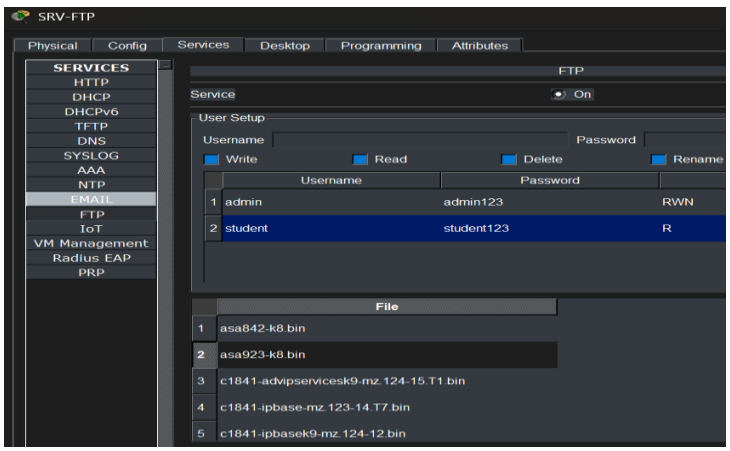
Ping test



Webserver Success

Mail Server Configuration and FTP Config





5. Conclusion

The university campus network was successfully designed and implemented using Cisco Packet Tracer. The project achieved all intended objectives including network segmentation, routing efficiency, centralized service deployment, redundancy, and security. The use of VLANs, OSPF, NAT, and ACLs ensures scalability and robustness. This project demonstrates practical knowledge of enterprise-level networking concepts and provides a strong foundation for real-world network design and implementation.

6. References

(as per the IEEE recommendations)

[1] CompTIA Network+ N10-008 Certification Guide by Glen D. Singh, 2*nd* Edition, Packt publication.

[2] Cisco Networking Academy, *Introduction to Networks*.

[3] Kurose, J. F., Ross, K. W., *Computer Networking: A Top-Down Approach*, Pearson.