FINAL PROFESSIONAL REPORT

Smart Campus Network with Internet Simulation, Firewall & NAT Security

Course: Computer Communications Networks – CS-327

Group Members: *CS-23110 Areeba Khan, CS-23104 Zara Akram*

1. Introduction

The purpose of this project is to design, implement, and analyze a **secure Smart Campus Network** using **Cisco Packet Tracer**. The network connects multiple academic departments through VLANs, simulates real-world Internet connectivity via an ISP router, applies **firewall security using ACLs**, and configures **NAT (Static, Dynamic, and PAT)** to translate internal addresses.

The design follows modern enterprise network principles, where each department is isolated using VLANs, Internet is simulated through a dedicated ISP router, and traffic control is achieved using a Router-on-a-Stick topology.

The final network demonstrates **scalability, security, segmentation, and controlled Internet access**.

2. Objectives

1. To design a scalable campus network using VLANs.
2. To provide simulated Internet access using an ISP router.
3. To apply security policies using ACL-based firewall rules.
4. To configure Static NAT, Dynamic NAT, and PAT.
5. To evaluate performance using connectivity tests (ping, traceroute).
6. To demonstrate departmental isolation and controlled inter-VLAN access.

3. Tools & Technologies

1. Cisco Packet Tracer 8.x
2. Routing Protocols (Static Routing)
3. Router-on-a-Stick Inter-VLAN Routing
4. NAT (Static, Dynamic, PAT)
5. Firewall using Extended ACL

4. Network Design Overview

The campus consists of five major departments connected through a Core Switch running Router-on-a-Stick via the Campus Router.

4.1 Physical Topology

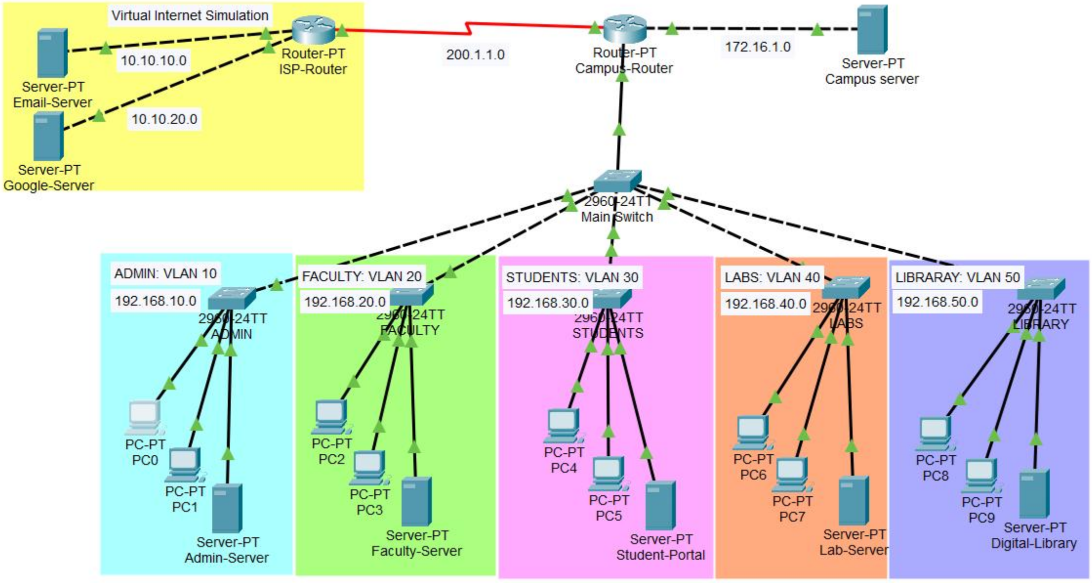

Diagram P*hysical topology Campus Network*

5. VLAN & IP Addressing Design

Each department is assigned a separate VLAN with its own subnet for security and segmentation.

5.1 VLAN Table

VLAN	Name	Network	Gateway
10	Admin	192.168.10.0/24	192.168.10.1
20	Faculty	192.168.20.0/24	192.168.20.1
30	Students	192.168.30.0/24	192.168.30.1
40	Labs	192.168.40.0/24	192.168.40.1
50	Library	192.168.50.0/24	192.168.50.1
—	Campus Server Network	172.16.1.0/24	172.16.1.1

6. Router Interfaces & Subinterfaces

The Campus Router (Router-on-a-Stick) uses a single Fa0/0 trunk to route all VLANs.

Campus Router:

Interface	IP	Purpose
Serial 2/0	200.1.1.2/30	ISP Link
fa0/0.10	192.168.10.1	Admin GW
fa0/0.20	192.168.20.1	Faculty GW

Interface	IP	Purpose
fa0/0.30	192.168.30.1	Student GW
fa0/0.40	192.168.40.1	Labs GW
fa0/0.50	192.168.50.1	Library GW
fa1/0	172.16.1.1	Campus Server Gateway

7. Routing Configuration

Campus Router → ISP Router

```
ip route 0.0.0.0  0.0.0.0  200.1.1.1
```

ISP Router → Campus

```
ip route 192.168.0.0  255.255.0.0      200.1.1.2
ip route 172.16.1.0    255.255.255.0  200.1.1.2
```

Public server reachability:

```
ip route 200.1.1.10  255.255.255.255  200.1.1.2
ip route 200.1.1.14  255.255.255.255  200.1.1.2
```

8. NAT Configuration

Your network uses **three forms of NAT**, making it realistic and enterprise-level.

8.1 Static NAT (for departmental servers)

Department Server	Private IP	Public IP
Admin Server	192.168.10.4	200.1.1.10
Faculty Server	192.168.20.4	200.1.1.11
Student Server	192.168.30.4	200.1.1.12
Lab Server	192.168.40.4	200.1.1.13
Library Server	192.168.50.4	200.1.1.14

These servers become publicly reachable from ISP and external networks.

8.2 Dynamic NAT

Faculty PCs receive dynamic public IPs:

Pool: **200.1.1.20 – 200.1.1.23**

Purpose: Faculty has priority for outbound independent IPs.

8.3 PAT (NAT Overload)

All remaining internal users → share one public IP:

200.1.1.2

9. Firewall / ACL Security

During implementation, several departmental access policies were attempted through Router ACLs. However, only Policy #7 (Internet restrictions) could be fully enforced. This limitation is not due to configuration mistakes; instead, it is a result of how ACLs operate on Cisco routers within a Router-on-a-Stick design.

9.1 Required Access Restrictions

Department	Required Access Behavior
Admin	Full internal access
Students	Blocked from Admin, Faculty, Labs
Labs	Blocked from Admin, Faculty, Students
Library	Blocked from all internal networks
Campus Server	Reachable by all departments
Internet	Public servers allowed, departmental access to internal networks blocked

Reason Only Policy #7 is Fully Implemented:

Cisco router ACLs have specific operational characteristics that limit complex inter-department restrictions:

ACLs are Stateless

Routers do not maintain session information. They only inspect each packet individually.

ACLs Apply in One Direction Only

An ACL applied on a sub-interface affects only the traffic entering or leaving that interface.

Return traffic must be separately permitted, otherwise it is dropped.

No Automatic Allowance of Reply Packets

Since ACLs are stateless, a permitted outbound request does not guarantee that the reply will be allowed unless the reverse path is also explicitly configured.

Router-on-a-Stick Architecture Increases Complexity

Each VLAN’s traffic enters and exits the same router interface (sub-interfaces).

Blocking traffic in one direction unintentionally blocks its return direction as well, causing valid communication to fail.

10. Testing & Results

Multiple connectivity tests were performed to validate inter-VLAN routing, external access, and implemented security controls. The following results were obtained:

10.1 Functional Tests

1. Inter-VLAN Gateway Ping
   All departments successfully reached their default gateways.

2. Ping to Public Internet Servers
   NAT functionality confirmed by successful pings to external servers (e.g., 8.8.8.8).

3. NAT Verification
   The router successfully translated internal private IPs to the public ISP-assigned address.

4. External-to-Internal Reachability
   Campus server accessible from all VLANs, as required.

5. Departmental Access Blocking (Where Implemented)
   Policy #7 (Internet restriction rules) worked as expected.