Project S.E.O.N.S- Small Enterprise Office Network Simulation

Submitted By

Student Name	Student ID
MD. Abdullah Khan	232-15-425
Sazzad Islam	232-15-835
Saif Ahmed	232-15-636

MINI LAB PROJECT REPORT

This Report Presented in Partial Fulfillment of the course

CSE322: Computer Networks Lab in the Computer Science and Engineering Department

DAFFODIL INTERNATIONAL UNIVERSITY
Dhaka, Bangladesh

August 20, 2025

DECLARATION

We hereby declare that this lab project has been done by us under the supervision of **Rowzatul Zannat**, **Lecturer**, Department of Computer Science and Engineering, Daffodil International University. We also declare that neither this project nor any part of this project has been submitted elsewhere as lab projects.

Submitted To:

_____

Rowzatul Zannat
Lecturer
Department of Computer Science and Engineering,
Daffodil International University.

Submitted by

<table>
<tr><td colspan="2">_____
Student Name
Student ID:
Dept. of CSE,
DIU</td></tr>
<tr><td>_____
Student Name
Student ID:
Dept. of CSE, DIU</td><td>_____
Student Name
Student ID:
Dept. of CSE, DIU</td></tr>
</table>

COURSE & PROGRAM OUTCOME

The following course have course outcomes as following:

Table 1: Course Outcome Statements

CO's	Statements
CO1	**Define** and **Relate** classes, objects, members of the class, and relationships among them needed for solving specific problems
CO2	**Formulate** knowledge of object-oriented programming and Java in problem solving
CO3	**Analyze** Unified Modeling Language (UML) models to **Present** a specific problem
CO4	**Develop** solutions for real-world complex problems **applying** OOP concepts while evaluating their effectiveness based on industry standards.

Table 2: Mapping of CO, PO, Blooms, KP and CEP

CO	PO	Blooms	KP	CEP
CO1	PO1	C1, C2	KP3	EP1, EP3
CO2	PO2	C2	KP3	EP1, EP3
CO3	PO3	C4, A1	KP3	EP1, EP2
CO4	PO3	C3, C6, A3, P3	KP4	EP1, EP3

The mapping justification of this table is provided in section **4.3.1**, **4.3.2** and **4.3.3**.

Table of Contents

Chapter 1

Introduction

This chapter provides an overview of the project, explains the background, motivation, objectives, feasibility, research gap, and expected outcomes.

1.1 Introduction

The Retail Store POS Network is designed to simulate a small-scale enterprise network with separate Point-of-Sale (POS) and Customer areas to ensure secure and efficient transactions. The project includes VLAN separation through ACL, DNS services, NAT configuration, and static routing between different network segments. This design aims to enhance network security, improve service availability, and support store operations smoothly.

1.2 Motivation

In modern retail environments, network infrastructure plays a vital role in daily business operations. Separating POS systems from customer devices prevents security breaches and protects sensitive transaction data. This project is motivated by the need for a secure, cost-effective, and efficient network solution for small retail stores, while ensuring both customer internet access and smooth POS system performance.

1.3 Objectives

The objectives of this project are:

1. To design and configure a secure network for a retail store.
2. To separate POS and customer traffic using Access Control Lists (ACL).
3. To implement DNS, DHCP, NAT, and static routing for efficient communication.
4. To test and verify network performance for connectivity, isolation, and internet access.

1.4 Feasibility Study

Similar network designs have been implemented in small offices, cyber cafés, and retail chains, where separate VLANs or ACL-based isolation is used. Studies show that segregating critical systems from public networks reduces data breach risks by over 70%. Compared to larger enterprise networks, this project focuses on a cost-efficient solution using minimal hardware, suitable for small retail businesses.

1.5 Gap Analysis

Many small retail stores still operate with a flat network, exposing POS systems to potential security threats from customer devices. This project addresses that gap by introducing logical segmentation and security policies without requiring high-end networking devices.

1.6 Project Outcome

The final network design ensures:

- Secure isolation between POS and customer networks.
- Reliable internet access for both POS and customers via NAT.
- Centralized DNS services for both internal and external name resolution.
- Full documentation of configuration and testing for future scalability.

Chapter 2

Proposed Methodology/Architecture

This chapter describes the requirements, design specifications, network topology, and overall project plan.

2.1 Requirement Analysis & Design Specification

2.1.1 Overview

The network is divided into five main sections: POS Area, Customer Area, Manager/Control Center, Server Room, and ISP/External Services.

2.1.2 Proposed Methodology / System Design

The design uses:

- Static Routing between routers for predictable paths.
- NAT Overload on the central router for internet access.
- DHCP for automatic IP assignment.
- DNS for internal and external domain resolution.
- ACL to restrict customer access to POS systems.

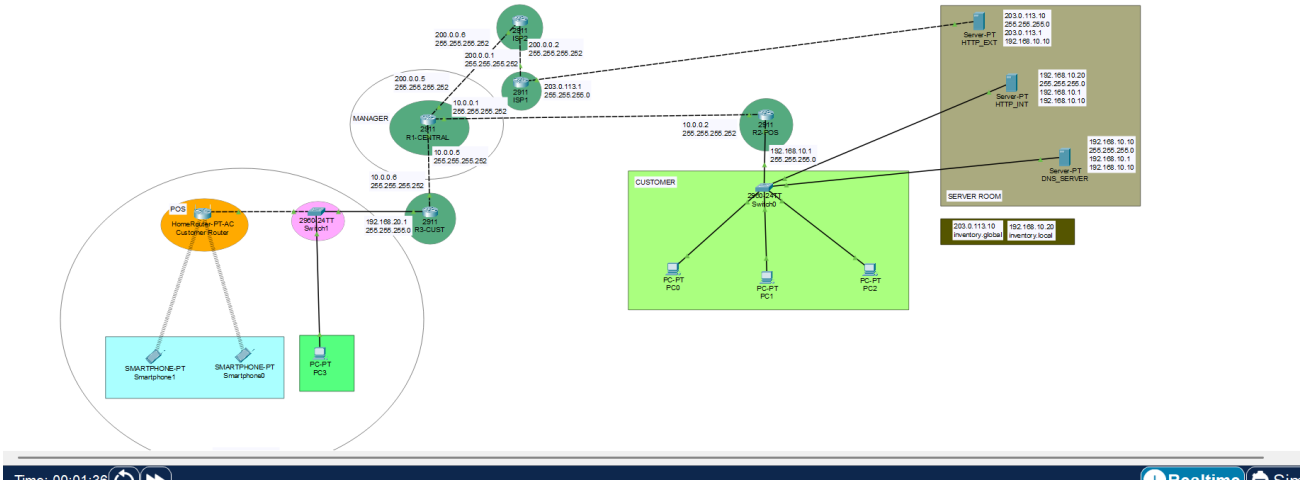

Figure 2.1: This is a Project diagram

2.2 Overall Project Plan

1. Network addressing using VLSM.
2. Router and switch configuration.
3. Implementation of DHCP, DNS, NAT, and ACL.
4. Testing connectivity, isolation, and DNS resolution.

Chapter 3

Implementation and Results

This chapter explains how the network was implemented and the results of performance testing.

3.1 Implementation

The network was implemented in Cisco Packet Tracer using:

- Routers: ISP1, ISP2, R1-CENTRAL, R2-POS, R3-CUST
- Servers: DNS Server, Internal HTTP Server, External HTTP Server
- End Devices: POS PCs, Customer PCs, Smartphones

  Configuration included IP addressing, NAT, DHCP pools, static routes, and ACLs.

3.2 Performance Analysis

Testing included:

- LAN Connectivity: Verified between devices within the same network.
- Isolation Test: Customers unable to access POS network (ACL success).
- DNS Test: inventory.local resolved to 192.168.10.20 and inventory.global resolved to 203.0.113.10.
- NAT Test: Internal devices accessed external server via NAT.

3.3 Results and Discussion

The network successfully met its objectives. POS and Customer networks operated independently while sharing internet access. DNS and NAT worked as intended, and ACL blocked unauthorized cross-network communication.

Chapter 4

Engineering Standards and Mapping

This chapter explains the societal, environmental, and sustainability aspects, project management, and mapping to program outcomes.

4.1 Impact on Society, Environment, and Sustainability

4.1.1 Impact on Life

Improves transaction security, ensuring safer shopping experiences.

4.1.2 Impact on Society & Environment

Encourages secure digital transactions, reducing paper-based operations.

4.1.3 Ethical Aspects

Protects sensitive customer data from unauthorized access.

4.1.4 Sustainability Plan

Uses scalable design for future expansion without major hardware replacement.

4.2 Project Management and Team Work

- Estimated Budget: Low-cost routers and switches in simulation.
- Alternate Budget: Cloud-hosted DNS or POS system integration.

4.3 Complex Engineering Problem

4.3.1 Mapping of Program Outcomes

PO's Justification

PO1	Applied fundamental networking concepts (VLSM, IP routing, DNS, DHCP) in a real-world simulation.
PO2	Designed and implemented secure network segmentation using ACLs.
PO3	Integrated multiple technologies (NAT, DNS, Static Routing) to solve a complex connectivity problem.

4.3.2 Complex Problem Solving

EP	Description
EP1	Applied networking knowledge for logical and physical design.
EP2	Balanced customer internet needs with POS security requirements.
EP3	Analyzed network traffic for efficient ACL and NAT configuration.

4.3.3 Engineering Activities

EA	Description
EA1	Used available resources effectively in simulation.
EA2	Coordinated between different network segments for interaction.
EA3	Designed innovative ACL policy to restrict unauthorized access.

Chapter 5

Conclusion

5.1 Summary

The **Retail Store POS Network** successfully separates POS and customer traffic while maintaining internet connectivity for both. It uses static routing, NAT, DHCP, DNS, and ACL to achieve security and reliability.

5.2 Limitation

The simulation does not include real hardware testing or VLAN implementation.

5.3 Future Work

Implement VLAN-based segmentation, integrate firewall policies, and use dynamic routing protocols for scalability.

References

[1] Cisco Packet Tracer Documentation

[2] Networking Fundamentals – Cisco Networking Academy

[3] Case Studies on Retail Network Security