<Document Title>

<Your Name>

<Student ID>

<Course Code>

<Professor Name>

<Due Date>

# Table of Contents

[Table of Contents 2](#_Toc48746339)

[Lab <n> - <Lab Name> 3](#_Toc48746340)

[Part <n> 3](#_Toc48746341)

[Description 3](#_Toc48746342)

[Preparation 3](#_Toc48746343)

[Observations 3](#_Toc48746344)

[Screenshots 3](#_Toc48746345)

[Reflection 3](#_Toc48746346)

[References 3](#_Toc48746347)

# Lab <n> - <Lab Name>

# Task <1>

## Description

The network topology project entails creating and deploying a fiber-optic network that connects two buildings to form an organization's network infrastructure. The business headquarters and engineering/test departments, each with distinct departments and network needs, are located on the organization's main campus.

## Preparation

VLAN Definition: List the names of the VLANs and their functions for each department in the two buildings.

Inter-VLAN Routing: Set up routing to facilitate departmental communication inside the same structure.

Use access control lists, or ACLs, to manage departmental traffic flow and maintain security.

DHCP Setup: To enable dynamic IP addressing, set up DHCP servers for every VLAN.

Quality of Service (QoS): Set up policies to provide priority to traffic related to important applications.

Use the Spanning Tree Protocol (STP) to maintain redundancy and stop network loops.

Wireless Networks: Configure WiFi networks for visitors and employees that are appropriately secured.

Network Address Translation (NAT): To access the internet, set up NAT on the router.

VLAN Tagging: For VLAN segmentation, apply VLAN tagging to switch ports.

Testing: To guarantee appropriate functioning and connection, carry out thorough testing.

## Observations

For logical segmentation, VLANs need to be appropriately designed and linked to the departments for which they are intended.

While preserving security, inter-VLAN routing need to enable easy departmental collaboration.

It is important to properly establish ACLs in order to manage traffic flow and prevent unwanted access.

Within each VLAN, IP addresses should be assigned appropriately by DHCP servers.

To guarantee optimal performance, QoS regulations should provide priority to traffic related to key applications.

STP is supposed to keep the network stable and avoid loops.

Secure configuration of wireless networks is necessary to thwart unwanted access.

Internal devices should be able to access the internet via the ISP connection thanks to NAT.

In order to guarantee appropriate routing and traffic separation, VLAN tagging must be applied appropriately.

The complete network infrastructure's connection and operation should be confirmed through testing.

## Reflection

This organization's network topology design and implementation was a difficult but worthwhile experience that greatly improved my knowledge of and proficiency with network architecture. Every step of the project—from creating VLANs and setting up inter-VLAN routing to putting access control lists (ACLs) into place, setting up DHCP, establishing Quality of Service (QoS) policies, configuring wireless networks, implementing NAT, tagging VLANs, and conducting extensive testing—contributed to a comprehensive understanding of network design and management. This project was a crucial networking learning experience because of the careful planning and execution needed to satisfy the unique needs of each department while maintaining overall network efficiency and security. These efforts also yielded insightful knowledge about the deployment of network infrastructure in the real world.