

**Computer Networks**

**Course Instructor: Sunduss Aamir**

**Student Name: Romaisa Ahmad**

**Roll Number: i211702**

Contents

[Computer Networks Project Documentation 3](#_Toc184589032)

[Project Overview 3](#_Toc184589033)

[Configuration Details 3](#_Toc184589034)

[1. Network Design 3](#_Toc184589035)

[2. Device Configuration 4](#_Toc184589036)

[3. Routing Implementation 4](#_Toc184589037)

[4. NAT Implementation 4](#_Toc184589038)

[5. Access Control Lists (ACLs) 4](#_Toc184589039)

[6. Email Configuration 5](#_Toc184589040)

[Design Explanation 5](#_Toc184589041)

[1. VLSM Subnetting 5](#_Toc184589042)

[2. Routing Strategy 5](#_Toc184589043)

[3. NAT Configuration 5](#_Toc184589044)

[4. ACLs 6](#_Toc184589045)

[5. DHCP Configuration 6](#_Toc184589046)

[Implementation Challenges 6](#_Toc184589047)

[1. Redistribution Configuration 6](#_Toc184589048)

[2. Email Server Setup 6](#_Toc184589049)

[3. ACL Optimization 6](#_Toc184589050)

[Conclusion 6](#_Toc184589051)

# Computer Networks Project Documentation

## Project Overview

This project demonstrates the implementation of a complex network design using Cisco Packet Tracer. The task involved configuring a given topology with specific IP addressing, routing, NAT, DHCP, ACLs, and additional requirements for email services. The entire configuration was designed to meet the specifications provided in the task document while adhering to strict academic guidelines.

## Configuration Details

### 1. Network Design

* The topology includes multiple networks labeled alphabetically (e.g., Network A, B, C...).
* The network used **Variable Length Subnet Masking (VLSM)** to optimize IP address allocation. The number of required hosts per subnet and inter-router links were calculated to ensure efficient use of the IP address space.
* **Private IP Addressing** and **Public IP Addressing** were implemented for specific networks:
  + Public IPs used: **203.0.113.15** and **10.0.0.50**.
  + NAT was configured on **Router20 (Network J)** and **Router8 (Network E)** to enable communication between private and public networks.

### 2. Device Configuration

* All devices and interfaces were appropriately labeled for easy identification.
* Host IPs within **EIGRP**, **OSPF (Areas 1 & 2)**, and **RIP** were assigned dynamically through the **DHCP server** located in the last block.
* Static and dynamic routing methods were configured as per the block specifications.

### 3. Routing Implementation

* **EIGRP**, **OSPF**, and **RIP** routing protocols were used within their respective areas.
* Redistribution was configured on routers that connected different protocol blocks to ensure seamless communication between areas.

### 4. NAT Implementation

* **Router20** was configured with NAT for **Network J**, while **Router8** was configured for **Network E**.
* The private IP ranges provided were used to set up NAT pools, ensuring secure communication between internal and external networks.

### 5. Access Control Lists (ACLs)

Access restrictions were implemented to meet the following requirements:

* One PC from **Network A** was blocked from accessing the **Web Server**.
* A smartphone from **Network E** and **Network J** was denied access to the **Web Server**.
* All devices in **Network D** were restricted from accessing the **Web Server**. The ACLs were applied on the router connected to the **Web Server** to enforce these restrictions.

### 6. Email Configuration

* A **Mail Server** was configured in the first block to facilitate communication among all hosts.
* Email accounts were set up for all users, allowing them to send and receive emails within the network.

## Design Explanation

### 1. VLSM Subnetting

* VLSM was chosen to minimize IP wastage while accommodating the host requirements in each subnet.
* Subnets were designed to ensure sufficient address allocation for current and potential future needs.

### 2. Routing Strategy

* A combination of EIGRP, OSPF, and RIP was used to maintain scalability and compatibility across different blocks.
* Redistribution provided a seamless transition between protocols without packet loss or latency issues.

### 3. NAT Configuration

* NAT was implemented to enable private networks to access the public internet using the provided public IPs.
* This ensured security and efficient utilization of IP resources.

### 4. ACLs

* ACLs were strategically placed to restrict access to the Web Server based on the given requirements.
* These configurations enhanced network security and ensured compliance with the task constraints.

### 5. DHCP Configuration

* The centralized DHCP server dynamically allocated IP addresses across all hosts within the topology.
* This reduced manual configuration efforts and ensured scalability.

## Implementation Challenges

1. Redistribution Configuration  
   Proper care was taken to configure redistribution points to avoid routing loops and ensure accurate route propagation.
2. Email Server Setup  
   Configuring the email server required additional research to integrate it into the network seamlessly.
3. ACL Optimization  
   Crafting ACL rules to block specific devices without affecting other traffic was challenging but successfully achieved.

## Conclusion

This project demonstrated the implementation of a comprehensive and efficient network topology in Cisco Packet Tracer. The configuration met all technical requirements and successfully showcased practical knowledge of subnetting, routing, NAT, DHCP, and ACLs. The design was documented and executed with clear labeling and detailed configurations, ensuring ease of understanding and replicability.