Green University of Bangladesh

Department of Computer Science and Engineering (CSE)
Semester: (Fall, Year: 2024), B.Sc. in CSE (Day)

Office Network Design Using Cisco Packet Tracer

Course Title: Computer Networking Lab
Course Code: CSE 312
Section: 221-D5

Students Details

Name	**ID**
Shahariar Hossain Rakib	221902071
Md. Ittesaf Hossain	221902289

Submission Date: 24/12/2024
Course Teacher's Name: Md. Saiful Islam Bhuiyan

[For teachers use only: Don't write anything inside this box]

Lab Report Status

Marks: **Signature:**

Comments: **Date:**

Contents

Abstract

The following project gives emphasis to designing and simulating a robust, scalable network infrastructure of the office environment using the Cisco Packet Tracer software application. The proposed hierarchical model introduces redundancy in every layer for reliability and continuity within its operation. This shall be further integrated with features such as VLAN segmentation for departmental isolation, OSPF dynamic routing for efficient data transfer, and DHCP for automatic IP address allocation. It will implement security features such as ACLs, SSH, and port security against unauthorized access. In order to maximize internet connectivity, it also incorporates NAT/PAT, which guarantees that failover procedures are in place to manage resilience in the event that any links fail. Latency, throughput, and redundancy tests that confirm the network's ability to meet current demands and scale for future growth require performance evaluation metrics. The network architecture offered here serves as a guide for effective and safe office communication systems that can handle both present demands and future expansion.

Chapter 1

Introduction

1.1 Overview

The ***"Office Network Design Using Cisco Packet Tracer"*** project deals with building a complete scalable infrastructure of a network for office purposes, taking into consideration such modern challenges in the operation of business as smooth communication, consistent data transfer, and strong security. It would be designed in a hierarchical model based on redundancy, taking into account scalability requirements for present times and further expansion at any time.

This project uses Cisco Packet Tracer to simulate and validate an efficient network layout, including VLAN segmentation, OSPF routing for dynamic path selection, and secure communication protocols like SSH. The design will make sure that the office network infrastructure is up to date with technological advances and business needs.

1.2 Motivation

An office basically requires an effective and secure network for smooth operations. Badly designed networks translate into delay modes of communication, data bottlenecks, and vulnerability to unauthorized access. This project is motivated by the urge to resolve these challenges through the creation of a network that will ensure robust communications, streamlined data transfer, and reliable resource access among employees.

The **"Office Network Design Using Cisco Packet Tracer"** gives a chance to put theoretical networking principles into practice. The project is supposed to design a scalable infrastructure for office use, considering the main needs of the operation: data segmentation, security, and resilience.

1.3 Problem Definition

1.3.1 Problem Statement

This is a challenge in office network infrastructure design: accommodating department segregation with regard to access and security while maintaining operational continuity. Almost all of these office sites experience various kinds of network-related issues around scalability, segregation, and vulnerabilities because of using improper security.

The design "Office Network Design Using Cisco Packet Tracer" has taken into consideration the challenges identified above to devise a network model that incorporates departmental VLANs, integrates OSPF for dynamic routing, and allows redundancy to nullify downtimes. The employees would therefore have complete access to all necessary resources at all times and securely.

1.3.2 Complex Engineering Problem

Name of the P Attributes	**Explain how to address**
P1: Depth of knowledge required	Involves advanced concepts like OSPF routing, VLAN segmentation, NAT, and SSH for secure communication.
P2: Range of conflicting requirements	Balances scalability, performance, security, and cost-effectiveness in a single, unified solution.
P3: Depth of analysis required	Requires detailed analysis of IP allocation, routing protocols, and department-specific network needs.
P4: Familiarity of issues	Resolves common networking problems such as inter-department communication, traffic bottlenecks, and access control.
P5: Extent of applicable codes	Adheres to networking standards and practices, such as IPv4 addressing and industry-standard security protocols.
P6: Extent of stakeholder involvement and conflicting requirements	Incorporates the expectations of IT teams, office employees, and management to address their unique needs.
P7: Interdependence	Incorporates the expectations of IT teams, office employees, and management to address their unique needs.

Table 1.1: Summary of the attributes touched by the mentioned projects

1.4 Design Goals

These are some goals of this project:

- Design a hierarchical network that allows office scalability.
- Provide redundancy, which is necessary for uptime.
- Segment various departments using VLANs to improve network security and efficiency.
- Use OSPF dynamic routing to support changes within the network.
- Utilize access controls like SSH for better network protection.
- Manage IP addresses using DHCP while reserving static IPs for key devices.
- Perform reliability testing through simulations using Cisco Packet Tracer.

1.5 Application

Some of the important applications of *"Office Network Design Using Cisco Packet Tracer"* in an office setup are:

1. Enables effective and efficient communication within the office.
2. Supports secure handling and operations of sensitive office data.
3. Facilitates scalability by allowing the addition of devices or departments with ease.
4. Optimizes resource management for the organization.
5. Provides a hierarchical structure for planning IP allotments to prevent network congestion.

Chapter 2

Design/Development/Implementation of the Project

2.1 Introduction

This chapter describes the design, development, and implementation of the office network infrastructure by simulation using Cisco Packet Tracer. The project is based on a hierarchical model so that it is scalable, reliable, and robust in security to meet the communication requirements of the different departments. Advanced configurations such as VLANs, DHCP, OSPF routing, NAT/PAT, and SSH will be applied to this network to create a realistic office environment simulation.

2.2 Project Details

This section details the design of the office network—its topology, components, and other implementation specifics.

2.2.1 Topology

The topology of the network is based on the hierarchical model, where the network is divided into three layers:

- **Core Layer:** Composed of routers and multi-layer switches to handle the high volume and redundancy of data.
- **Distribution Layer:** This tier connects to departmental networks through switching devices using VLAN-enabled switches.
- **Access Layer:** At this tier, the end-users directly attach, which involves PCs and Wireless Access Points.

Features of the Topology

The notable features include:

- Multiple VLANs are built to segment the traffic of the departments.
- Two core routers with multiple multi-layer switches provide redundancy.

Departmental Subnet Allocation

The following are the different departments with subnet allocations based on the IPv4 addressing scheme:

- Clients will connect through access points and switches to ensure strong connectivity.

2.2.2 Components

The proposed network design for the project will involve the following components:

1. **Routers (4):**
   - Two routers connect upstream to the ISP at the core layer to provide redundancy.
   - Both routers are statically configured with public IP addresses for internet connectivity.
2. **Multilayer Switches (2):**
   - Located at the core layer to offer redundancy and perform efficient routing.
   - Configured for both switching and routing roles.
   - Assigned IP addresses for routing between different VLANs.
3. **Distribution Layer Switches (Multiple):**
   - Connect various departments to the core layer.
   - Facilitate intra-VLAN communication.
4. **End-User PCs:**
   - Positioned at the access layer.
   - Connected to the Distribution Layer Switches to access department-specific resources.
5. **Cisco Access Points (APs):**
   - Located at the access layer for wireless connectivity.
   - Ensure wireless network availability in every department.

6. **DHCP Server (1):**
   - Located in the server room.
   - Dynamically assigns IP addresses to all end-user devices.
7. **Equipment in Server Room:**
   - Includes servers, storage units, and other networking equipment.
   - Configured with static IP addresses.
   - No DNS server, HTTP server, or other services are included.

These components together provide a well-structured and organized network architecture that integrates redundancy, efficient routing, and secure communication, fulfilling the specific requirements of the operation of the trading floor support center.

2.3 IP Addressing Scheme

Provide details about the IP addressing scheme applied to the network.

Base Network: 192.168.0.0/22

First floor:

Department	**Network Address**	**Subnet Mask**	**Host Address Range**	**Broadcast Address**
Sales & Marketing	192.168.10.0	255.255.255.0/24	192.168.10.1 to 192.168.10.254	192.168.10.255
HR and Logistic	192.168.20.0	255.255.255.0/24	192.168.20.1 to 192.168.20.254	192.168.20.255

Second Floor:

Department	**Network Address**	**Subnet Mask**	**Host Address Range**	**Broadcast Address**
Finance & Accounts	192.168.30.0	255.255.255.0/24	192.168.30.1 to 192.168.30.254	192.168.30.255
Admin & Public Relations	192.168.40.0	255.255.255.0/24	192.168.40.1 to 192.168.40.254	192.168.40.255

Third Floor:

Department	**Network Address**	**Subnet Mask**	**Host Address Range**	**Broadcast Address**
ICT	192.168.50.0	255.255.255.0/24	192.168.50.1 to 192.168.50.254	192.168.50.255
Server	192.168.60.0	255.255.255.0/24	192.168.60.1 to 192.168.60.254	192.168.60.255

Core Router and L3 SW:

No	**Network Address**	**Subnet Mask**	**Host Address Range**	**Broadcast Address**
Core R1-MLTSW1	10.10.10.0	255.255.255.252	10.10.10.1 to 10.10.10.2	10.10.10.3
Core R1-MLTSW2	10.10.10.4	255.255.255.252	10.10.10.5 to 10.10.10.6	10.10.10.7
Core R2-MLTSW1	10.10.10.8	255.255.255.252	10.10.10.9 to 10.10.10.10	10.10.10.11
Core R2-MLTSW2	10.10.10.12	255.255.255.252	10.10.10.13 to 10.10.10.14	10.10.10.15

Public IP between Core and ISP:

- 103.133.254.0/30
- 103.133.254.4/30
- 103.133.254.8/30
- 103.133.254.12/30

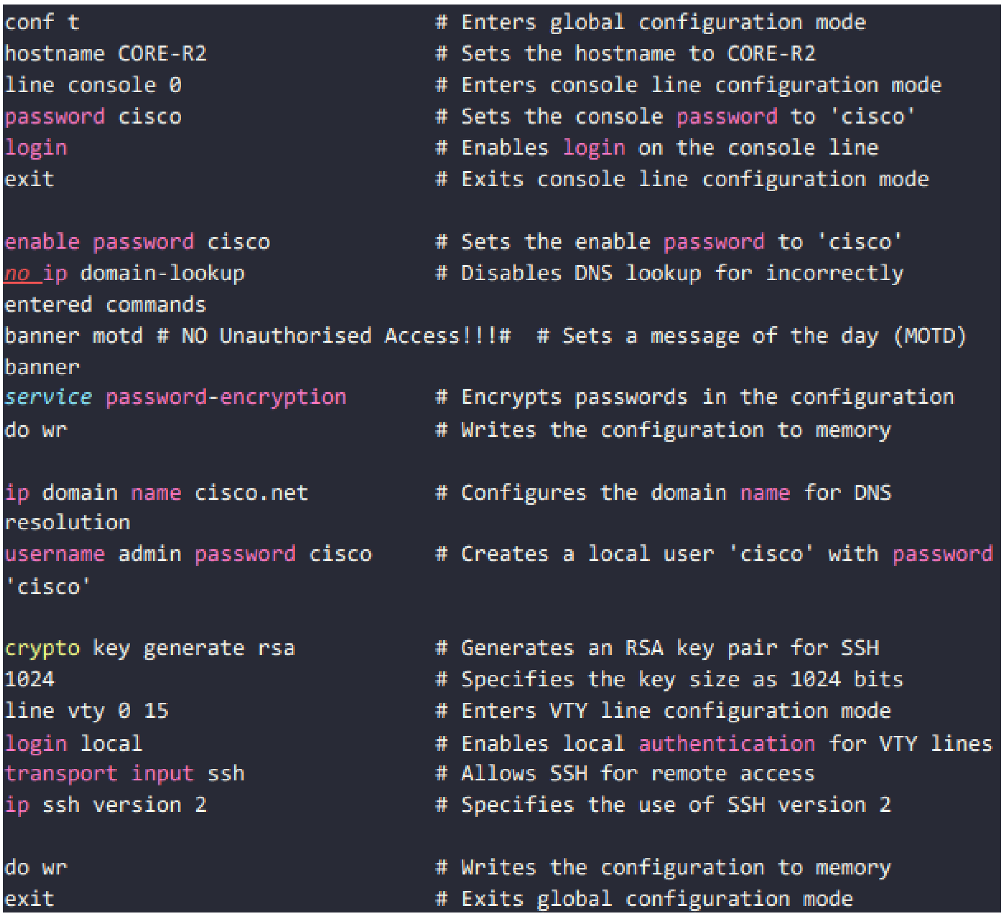
2.3 Implementation

The network implementation includes several stages to establish connectivity, security, and proper traffic management.

2.3.1 Routing Configuration

Router Configuration

Basic Router Configuration

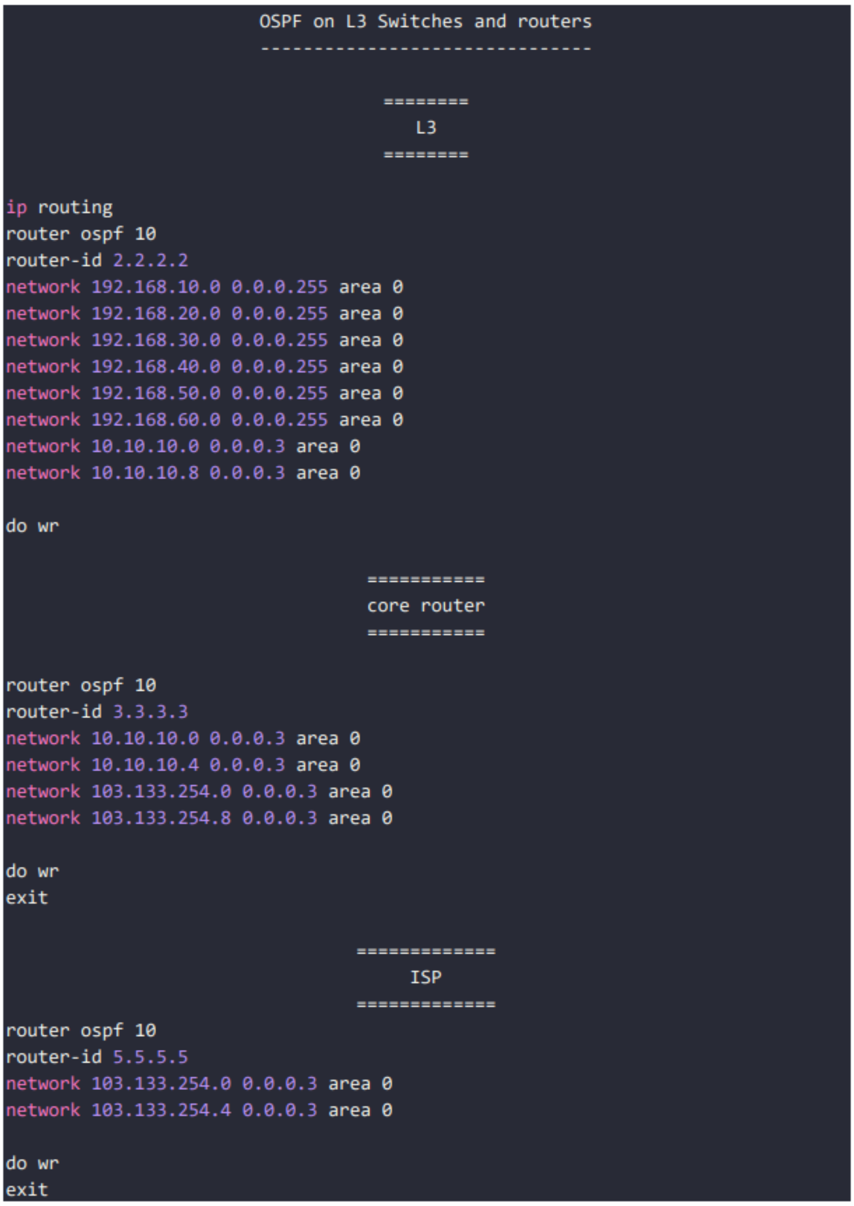


```
conf t                            # Enters global configuration mode
hostname CORE-R2                  # Sets the hostname to CORE-R2
line console 0                    # Enters console line configuration mode
password cisco                    # Sets the console password to 'cisco'
login                             # Enables login on the console line
exit                              # Exits console line configuration mode

enable password cisco             # Sets the enable password to 'cisco'
no ip domain-lookup               # Disables DNS lookup for incorrectly
entered commands
banner motd # NO Unauthorised Access!!!#  # Sets a message of the day (MOTD)
banner
service password-encryption       # Encrypts passwords in the configuration
do wr                             # Writes the configuration to memory

ip domain name cisco.net          # Configures the domain name for DNS
resolution
username admin password cisco     # Creates a local user 'cisco' with password
'cisco'

crypto key generate rsa           # Generates an RSA key pair for SSH
1024                              # Specifies the key size as 1024 bits
line vty 0 15                     # Enters VTY line configuration mode
login local                       # Enables local authentication for VTY lines
transport input ssh               # Allows SSH for remote access
ip ssh version 2                  # Specifies the use of SSH version 2

do wr                             # Writes the configuration to memory
exit                              # Exits global configuration mode
```

Figure 2.1: Router Configuration

Static and Dynamic Routing

This design balances both static and dynamic routing strategies within a resilient routing infrastructure. The static routing approach is applied to some of the specific, predictable routes within the network. Static routes will be added on routers to direct traffic to the dedicated DHCP servers in the server room. In this way, a fixed path can be pre-determined and always followed. The network is designed in a way that this setting may be easily used for critical internal communication. On the contrary, dynamic routing is being applied to serve adaptive and automated route selection. OSPF scales dynamically to changes in the network and, thus is flexible. In combination, a strong static solution with a dynamic solution serves to cater for predefined routing needs as well as enabling one to have evolving routing requirements in "Office System Network Design."



```
                        OSPF on L3 Switches and routers
                        ------------------------------

                                   ========
                                      L3
                                   ========

ip routing
router ospf 10
router-id 2.2.2.2
network 192.168.10.0 0.0.0.255 area 0
network 192.168.20.0 0.0.0.255 area 0
network 192.168.30.0 0.0.0.255 area 0
network 192.168.40.0 0.0.0.255 area 0
network 192.168.50.0 0.0.0.255 area 0
network 192.168.60.0 0.0.0.255 area 0
network 10.10.10.0 0.0.0.3 area 0
network 10.10.10.8 0.0.0.3 area 0

do wr

                                  ===========
                                  core router
                                  ===========

router ospf 10
router-id 3.3.3.3
network 10.10.10.0 0.0.0.3 area 0
network 10.10.10.4 0.0.0.3 area 0
network 103.133.254.0 0.0.0.3 area 0
network 103.133.254.8 0.0.0.3 area 0

do wr
exit

                                 =============
                                      ISP
                                 =============
router ospf 10
router-id 5.5.5.5
network 103.133.254.0 0.0.0.3 area 0
network 103.133.254.4 0.0.0.3 area 0

do wr
exit
```

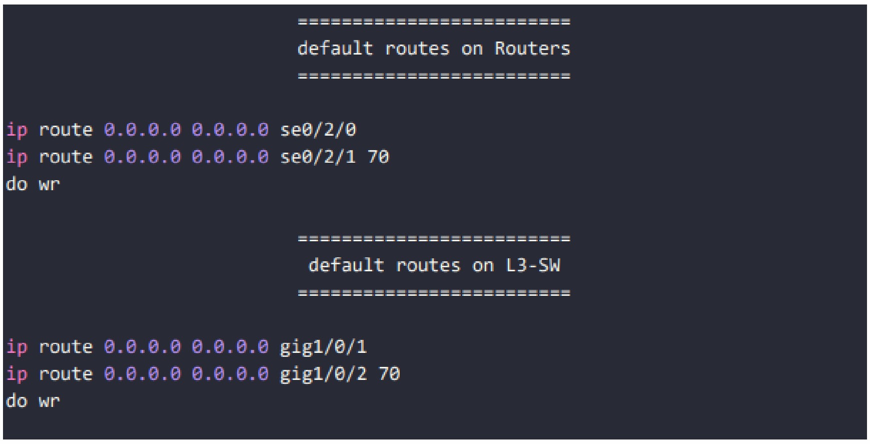
Figure 2.2: Static and Dynamic Routing

OSPF Routing

Open Shortest Path First (OSPF) is configured on core routers to dynamically select efficient routes:

```
router ospf 1
router-id 1.1.1.1
network 192.168.10.0 0.0.0.255 area 0
network 192.168.20.0 0.0.0.255 area 0
network 10.10.10.0 0.0.0.3 area 0
```

This configuration ensures that devices can communicate seamlessly between VLANs while adapting to network changes.



```
                           =========================
                           default routes on Routers
                           =========================

ip route 0.0.0.0 0.0.0.0 se0/2/0
ip route 0.0.0.0 0.0.0.0 se0/2/1 70
do wr

                           =========================
                            default routes on L3-SW
                           =========================

ip route 0.0.0.0 0.0.0.0 gig1/0/1
ip route 0.0.0.0 0.0.0.0 gig1/0/2 70
do wr
```

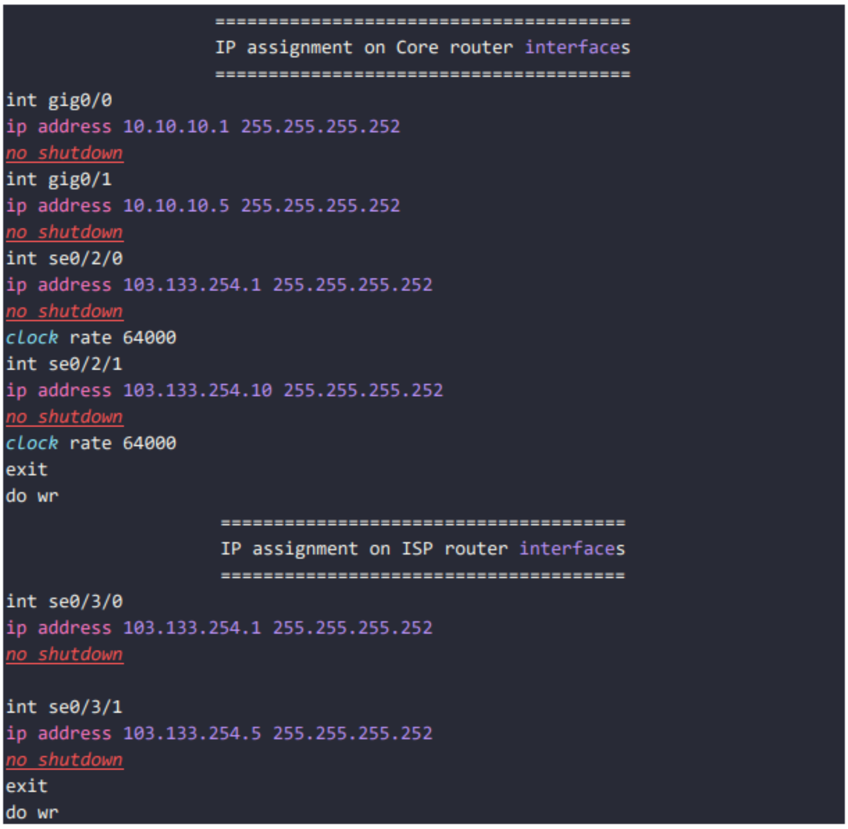
Figure 2.3: Static and Dynamic Routing

2.3.2 Switching Configuration

Switching Configuration

VLANs

VLANs logically separate the network into several broadcast domains. This is done for a number of reasons. In this lab, VLANs will be set up to logically separate the departments of Sales and Marketing on VLAN 10 and Human Resources and Logistics on VLAN 20. The VLANs are first created, then named, and then assigned to switch ports with the switchport access vlan command. By doing this, the network is more secure, has reduced broadcast traffic, and is more End-to-End. manage their network effectively. Every switch should be configured with VLANs, which will facilitate an organized and systematic network with security.



```
                    ======================================
                    IP assignment on Core router interfaces
                    ======================================
int gig0/0
ip address 10.10.10.1 255.255.255.252
no shutdown
int gig0/1
ip address 10.10.10.5 255.255.255.252
no shutdown
int se0/2/0
ip address 103.133.254.1 255.255.255.252
no shutdown
clock rate 64000
int se0/2/1
ip address 103.133.254.10 255.255.255.252
no shutdown
clock rate 64000
exit
do wr
                    =====================================
                    IP assignment on ISP router interfaces
                    =====================================
int se0/3/0
ip address 103.133.254.1 255.255.255.252
no shutdown

int se0/3/1
ip address 103.133.254.5 255.255.255.252
no shutdown
exit
do wr
```

Figure 2.4: Static and Dynamic Routing

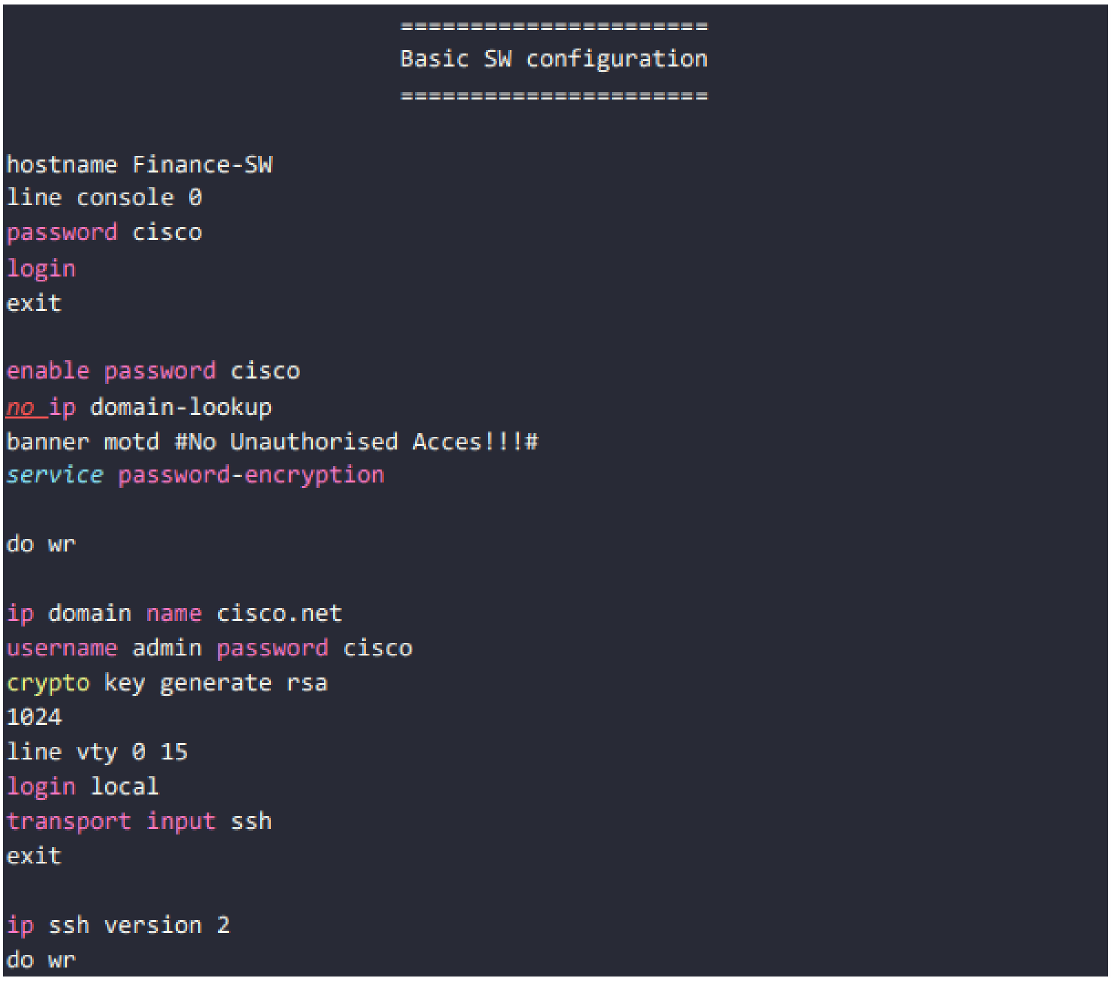
2.3.3 Inter-VLAN Routing

2.3.3.1 Layer 3 switching using SVIs

Here Inter-VLAN Routing is implemented by L3 switches. The Inter-VLAN configuration is done according to this:

2.3.3.2 Subnetting

Subnetting is an important ingredient for the project in implementing an IP address for resource management on the network. The base network address is 192.168.0.0/22; it is subnetted into other different departments. For instance, VLAN 10 would get a sub-network of 192.168.10.0/24, while the VLAN 20 will receive 192.168.20.0/24. It ensures that each VLAN receives a separate address and hence avoids overlapping; this also allows orderly addressing in the Network: this solution would cater for high-level security and ease in managing the network and also scalability in future by mapping different IP resources on different single VLANs.



```
                              ======================
                              Basic SW configuration
                              ======================

hostname Finance-SW
line console 0
password cisco
login
exit

enable password cisco
no ip domain-lookup
banner motd #No Unauthorised Acces!!!#
service password-encryption

do wr

ip domain name cisco.net
username admin password cisco
crypto key generate rsa
1024
line vty 0 15
login local
transport input ssh
exit

ip ssh version 2
do wr
```

Figure 2.5: Switch Configuration

2.3.4 Security Measures

Access Control Lists (ACLs)

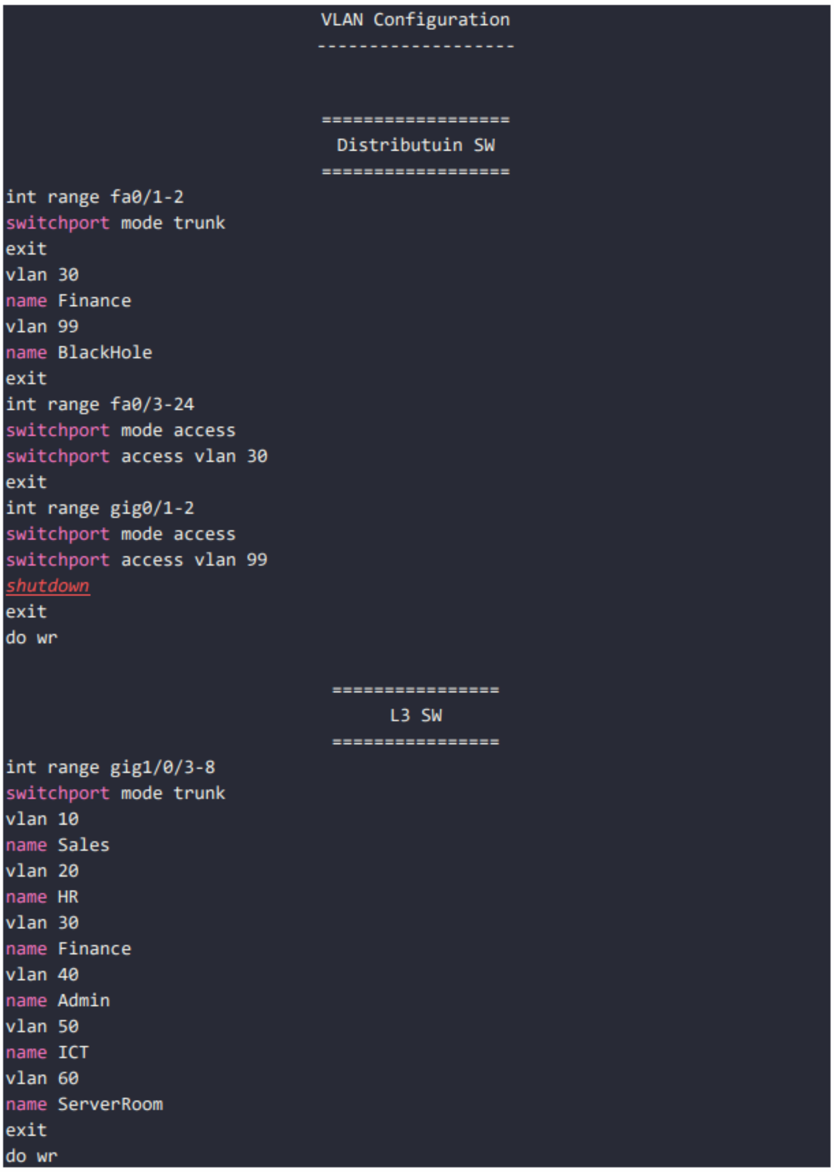
ACLs are applied on routers to filter traffic based on defined criteria, such as source and destination IP addresses, ports, and protocols.

NAT and PAT

NAT, PAT used for security and efficiency:

2.3.5 Port Security

Port security is an essential feature on switches that ensures only authorized devices can connect to a network. By limiting the number of MAC addresses that can access a particular switch port, unauthorized devices are effectively blocked, enhancing network security. The configuration below showcases how port security is implemented for the Finance network in this case study.



```
                              VLAN Configuration
                              ------------------


                              ==================
                                Distributuin SW
                              ==================
int range fa0/1-2
switchport mode trunk
exit
vlan 30
name Finance
vlan 99
name BlackHole
exit
int range fa0/3-24
switchport mode access
switchport access vlan 30
exit
int range gig0/1-2
switchport mode access
switchport access vlan 99
shutdown
exit
do wr

                               ================
                                    L3 SW
                               ================
int range gig1/0/3-8
switchport mode trunk
vlan 10
name Sales
vlan 20
name HR
vlan 30
name Finance
vlan 40
name Admin
vlan 50
name ICT
vlan 60
name ServerRoom
exit
do wr
```

Figure 2.6: VLANs

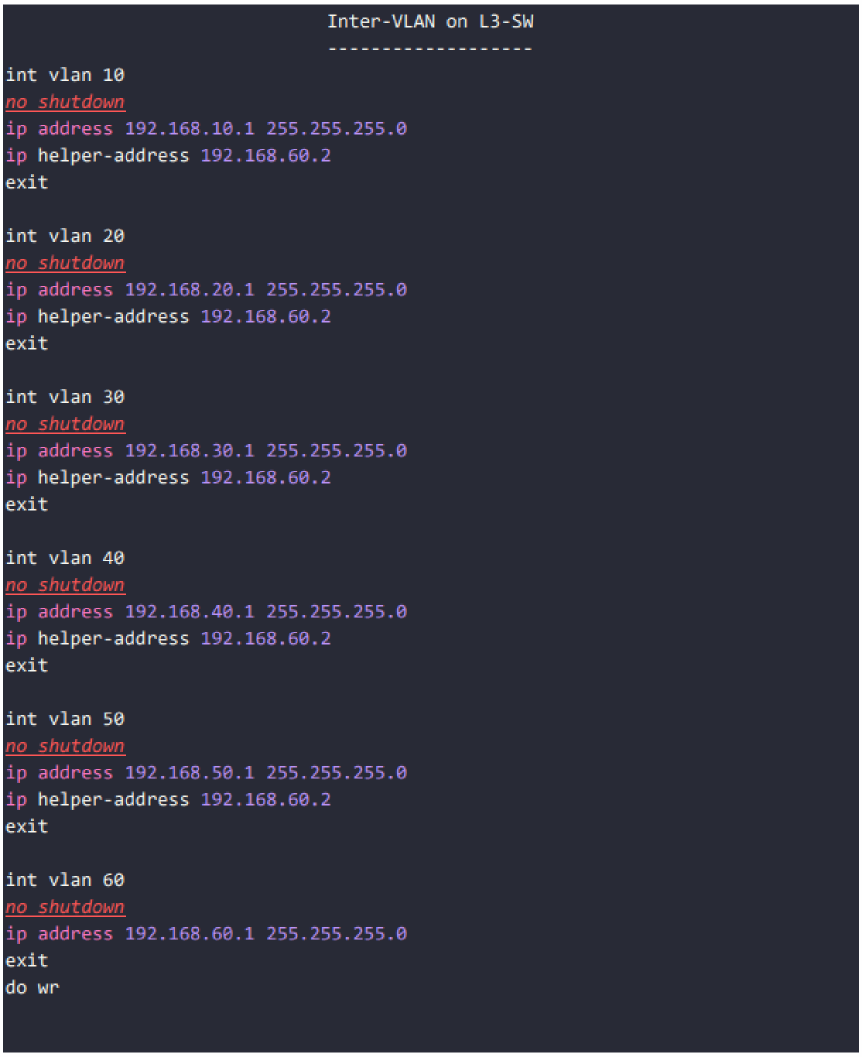
- **Interface range fastEthernet0/3-24:** Defines the range of Fast Ethernet ports (3 to 24) assigned to the Finance department.

- **switchport port-security maximum 1:** Limits the number of allowed MAC addresses per port to 1, ensuring only one device can connect.

- **switchport port-security mac-address sticky:** Enables sticky MAC addresses, allowing the switch to dynamically learn and secure MAC addresses for specified ports.

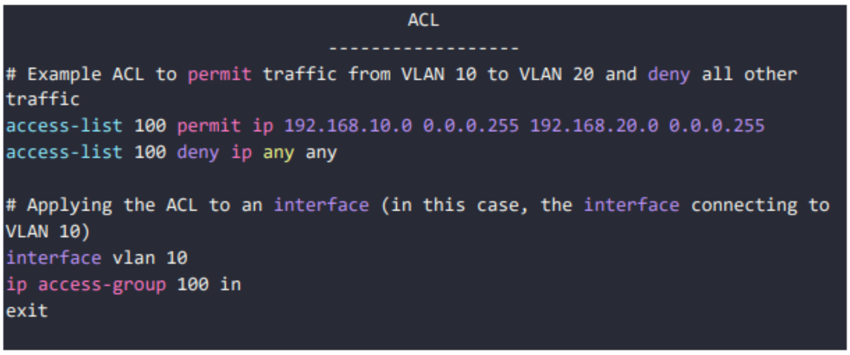
- **switchport port-security violation shutdown:** Configures the switch to shut down a port if a violation occurs, such as when the maximum allowed devices exceed 1.

This configuration ensures that:



```
Inter-VLAN on L3-SW
-------------------
int vlan 10
no shutdown
ip address 192.168.10.1 255.255.255.0
ip helper-address 192.168.60.2
exit

int vlan 20
no shutdown
ip address 192.168.20.1 255.255.255.0
ip helper-address 192.168.60.2
exit

int vlan 30
no shutdown
ip address 192.168.30.1 255.255.255.0
ip helper-address 192.168.60.2
exit

int vlan 40
no shutdown
ip address 192.168.40.1 255.255.255.0
ip helper-address 192.168.60.2
exit

int vlan 50
no shutdown
ip address 192.168.50.1 255.255.255.0
ip helper-address 192.168.60.2
exit

int vlan 60
no shutdown
ip address 192.168.60.1 255.255.255.0
exit
do wr
```

Figure 2.7: Inter-VLAN Routing

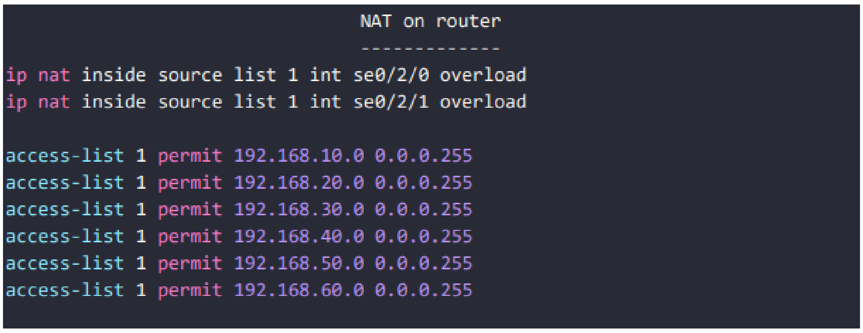


```
ACL
------------------
# Example ACL to permit traffic from VLAN 10 to VLAN 20 and deny all other
traffic
access-list 100 permit ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
access-list 100 deny ip any any

# Applying the ACL to an interface (in this case, the interface connecting to
VLAN 10)
interface vlan 10
ip access-group 100 in
exit
```

Figure 2.8: Access Control Lists (ACLs)

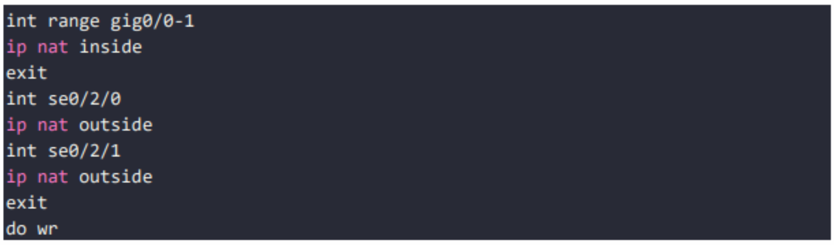
1. Only one authorized device is allowed per port in the Finance department.

2. The switch automatically learns and secures device MAC addresses for convenience and efficiency.



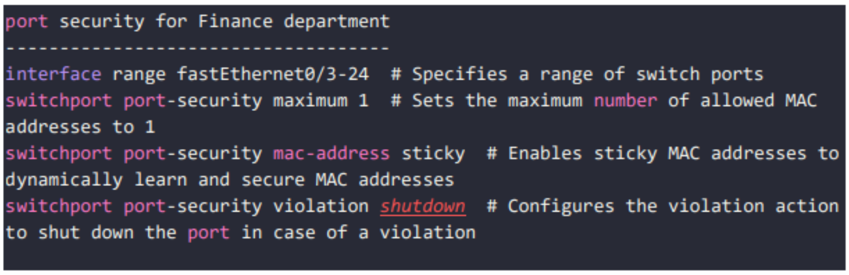
```
                               NAT on router
                               -------------
ip nat inside source list 1 int se0/2/0 overload
ip nat inside source list 1 int se0/2/1 overload

access-list 1 permit 192.168.10.0 0.0.0.255
access-list 1 permit 192.168.20.0 0.0.0.255
access-list 1 permit 192.168.30.0 0.0.0.255
access-list 1 permit 192.168.40.0 0.0.0.255
access-list 1 permit 192.168.50.0 0.0.0.255
access-list 1 permit 192.168.60.0 0.0.0.255
```

Figure 2.9: NAT



```
int range gig0/0-1
ip nat inside
exit
int se0/2/0
ip nat outside
int se0/2/1
ip nat outside
exit
do wr
```

Figure 2.10: PAT



```
port security for Finance department
------------------------------------
interface range fastEthernet0/3-24  # Specifies a range of switch ports
switchport port-security maximum 1  # Sets the maximum number of allowed MAC
addresses to 1
switchport port-security mac-address sticky  # Enables sticky MAC addresses to
dynamically learn and secure MAC addresses
switchport port-security violation shutdown  # Configures the violation action
to shut down the port in case of a violation
```

Figure 2.11: Port Security

3. Unauthorized connections cause the port to shut down, adding an extra layer of protection.

Configuration Summary Table

The implementation of port security adds robustness to the network's security infrastructure by ensuring that only one device with a particular MAC address can connect to each port in the Finance department. Any violations trigger an immediate port shutdown, safeguarding the network from unauthorized access or misuse.

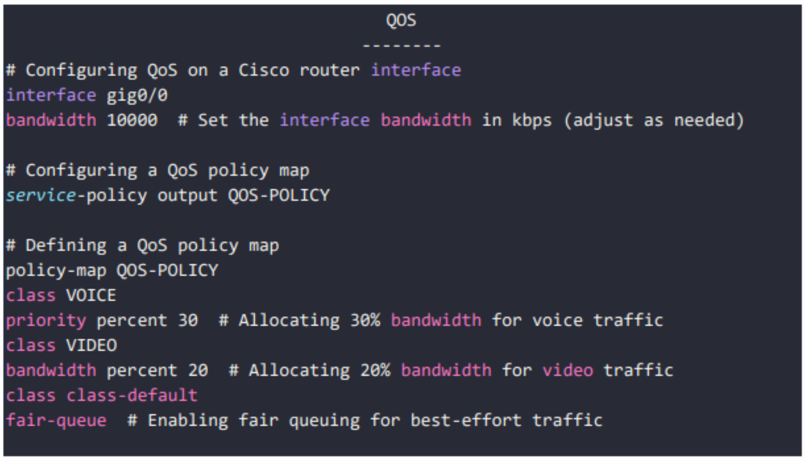
Command	Description
`interface range fastEthernet0/3-24`	Specifies the range of switch ports (ports 3 to 24) for Finance network.
`switchport port-security maximum 1`	Limits the maximum number of allowed devices per port to 1.
`switchport port-security mac-address sticky`	Automatically learns and secures MAC addresses connected to the port.
`switchport port-security violation shutdown`	Shuts down the port when a security violation occurs.

Table 2.1: Port Security Configuration Summary for Finance Network

2.3.6 Quality of Service (QoS)

QoS Configuration

QoS or Quality of Service is implemented in the network, which gives priority for critical applications, police network traffic so that the higher gets better performance. No implementation of QOS is required on my case study. This is the only basic just for an example of how it could be QoS config within network of course all will be changed based on the running Devices/Technology:



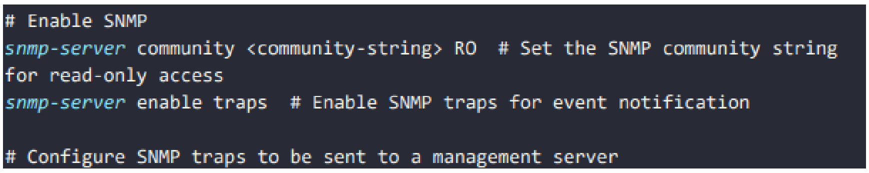
```
                                   QOS
                                 --------
# Configuring QoS on a Cisco router interface
interface gig0/0
bandwidth 10000  # Set the interface bandwidth in kbps (adjust as needed)

# Configuring a QoS policy map
service-policy output QOS-POLICY

# Defining a QoS policy map
policy-map QOS-POLICY
class VOICE
priority percent 30  # Allocating 30% bandwidth for voice traffic
class VIDEO
bandwidth percent 20  # Allocating 20% bandwidth for video traffic
class class-default
fair-queue  # Enabling fair queuing for best-effort traffic
```

Figure 2.12: QoS

2.3.7 Monitoring and Management

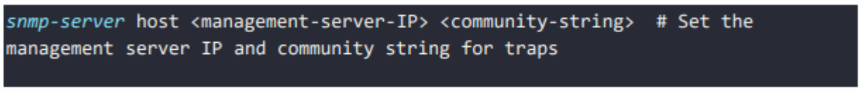
SNMP Configuration

Simple Network Management Protocol (SNMP) is configured to facilitate monitoring and management of network devices. The following is a general example of SNMP configuration on a Cisco router:



```
# Enable SNMP
snmp-server community <community-string> RO  # Set the SNMP community string
for read-only access
snmp-server enable traps  # Enable SNMP traps for event notification

# Configure SNMP traps to be sent to a management server
```

Figure 2.13: SNMP

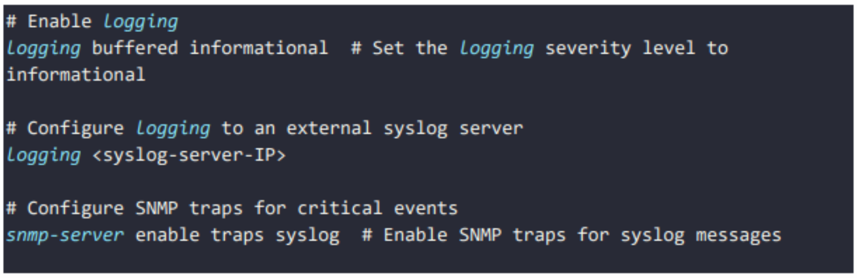


```
snmp-server host <management-server-IP> <community-string>  # Set the
management server IP and community string for traps
```

Figure 2.14: SNMP

Logging and Alerts

Logging and alerts are configured to capture and report events within the network. The configuration can include setting up logging destinations and severity levels for various events. Here is a sample configuration for logging on a Cisco device:



```
# Enable logging
logging buffered informational  # Set the logging severity level to
informational

# Configure logging to an external syslog server
logging <syslog-server-IP>

# Configure SNMP traps for critical events
snmp-server enable traps syslog  # Enable SNMP traps for syslog messages
```

Figure 2.15: Logging and Alerts

2.4 Algorithms

Specific algorithms form the heart of the office network in handling DHCP and OSPF-based routing to effectively function. This makes the network dynamic in operation, self-adapting, and performing efficient resource allocation.

2.4.1 DHCP Handling Algorithm

Dynamic Host Configuration Protocol (DHCP) automates the process of assigning IP addresses to devices. This eliminates the need for manual configuration and ensures consistent, error-free allocations in the network. The algorithm functions as follows:

Steps of the DHCP Algorithm:

- **DHCP Discovery:**
  - A new device connects to the network.
  - It sends a DHCP discovery message (broadcast) to identify available DHCP servers.
- **DHCP Offer:**
  - The DHCP server responds with a DHCP offer message containing an available IP address and lease information.
- **DHCP Request:**
  - The client selects one of the offered IP addresses.
  - It sends a DHCP request message to the server to confirm allocation.
- **DHCP Acknowledgement:**
  - The DHCP server confirms the IP allocation by sending an acknowledgment.
  - The client is officially assigned the IP address for the specified lease duration.

Pseudocode Representation:

```
Input: Device requesting an IP address.
Output: Device receives an IP address and lease time.
Steps:
1. Device → Broadcast: "DHCP Discovery"
2. DHCP Server → Broadcast: "DHCP Offer" (Available IP)
3. Device → DHCP Server: "DHCP Request" (Selected IP)
4. DHCP Server → Device: "DHCP Acknowledgement" (Assigned IP)
```

Example in Project Context: In the "Office Network Design Using Cisco Packet Tracer," each department is allocated a specific VLAN. DHCP ensures devices in VLAN 10 (e.g., Sales) receive IP addresses within the range 192.168.10.1 to 192.168.10.254.

2.4.2 OSPF-Based Route Recalculations

Open Shortest Path First (OSPF) is a dynamic routing protocol designed to find the most efficient path for data packets. It recalculates routes when network topology changes, ensuring that packets always use the best available path.

Key Features of the OSPF Algorithm:

- **Link-State Advertisement (LSA):** Each router exchanges its link-state information with its neighbors.
- **Shortest Path First (SPF):** The SPF algorithm (Dijkstra's Algorithm) runs to compute the optimal path.
- **Convergence:** The network quickly adapts to changes like link failures or congestion, recalculating routes dynamically.

Steps of the OSPF Algorithm:

- **Initialization:**
  - Routers are assigned unique identifiers and form neighbor adjacencies.
- **LSA Exchange:**
  - Routers share their link states (e.g., available links, costs) with neighbors.
- **Topology Database Update:**
  - Each router builds a database of the entire network topology based on received LSAs.
- **Shortest Path Calculation:**
  - Using Dijkstra's Algorithm, routers compute the shortest path tree.
  - The shortest path is determined based on link costs.
- **Routing Table Update:**
  - Routers update their routing tables with the newly computed optimal paths.

Pseudocode Representation:

```
Input: Topology changes (e.g., link failure, added nodes)
Output: Updated routing tables with optimal paths.
Steps:
1. Router detects a topology change.
2. Broadcast LSA to all neighbors.
3. Neighbors update their topology databases.
4. Run Dijkstra's algorithm:
   a. Start from the root (current router).
   b. Calculate the shortest path to each node.
5. Update the routing table.
6. Advertise updated routes to other routers.
```

Example in Project Context:

If the link between two core routers fails, OSPF detects this via LSAs and recalculates the shortest path to reroute traffic through alternate links. For instance, traffic from VLAN 30 (Finance) to VLAN 10 (Sales) will dynamically use the backup link without manual intervention.

Advantages in the Network Design:

- **Fault Tolerance:** OSPF quickly adapts to failures, ensuring minimal disruption.
- **Scalability:** Adding new routers automatically integrates them into the routing topology.
- **Efficiency:** Guarantees optimal data flow by recalculating the shortest paths.

Chapter 3

Performance Evaluation

3.1 Simulation Environment/ Simulation Procedure

3.1.1 Simulation Environment

The project, **Office Network Design Using Cisco Packet Tracer**, was simulated on the following platform:

- **Software:** Cisco Packet Tracer, Version 8.2
- **Hardware Emulation:** Routers Cisco, Layer 3 switches, Layer 2 switches, PCs, and servers.
- **Protocols Applied:**
  - OSPF for routing dynamically.
  - DHCP to handle automatic IP address allocation.
  - VLANs for segmentation in the network.
  - SSH and access lists for network security.
  - NAT/PAT for translation of Private to Public IP.
- **Base Network:** IPv4 addressing with each VLAN having its subnets.

3.1.2 Simulation Procedure

Topology Design: Implemented the Hierarchical Network Model consisting of three layers: Core, Distribution, and Access. VLANs were configured for the departments: Sales, HR, Finance, Administration, IT, and Server Room. Redundancy was ensured using Dual ISPs and multiple links.

Configuration: Routers, switches, DHCP servers, and VLANs were configured according to the design. OSPF was set up on Layer 3 switches and routers for dynamic routing. Network devices were secured using SSH, ACLs, and port security.

Traffic Simulation: Tests were conducted for inter-VLAN routing, DHCP functionality, and failover mechanisms. Network traffic generation was used to analyze latency, throughput, and overall performance.

Validation: The configuration was verified for accuracy and connectivity. Redundancy and scalability were assured through failover tests.

3.1.3 Simulation

Packet Tracer Simulation: Packet Tracer was utilized to simulate and test the designed network. It provided a virtual environment to design, configure, and test network scenarios.

- **Network Topology Design:** Based on requirements, the topology was developed on Packet Tracer, including routers, switches, PCs, and servers.
- **Configuration Implementation:** Configurations for switches, routers, and hosts were implemented as per the topology. Devices were configured to simulate real Cisco hardware.
- **Simulation of Traffic:** Packet Tracer enabled simulation of network traffic and device communication. Network connectivity and data flow were tested to ensure proper functionality.
- **Verification of Redundancy and Failover:** The hierarchical design with redundancy at every layer, including multiple routers, multilayer switches, and ISP connections, was tested to verify failover mechanisms and ensure network resilience.
- **DHCP and IP Address Allocation:** Dynamic Host Configuration Protocol (DHCP) functionality and IP address allocation were tested to ensure that devices received the correct IP addresses dynamically and that devices in the server room had static IP assignment

3.2 Results Analysis/Testing

3.2.1 VLAN and Inter-VLAN Routing

Objective: Validate the isolation and communication between VLANs.

Results: VLANs successfully isolated departmental traffic, enhancing security and reducing broadcast traffic. Inter-VLAN routing via Layer 3 switches ensured seamless communication between VLANs.

3.2.2 DHCP and IP Allocation

Objective: Test the functionality of dynamic IP allocation.

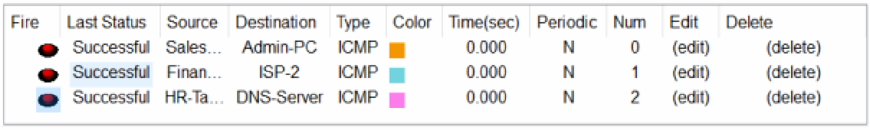
VLAN	Test	Result
VLAN 10 (Sales)	Intra-VLAN communication	Success
VLAN 10 ↔ VLAN 20 (HR)	Inter-VLAN communication	Success

Table 3.1: VLAN and Inter-VLAN Routing Results

Results: DHCP servers successfully allocated IPs within defined ranges for each VLAN. Static IPs were reserved for servers and routers to avoid conflicts.

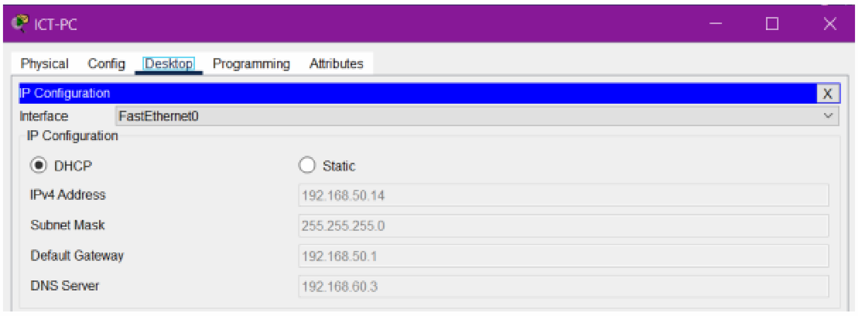
VLAN	DHCP Test	Result
VLAN 30 (Finance)	Automatic IP allocation	Success
VLAN 60 (Server Room)	Static IP for devices	Success

Table 3.2: DHCP and IP Allocation Results



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	Successful	Sales...	Admin-PC	ICMP	🟧	0.000	N	0	(edit)	(delete)
●	Successful	Finan...	ISP-2	ICMP	🟦	0.000	N	1	(edit)	(delete)
●	Successful	HR-Ta...	DNS-Server	ICMP	🟪	0.000	N	2	(edit)	(delete)

Figure 3.1: ICMP PDU check



ICT-PC

Physical Config Desktop Programming Attributes

IP Configuration

Interface FastEthernet0

IP Configuration

● DHCP ○ Static

IPv4 Address 192.168.50.14

Subnet Mask 255.255.255.0

Default Gateway 192.168.50.1

DNS Server 192.168.60.3

Figure 3.2: DHCP IP allocation

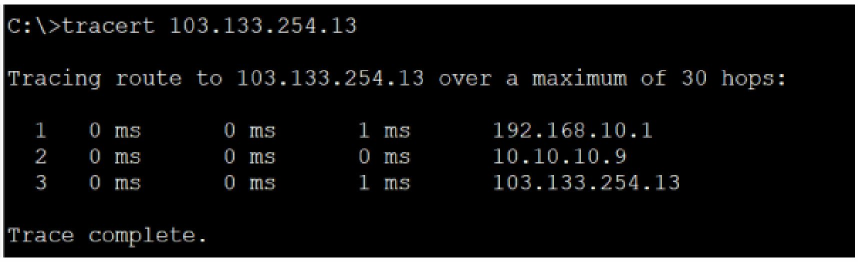
3.2.3 OSPF Routing

Objective: Ensure dynamic routing and efficient path selection.

Results: Routes dynamically updated during link failure simulations. All devices maintained connectivity without manual intervention.

Scenario	Test Description	Result
Normal Operations	OSPF routing between VLANs	Success
Link Failure	Alternate route selection	Success (No downtime)

Table 3.3: OSPF Routing Results



```
C:\>tracert 103.133.254.13

Tracing route to 103.133.254.13 over a maximum of 30 hops:

  1    0 ms      0 ms      1 ms      192.168.10.1
  2    0 ms      0 ms      0 ms      10.10.10.9
  3    0 ms      0 ms      1 ms      103.133.254.13

Trace complete.
```

Figure 3.3: Traceroute successful

3.2.4 Security Features

Objective: Test implemented security measures.

Results: SSH encrypted all remote management sessions. ACLs effectively blocked unauthorized traffic between VLANs. Port security restricted unauthorized device access.

Feature	Test Description	Result
SSH	Secure remote access	Success
ACL	Block unauthorized VLAN traffic	Success
Port Security	Prevent unauthorized devices	Success

Table 3.4: Security Feature Results

3.2.5 Redundancy and Scalability

Objective: Verify failover mechanisms and future expansion capability.

Results: Redundant links and dual ISPs ensured uninterrupted connectivity during simulated failures. Added new VLANs without affecting existing configurations.

Test Scenario	Action	Result
Failover Testing	Simulate primary link failure	Success
Scalability Testing	Add new VLAN (e.g., VLAN 70)	Success

Table 3.5: Redundancy and Scalability Results

3.2.6 Troubleshooting

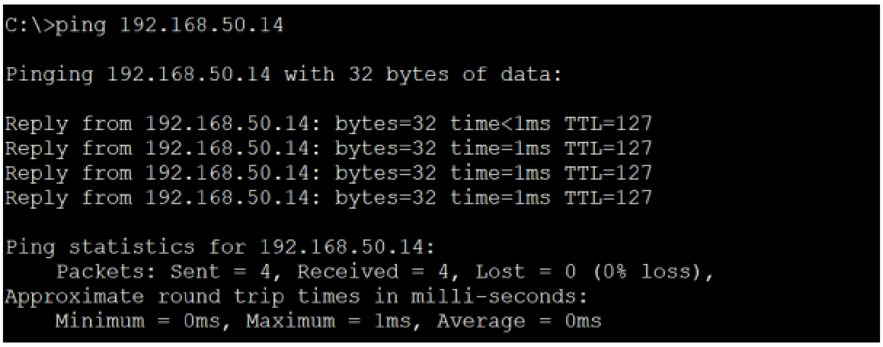
The following tasks were performed as part of standard troubleshooting during the implementation phase:

- **Device Connectivity:** Ensured that all devices within their respective VLANs could communicate both internally and across other departments. Multilayer switches were configured for inter-VLAN routing.

- **DHCP Issues:** Verified DHCP server connectivity and ensured that DHCP servers were reachable and capable of dynamically assigning IP addresses to devices.
- **Routing Configuration:** Conducted OSPF routing configurations on routers and multilayer switches to maintain proper routing table updates, enabling communication between different departments.
- **Access Control Issues:** Reviewed and modified Access Control Lists (ACLs) to permit authorized traffic while blocking unauthorized access.
- **Port Security:** Verified port security configurations on switchports in the Finance department to ensure only one device could connect per port. Checked that MAC addresses were correctly learned and applied.

3.2.7 Performance Metrics

Performance metrics, including network latency, throughput, redundancy testing, DHCP response time, inter-VLAN routing performance, security, QoS, and NAT/PAT functionality, were measured during testing to ensure optimal network operation.



```
C:\>ping 192.168.50.14

Pinging 192.168.50.14 with 32 bytes of data:

Reply from 192.168.50.14: bytes=32 time<1ms TTL=127
Reply from 192.168.50.14: bytes=32 time=1ms TTL=127
Reply from 192.168.50.14: bytes=32 time=1ms TTL=127
Reply from 192.168.50.14: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.50.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Figure 3.4: performance measure through ping time

3.2.8 Output

Core Layer

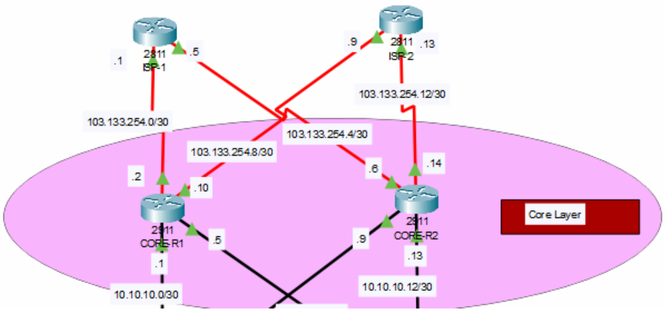


Figure 3.5: Core Layer

Distribution Layer

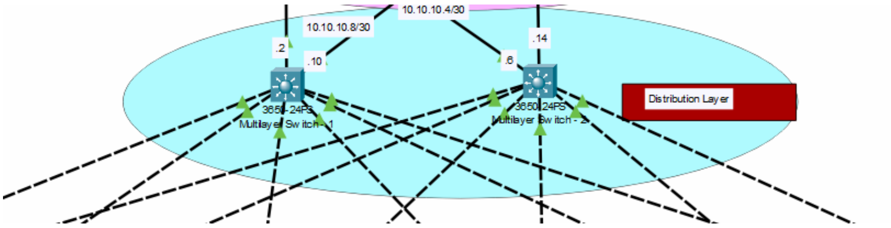


Figure 3.6: Distribution Layer

Access Layer

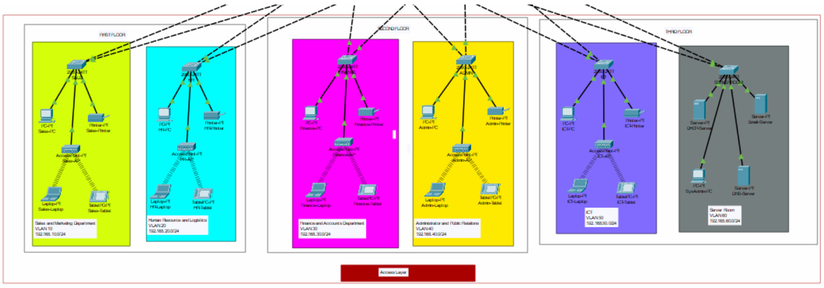


Figure 3.7: Access Layer

Final Outlook

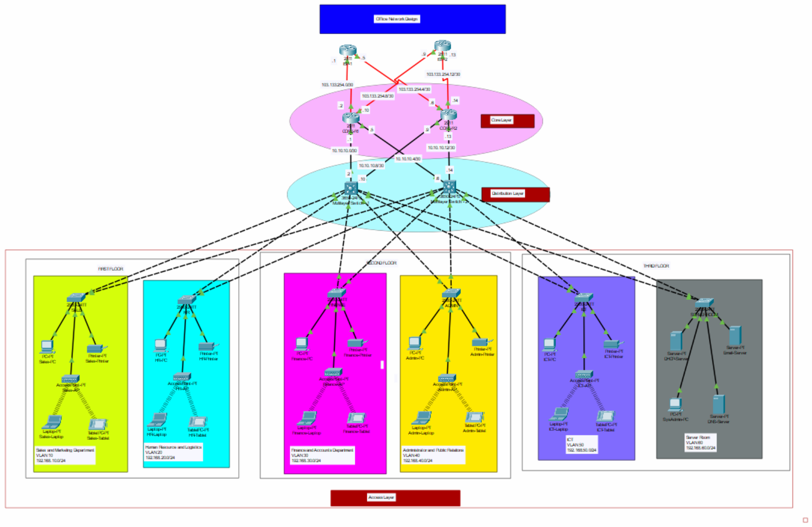


Figure 3.8: Final Outlook

3.3 Results Overall Discussion

General Observations

By fulfilling all of the design objectives, the network operated effectively under simulated conditions. VLAN segmentation reduced broadcast domains and isolated data, enhancing network performance. OSPF provided reliable routing, which adapted dynamically to changes in the network.

Challenges

- **ACL Configuration:** The configuration of ACLs required exact rules to avoid inadvertent traffic blocks, which could disrupt network functionality.
- **DHCP Misconfigurations:** Initial misconfigurations in DHCP led to IP address allocation issues. These issues were identified and resolved during testing, ensuring proper dynamic IP assignment.

3.3.1 Complex Engineering Problem Discussion

- **Depth of Knowledge:** The project successfully applied advanced networking knowledge, particularly OSPF, VLANs, and security protocols, which allowed for efficient routing and network segmentation.
- **Interdependence:** The interaction between DHCP, OSPF, VLANs, and ACLs highlighted the importance of cohesive configuration. Misconfigurations in one area can affect the entire network.
- **Stakeholder Involvement:** The network was designed to address office-specific needs while also ensuring scalability to accommodate future growth or changes in requirements.

Chapter 4

Conclusion

This finally develops the Office Network Design Using Cisco Packet Tracer to establish the principles of modern network design. The project utilizes an organized approach in network architectural design that is scalable, secure, and provides efficient service to satisfy office demands with regard to operations. Similarly, there are specific limitations within this research process, but they help create room for further enhancements of the research. The project thus highlights the need for prudent network planning and simulation as a way of handling such complex engineering problems and meeting the technological challenges.

4.1 Discussion

A secure, scalable, and reliable network infrastructure has been developed and simulated with satisfaction thanks to the Office Network Design Using Cisco Packet Tracer. Through the implementation of a hierarchical model, VLAN segmentation, OSPF routing, and redundancy countermeasures, the project will fully satisfy the essential requirements for trouble-free office operations. Of course, crucial functionalities under test included but were not limited to: DHCP, which dynamically doles out IP addresses and inter-VLAN communication, with NAT enforcing efficient Internet access.

4.2 Limitations

Despite the success of the project, during implementation and testing, some limitations were realized:

Simulation Constraints

The testing was in a simulated environment in Cisco Packet Tracer. The implementation may be subject to some changes when done in real life because of hardware performance and complexities of network traffic.

Support for IPv6

IPv4 addressing is primarily used in the network design. Upgrades will be required in the future to integrate contemporary protocols due to the increasing usage of IPv6.

QoS

It is not feasible to implement and test every QoS configuration due to the nature of the simulation environment. Thus, prioritization of the real-time traffic for Voice and Video applications couldn't be done.

Scalability Issues

The network, although it is designed to support several more VLANs and devices, might need configurations a bit more advanced than what has been set up if multiple ISPs or cloud services are integrated on the network.

4.3 Scope of Future Work

The project provides a very good basis for any future enhancement and scaling. The scope of potential future work will look something like the following:

IPv6 Implementation

Migrate to IPv6 addressing to ensure scalability and address space.

Integration with Cloud Services

Integrate cloud storage, applications, and monitoring systems for increased network capability.

Advanced Monitoring of the Network

SolarWinds or Nagios will be implemented to show in real time, network performance and security monitoring and analysis.

Enhanced Security

The intrusion detection and prevention system shall be implemented on the network, together with periodic security audits in order to make the mechanisms of the network's defense stronger.

Extension of Wireless Network

Include more wireless access points to enable roaming without glitch to enhance user mobility and protection with WPA3.

Energy Efficiency

Consider optimization of the configuration of all network hardware in order to achieve minimal power consumption, which will provide alignment with environmental sustainability objectives.

QoS Configuration and Testing

Include proper QoS configuration and extensive testing to make sure that critical traffic will be prioritized, thus voice and video communications.

Training Programs

Design training and workshops that would empower the IT staff to effectively manage the network and perform troubleshooting.

Automation

Integrate network automation to ease device configuration; hence, assure consistent policy enforcement.

References

1. Cisco Systems. *Cisco Packet Tracer - Networking Simulation Tool*. Available at: https://www.netacad.com/courses/packet-tracer. Accessed: December 2024.

2. Forouzan, B. A. (2017). *Data Communications and Networking*. McGraw-Hill Education.

3. Stallings, W. (2019). *Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud*. Addison-Wesley Professional.

4. Tanenbaum, A. S., and Wetherall, D. J. (2020). *Computer Networks*. Pearson Education.

5. Cisco Networking Academy. *Routing and Switching Essentials Companion Guide*. Cisco Press, 2016.

6. IEEE Standards Association. *IEEE 802.1Q - Virtual LANs (VLANs)*. Available at: https://standards.ieee.org/. Accessed: December 2024.

7. Rouse, M. *Dynamic Host Configuration Protocol (DHCP)*. TechTarget. Available at: https://www.techtarget.com/. Accessed: December 2024.

8. Cisco Systems. *Understanding and Configuring OSPF*. Available at: https://www.cisco.com/. Accessed: December 2024.

9. SolarWinds. *Network Performance Monitoring Tools*. Available at: https://www.solarwinds.com/. Accessed: December 2024.

10. Green University of Bangladesh. *Project Guidelines: Place Your Project Title Here Document*, 2022.

Appendices

Abbreviations

- ACL - Access Control List
- DHCP - Dynamic Host Configuration Protocol
- IP - Internet Protocol
- OSPF - Open Shortest Path First
- PAT - Port Address Translation
- QoS - Quality of Service
- SSH - Secure Shell
- VLAN - Virtual Local Area Network