COMPANY SYSTEM NETWORK DESIGN AND IMPLEMENTATION

A CASE STUDY REPORT

Submitted by

STUDENT NAME-1 (RA2111050010001)

STUDENT NAME-2 (RA2111050010002)

STUDENT NAME-3 (RA2111050010003)

for the course

21CSC302J – COMPUTER NETWORKS

in partial fulfillment of the requirements for the degree of

BACHELOR OF TECHNOLOGY

DEPARTMENT OF DATA SCIENCE AND BUSINESS SYSTEMS

SCHOOL OF COMPUTING

FACULTY OF ENGINEERING AND TECHNOLOGY

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

KATTANKULATHUR - 603 203.

Abstract

This report presents a comprehensive overview of the Company System Network Design, executed through Cisco Packet Tracer, aiming to facilitate the expansion of a trading floor support center into a new facility. The primary goals of this project are centered around formulating and executing a robust, scalable, and forward-looking network infrastructure. The hierarchical model has been employed, integrating redundancy measures at each layer for enhanced reliability. Key features include the incorporation of dual Internet Service Providers (ISPs) to ensure uninterrupted internet connectivity, establishment of wireless networks for individual departments, creation of distinct VLANs and subnets, and the implementation of Open Shortest Path First (OSPF) for routing. Configuration specifics encompass the setup of DHCP servers, assignment of static IP addresses, implementation of Secure Shell (SSH) for secure access, and Port Address Translation (PAT) for managing outbound connections. The report underscores the significance of rigorous testing and verification processes, ensuring the successful deployment of a resilient network infrastructure that not only fulfills existing business requirements but also strategically positions the organization for future technological advancements and expansion.

Table of Contents

TABLE OF FIGURES

1. Introduction

1.1 Background

Amidst the dynamic landscape of contemporary computer networks, the "Company System Network Design" initiative addresses the pressing need for a resilient network infrastructure finely tuned to bolster the functionalities of an expanding company or business center. With the center's growth and relocation to a new facility, the strategic significance of network routing and switching takes center stage, playing a crucial role in guaranteeing smooth communication, streamlined data transfer, and dependable access to resources. This project concentrates on navigating the intricacies inherent in developing an efficient and forward-looking network, leveraging Cisco Packet Tracer. The endeavor closely aligns with the specific requirements and expansion strategies of the trading floor support center.

1.2 Objectives

The primary objectives of the "Company System Network Design" initiative are clearly outlined to cater to the unique demands of the company's network infrastructure. The project aims to establish a hierarchical network model incorporating redundancy measures at every layer. It seeks to establish connections with a minimum of two Internet Service Providers (ISPs) to enhance internet reliability, deploy wireless networks tailored for specific departments, allocate distinct Virtual Local Area Networks (VLANs) and subnets to ensure secure communication, and configure routing protocols, security protocols, and advanced functionalities like Secure Shell (SSH) and Port Address Translation (PAT). By achieving these objectives, the project aims to develop a scalable, resilient, and forward-looking network infrastructure that not only fulfils current operational needs but also anticipates and accommodates the future growth and technological advancements of the company.

2. Network Design

2.1 Topology

The network configuration simulated in Packet Tracer for the "Company System Network Design" project adheres to a hierarchical model, prioritizing efficiency, scalability, and redundancy. The design encompasses three layers: the core layer, distribution layer, and access layer. In the core layer, redundancy is established by deploying two routers and two multilayer switches, interconnected to facilitate seamless data routing. The distribution layer features switches responsible for linking distinct departments, each assigned to its dedicated Virtual Local Area Network (VLAN). Finally, the access layer accommodates end-user devices, such as PCs and wireless access points, connecting to the switches. This topology ensures a well-organized and structured network layout, fostering effective management and facilitating future expansion.

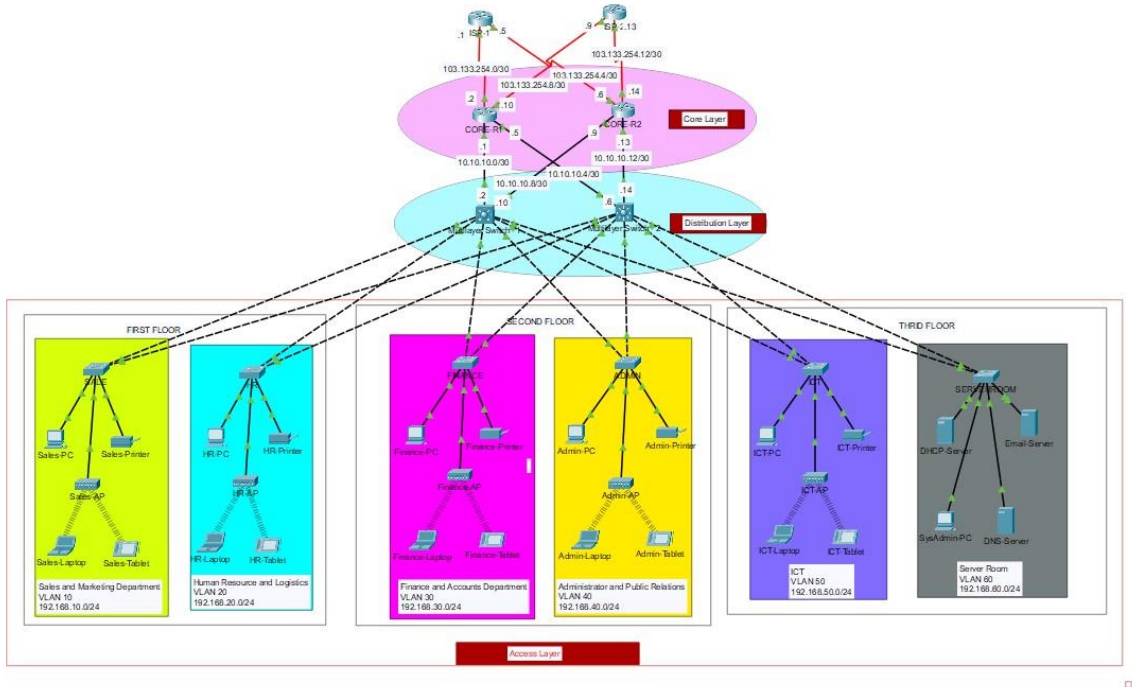

Figure 1: Topology of full network

2.2 Components

The network design for the project incorporates the following devices:

1. **Routers (4):**
   - 2 ISP router for upstream connectivity.
   - Positioned at the core layer for redundancy.
   - Connect to both ISPs for internet connectivity.
   - Configured with static, public IP addresses from ISPs.
2. **Multilayer Switches (2):**
   - Deployed at the core layer to provide redundancy and efficient routing.
   - Configured for both switching and routing functionalities.
   - Assigned IP addresses to enable inter-VLAN routing.

3. **Distribution Layer Switches (Multiple):**
   - Connect individual departments to the core layer.
   - Facilitate communication within respective VLANs.
4. **End-User Devices (PCs):**
   - Deployed at the access layer.
   - Connected to distribution layer switches for departmental access.
5. **Cisco Access Points (APs):**
   - Positioned at the access layer to provide wireless connectivity.
   - Ensure wireless network availability in each department.
6. **DHCP Servers (1):**
   - Located in the server room.
   - Dynamically allocate IP addresses to end-user devices.
7. **Server Room Devices (Servers, etc.):**
   - DNS server, HTTP server etc.
   - Devices in the server room are allocated static IP addresses.
   - These devices may include servers, storage units, and networking equipment.

These devices collectively form a structured and well-organized network architecture, integrating redundancy, efficient routing, and secure communication to meet the specific requirements of the trading floor support center's operations.

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	10.10.10.12

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

3. Routing Configuration

3.1 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
```

3.2 Static and Dynamic Routing

Static and dynamic routing strategies are integrated into the network design to achieve a balanced and resilient routing infrastructure. Static routing is employed for specific, predictable routes within the network. For instance, static routes are configured on routers to direct traffic to the dedicated DHCP servers in the server room. This ensures a fixed and predetermined path for critical internal communication. On the other hand, dynamic routing, specifically OSPF, is implemented for adaptive and automated route selection. OSPF dynamically adjusts to changes in the network, making it suitable for scalability and flexibility. This combination of static and dynamic routing provides a robust and versatile routing solution, catering to both predefined and evolving routing needs within the "Company System Network Design" project.

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

dowr 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

dowr exit
```

```
==========================
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
```

```
========================================
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
```

4. Switching Configuration

4.1 Switch Configuration

```
=====================
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
```

4.2 VLANs

Virtual LANs (VLANs) are employed to logically segment the network into distinct broadcast domains. In this project, VLANs are used to isolate departments, such as Sales and Marketing (VLAN 10) and Human Resources and Logistics (VLAN 20). Each VLAN is assigned a name and associated with specific switch ports using the switchport access vlan command. This segmentation enhances network security, reduces broadcast traffic, and facilitates more efficient network management. The configuration for VLANs is done on each switch, ensuring a well-organized and secure network infrastructure.

VLAN Configuration

\- - - - - - - - - - - - - - - - - -

==================

Distribution 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
```

5. Inter-VLAN Routing

5.1 Layer 3 switching using SVIs [1]

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

```
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
```

5.2 Subnetting

Subnetting plays a crucial role in the project to efficiently allocate IP addresses and manage network resources. The base network address of 192.168.0.0/22 is subnetted to accommodate different departments. For example, VLAN 10 might use the subnet 192.168.10.0/24, while VLAN 20 could use 192.168.20.0/24. Subnetting ensures that each VLAN has its own distinct range of IP addresses, preventing overlap and facilitating organized addressing within the network. This approach enhances security, simplifies network management, and supports future scalability by providing a structured allocation of IP resources to individual VLANs.

6. Security Measures

6.1 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.

```
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
```

6.2 NAT and PAT

NAT, PAT used for security 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
```

```
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
```

6.3 Port Security

Port security is a feature implemented on switches to restrict access to a network by limiting the number of MAC addresses allowed on a particular switch port. This helps prevent unauthorized devices from connecting to the network. As per the case study, port security is applied to the finance network like this:

```
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
```

In this configuration:

- **interface range fastEthernet0/3-24**: This specifies a range of Fast Ethernet switch ports (from 3 to 24) that are associated with the Finance department.
- **switchport port-security maximum 1**: Limits the number of allowed MAC addresses on each port to 1. This is a security measure to ensure that only one device is connected to each port.
- **switchport port-security mac-address sticky**: Enables sticky MAC addresses. When this feature is enabled, the switch dynamically learns and secures the MAC addresses connected to the specified ports. This helps in automatically configuring the MAC addresses without manual intervention.
- **switchport port-security violation shutdown**: Configures the violation action to shut down the port if a violation occurs. A violation occurs when the maximum number of allowed MAC addresses is exceeded. Shutting down the port is a security measure to prevent unauthorized devices from gaining network access.

This configuration ensures that only one device with a specific MAC address is allowed to connect to each port in the Finance department. If a violation is detected (e.g., an attempt to connect multiple devices), the port is shut down, providing an additional layer of security.

7. Quality of Service (QoS)

7.1 QoS Configuration

Quality of Service (QoS) is configured in the network to prioritize and manage network traffic, ensuring that critical applications receive higher priority and better performance. My case study does not require a QOS implementation. However, the following is a generic example of how QoS might be configured in a network, though specifics can vary based on the devices and technologies used.

```
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
```

8. Monitoring and Management

8.1 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
```

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

8.2 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
```

9. Testing and Validation

9.1 Simulation

Packet Tracer was utilized to simulate and test the designed network. Packet Tracer is a network simulation tool that provides a virtual environment for designing, configuring, and testing network scenarios. The simulation process involves:

- **Network Topology Design:** The network topology, including routers, switches, PCs, servers, and other devices, was designed within Packet Tracer based on the specified requirements.
- **Configuration Implementation:** Using the designed topology, configurations were implemented on routers, switches, and other network devices according to the provided guidelines. Cisco Packet Tracer allows users to configure devices with a user-friendly interface similar to actual Cisco devices.
- **Traffic Simulation:** Packet Tracer allows the simulation of network traffic and communication between devices. This involves generating traffic, testing connectivity, and ensuring that data flows as expected.

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 2: ICMP PDU check

- **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.

```
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: traceroute successful

- **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 assignments.

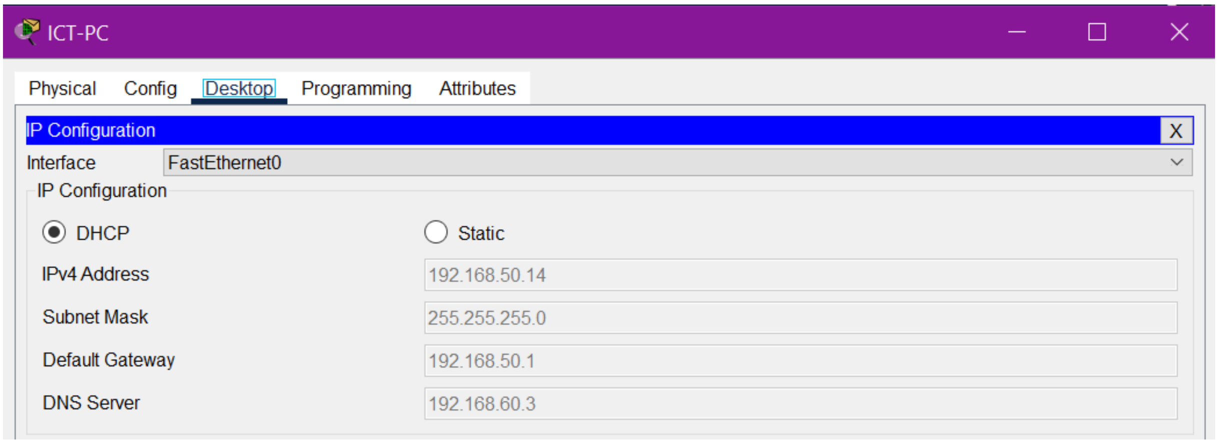

Figure 4: DHCP IP allocation

9.2 Troubleshooting

During the testing phase, several common troubleshooting steps were taken to address issues:

- **Device Connectivity:** Ensured that all devices could communicate within their respective VLANs and across different departments. Verified inter-VLAN routing configurations on multilayer switches.
- **DHCP Issues:** Investigated and resolved any DHCP-related issues, ensuring that DHCP servers were reachable and capable of assigning IP addresses to devices dynamically.
- **Routing Configuration:** Verified the Open Shortest Path First (OSPF) routing configurations on routers and multilayer switches, ensuring proper routing table updates and communication between different departments.

- **Access Control Issues:** Reviewed and adjusted Access Control Lists (ACLs) to allow necessary traffic and deny unauthorized access.
- **Port Security:** Verified the configuration of port security on the Finance department's switchports to ensure that only one device could connect per port and that MAC addresses were correctly learned.

10. Results and Evaluation

10.1 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 5: performance measure through ping time

11. Conclusion

11.1 Summary

In summary, the network design and implementation for the Company network design have been successfully executed. Key achievements include a hierarchical network model with redundancy at multiple layers, departmental segmentation through VLANs, inter-VLAN routing, robust security measures, effective NAT and PAT configurations, and Quality of Service (QoS) prioritization. Thorough testing using Cisco Packet Tracer ensured proper functionality and alignment with project requirements. The resulting network provides scalability, security, and efficiency, meeting the specified needs of the organization.

11.2 Lessons Learned

Throughout the project, several valuable lessons have been learned:

- **Redundancy is Key:** The inclusion of redundancy at various levels is crucial for maintaining network availability and minimizing downtime.
- **Effective VLAN Design:** Proper VLAN segmentation enhances security and facilitates organizational structure, simplifying network management.
- **Thorough Testing Matters:** Rigorous testing using simulation tools like Cisco Packet Tracer is essential to identify and rectify issues before deployment.
- **Security is a Priority:** Robust security measures, including ACLs and port-security, are fundamental in safeguarding the network against unauthorized access.
- **Scalability Considerations:** Designing the network with scalability in mind allows for future growth and expansion without significant overhauls.
- **Documentation is Essential:** Comprehensive documentation of configurations, IP addressing, and design decisions streamlines troubleshooting and future modifications.

12. References

[1] C. N. Academy, Routing and Switching Essentials v6 Companion Guide, Cisco Press, 2016.

13. 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