Eastern University

A Leader in Quality Education

**Project Report** on

# “Company Network System”

**Course Code**: CSE-416

**Course Title:** Computer Network Lab

**Submitted to**

Momtaj Hossain Mow(Lecturer)
Department of CSE
Eastern University

**Submitted by**

Nur-A Khadija Khandaker Piya
ID : 222400003
Department of CSE

# Contents

## Introduction

In the modern era of information and communication technology, an efficient and secure network infrastructure is crucial for any business organization. Our project, titled **"Company System Network Design,"** aims to simulate a real-world enterprise network using Cisco Packet Tracer, focusing on structured connectivity, departmental segmentation, internet access, and robust network security.

## Objectives

The primary objectives of this project are as follows:

- **Design a hierarchical company network model** simulating a real-world corporate environment.
- **Segment departments using VLANs** for improved security, traffic management, and isolation.
- **Implement inter-VLAN routing** using **Layer 3 switches** for seamless communication across VLANs.
- **Configure dynamic routing using OSPF** to ensure efficient path selection and fast convergence.
- **Implement DHCP** for automated and centralized IP address management.
- **Enhance network security** using **SSH**, **Access Control Lists (ACLs)**, **Port Security**, and **NAT**.
- **Simulate dual ISP connections** for redundancy and automatic failover.

## Company Scenario

The company is relocating to a newly constructed three-story office building, with each floor housing specific departments:

- **First Floor:** Sales & Marketing, Human Resources & Logistics
- **Second Floor:** Finance & Accounts, Administration & Public Relations
- **Third Floor:** ICT Department, Server Room

## IP Addressing Scheme

For the IP addressing, the **10.0.0.0/16** private IP block is used. The addressing scheme for each department is as follows:

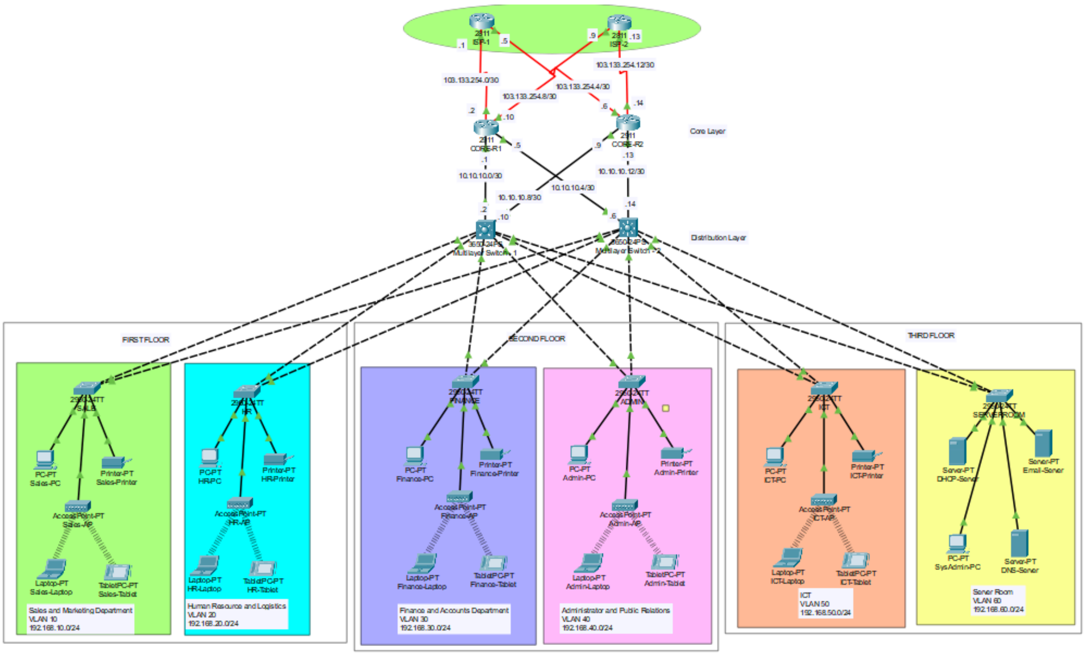
| Department | VLAN | Subnet | Subnet Mask | Gateway |
|---|---|---|---|---|
| Sales & Marketing | 10 | 10.10.10.0/24 | 255.255.255.0 | 10.10.10.1 |
| Human Resources & Logistics | 20 | 10.10.20.0/24 | 255.255.255.0 | 10.10.20.1 |
| Finance & Accounts | 30 | 10.10.30.0/24 | 255.255.255.0 | 10.10.30.1 |
| Administration & Public Relations | 40 | 10.10.40.0/24 | 255.255.255.0 | 10.10.40.1 |
| ICT Department | 50 | 10.10.50.0/24 | 255.255.255.0 | 10.10.50.1 |
| Server Room | 60 | 10.10.60.0/24 | 255.255.255.0 | 10.10.60.1 |
| Management VLAN (Admin PCs) | 99 | 10.10.99.0/24 | 255.255.255.0 | 10.10.99.1 |
| **ISP Connections** | N/A | 192.168.100.0/30 | 255.255.255.252 | - |

## Network Design:

### Topology:

The network design follows a hierarchical structure, consisting of core, distribution, and access layers. This model is chosen for its scalability and redundancy, which ensures high availability and fault tolerance. The core layer includes redundant routers and multilayer switches, which provide efficient routing and switching functions. The distribution layer connects various departmental networks, while the access layer provides connectivity to end-user devices such as computers, printers, and wireless access points.

### Figure: Network Topology



## Components

The network design incorporates several key components:

- **Routers (4):** Two core routers, each connected to one ISP for internet access, and two additional routers for internal routing and redundancy.
- **Multilayer Switches (2):** These switches perform both Layer 2 switching and Layer 3 routing functions, providing flexibility and efficient traffic management.
- **Switches (2):** Distribution layer switches that connect the departments to the network.

- **End-user Devices (PCs, Printers, etc.):** Located at the access layer, these devices connect to distribution switches for network access.

- **Cisco Access Points:** Used to provide wireless connectivity to departments, ensuring mobility for end-users.

- **DHCP Server:** Allocates dynamic IP addresses to end-user devices, minimizing manual configuration.

- **Servers:** Hosts providing DNS, HTTP, and other essential services, with static IP addresses for reliable access.

**Core Network Features:**

**a. VLAN Segmentation**

Each department is assigned a unique VLAN to logically separate traffic, enhancing security and reducing unnecessary broadcast domains.

**b. Inter-VLAN Routing**

The Layer 3 switch is configured to route traffic between VLANs using **SVIs (Switch Virtual Interfaces)**.

**c. DHCP Configuration**

**DHCP** is configured on the core switch to dynamically assign IP addresses to all devices, with separate pools for each VLAN subnet.

**d. OSPF Dynamic Routing**

**OSPF** is implemented across the Layer 3 switch and routers, facilitating the dynamic sharing of routing information for optimal routing paths.

**e. NAT and Internet Access**

**NAT** is configured on the edge routers to allow internal private IP addresses to access external public resources, with translation done on the public-facing router interfaces.

**f. Redundancy with Dual ISPs**

Two routers (ISP1 and ISP2) are connected to the core switch to ensure **automatic failover** in case one ISP goes down.

### g. SSH and Network Security

SSH is configured for secure remote management of the network devices. **Port Security** is implemented to limit access to authorized devices only, and **ACLs** are configured to restrict traffic between different VLANs based on organizational policies.

## Configuration Overview

### VLAN Configuration on Core Switch:

```
interface vlan 10
 ip address 10.10.10.1 255.255.255.0
interface vlan 20
 ip address 10.10.20.1 255.255.255.0
ip routing
```

### OSPF Configuration:

```
router ospf 1
 network 10.10.0.0 0.0.255.255 area 0
 network 192.168.100.0 0.0.0.3 area 0
```

### NAT Configuration on Router:

```
access-list 1 permit 10.10.0.0 0.0.255.255
ip nat inside source list 1 interface g0/1 overload
```

## Testing and Validation

- **Inter-VLAN Communication:** Verified successful communication between devices in different VLANs using **ping** tests.

- **Internet Access:** Tested using simulated external servers, confirming that the network can access the internet.
- **Redundant Routing:** Validated **automatic failover** by disconnecting ISP1, ensuring uninterrupted network access.
- **DHCP:** Confirmed that devices in each VLAN are correctly assigned IP addresses.
- **SSH Access:** Validated secure remote access to the core switch from an Admin PC.

### Challenges and Solutions

| Challenge | Solution Implemented |
|---|---|
| VLAN misconfiguration | Rechecked trunk and access port settings |
| Inter-VLAN routing issues | Verified SVI configurations |
| NAT issues | Checked ACLs and NAT overload syntax |
| Redundant links causing loops | Enabled **STP (Spanning Tree Protocol)** |

### Conclusion

This project successfully demonstrates the design and implementation of a scalable, secure, and efficient enterprise network for a multi-department company. All objectives, including VLAN segmentation, inter-VLAN routing, dynamic routing with OSPF, redundancy, and network security, were successfully met.

## Future Work

- **Implement centralized AAA authentication** for more robust security.
- **Add wireless access points** with **WPA2 Enterprise** for secure wireless communication.
- **Integrate real-time network monitoring tools** for proactive management.
- Enhance failover using **HSRP or VRRP** for router redundancy.

## References

- Cisco Packet Tracer Simulation Tool
- Cisco Networking Academy Resources
- CCNA Routing and Switching Guide
- Lecture Notes and Lab Assignments