RV UNIVERSITY

Go, change the world

an initiative of RV EDUCATIONAL INSTITUTIONS

CS2120 COMPUTER NETWORKS

Mini Project Report

Company System Network Design

Submitted

By

Aditi Gopinath (1RVU23CSE026)

Aditya Kumar (1RVU23CSE029)

Prerana M Shirur (1RVU23CSE354)

Under the guidance of:

Prof. Rajeev B R

School of Computer Science and Engineering

RV University, Bangalore

RV UNIVERSITY

Go, change the world

an initiative of RV EDUCATIONAL INSTITUTIONS

School of Computer Science and Engineering

CERTIFICATE

Certified that the CS2120 Computer Networks Mini Project work titled *Company Network Design* is carried out by *Aditi Gopinath (1RVU23CSE026), Aditya Kumar (1RVU23CSE029) and Prerana M Shirur (1RVU23CSE354)* who are bonafide students of the School of Computer Science and Engineering, RV University, Bengaluru, during the year 2024–25. It is certified that all corrections/ suggestions from all the continuous internal evaluations have been incorporated into the project and in this report.

Dr./ Prof. _____

Faculty Guide

Dr. Sudhakar K. N

Program Director

1 Problem statement

1.1 Context and Need for Network Design

In the modern business era with its advanced technologies, smooth communication, safe data transfer, and **scalable infrastructure** are of paramount concern. With the growth of businesses and relocations to new physical premises, the basis of the business lies in the dependability and performance of its internal network. The "**Company System Network Design**" project emulates the network infrastructure of a trading floor support center moving into a new building. The move necessitates the deployment of an expandable and reliable network that supports the growing demands of different departments and ensures smooth internet connectivity, internal communication, and remote access to services.

To address this, the simulation is performed within **Cisco Packet Tracer**, and various configurations like dual ISPs, inter-VLAN routing, redundant devices, and multiple subnets are used to emulate the actual deployment of a business-grade network. This simulation is used to pave the way for learning about hands-on uses of routing, switching, segmentation, and security protocols in business scenarios.

1.2 Objective and Scope

The primary goal of this project is to implement and deploy a hierarchical, secure, and scalable network. This is done by implementing a three-tier network design model:

- **Core Layer:** Holds routers and multilayer switches for high-speed interconnects and redundancy.
- **Distribution Layer:** Interconnects departmental switches and regulates traffic between VLANs.
- **Access Layer**: Provides end-user connectivity, wired and wireless.

Principal goals are:

- Offering redundancy and failover features by the use of dual routers, multilayer switches, and dual ISP links.
- Establishment of different VLANs for different departments (i.e., Sales, HR, Finance) to separate and safeguard.
- Implementing DHCP for dynamic IP and static IPs in high-priority areas like the server room.
- Incorporating OSPF as the dynamic routing protocol for flexibility and route optimization.
- SSH, ACLs, and Port Security configuration for administrative access and traffic management.
- Facilitating NAT/PAT for external connectivity using sparse public IPs.

This simulation not only addresses the current operational needs but also prepares the network for future growth, technology developments, and higher-level network services like monitoring, cloud integration, and virtualization.

2. Introduction

2.1 Overview of the Company Network

A modern infrastructure trading floor support center network has received a customized simulated design which matches its functional demands. The simulation constructs a network through Cisco Packet Tracer utilizing a modular structure which provides distinct partitions and backup capabilities and unified commands.

The topology consists of:

- Two redundant core routers work together with multilayer switches (MLTSW) to maintain fault tolerance and optimize load distribution. These multifunctional equipment unite both Internet service providers while maintaining their position as communication centers for additional network layers.
- The distribution switches function as individual points of connection for Sales, HR, Finance, Admin and ICT departments which maintain separate VLANs to provide departmental segmentation across multiple floors.
- The system manages end-user connection through wired ports along with wireless signals by using Cisco APs to supervise both.
- DNS and HTTP servers possess static Internet Protocol addresses through Server VLAN 60 to provide internal services connection.
- The DHCP Server function handles automatic IP allocation for non-server devices.

The infrastructure supports independent operations and efficient management alongside better traffic control while planning for future additions of new business units within and outside corporate locations.

2.2 Technologies and Protocols Used

The configuration implements contemporary network protocols alongside security features which results in a useful network infrastructure that will remain operational into the future. The following provides details about important technologies employed:

OSPF (Open Shortest Path First):

The core routers and switches employ OSPF to operate as their dynamic routing protocol. OSPF works as a perfect solution for the described multi-layer environment because it delivers automatic route discovery and fault tolerance capabilities.

VLANs (Virtual Local Area Networks):

Each department possesses its own VLAN (Sales has VLAN 10 and HR has VLAN 20) and gets attached to distribution switch ports. The implementation of VLANs delivers two essential advantages by reducing broadcast domain size and optimizing performance and boosting security levels.

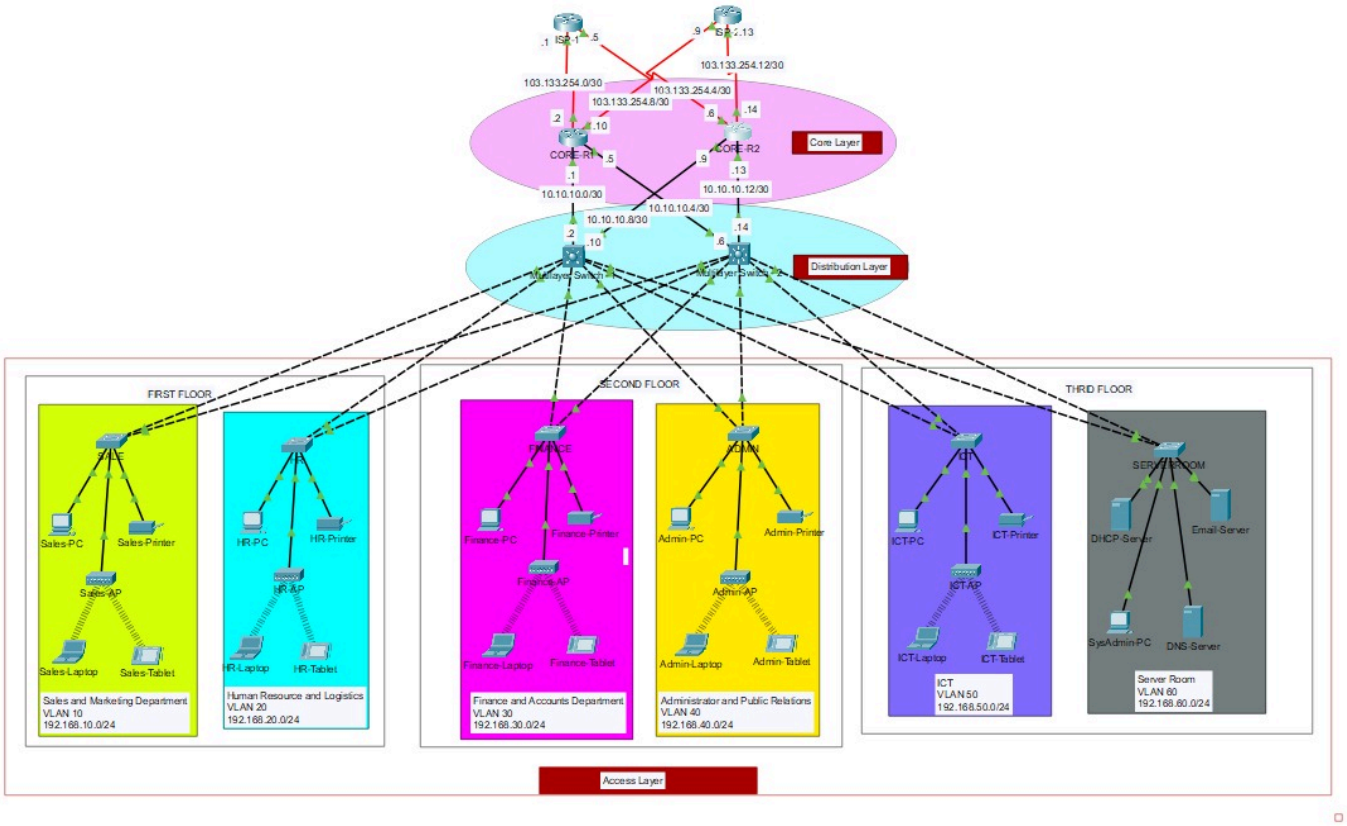
SSH (Secure Shell):

The remote access feature of all routers and switches through SSH provides administrative security because it encrypts login sessions and authentication credentials.

PAT/NAT:

The combination of Port Address Translation allows private internal network addresses to obtain public addresses when reaching the internet thus enabling several devices to share constrained internet addresses with their internal locations remaining anonymous.

3 Network Diagram



4. Configuration setup

4.1 Topology

The proposed network follows a three-tier hierarchical model, promoting efficiency, scalability, and redundancy:

- Core Layer: Two routers and two multilayer switches are configured with redundant links for high availability.
- Distribution Layer: Switches connect specific departments and manage traffic within their respective VLANs.
- Access Layer: End-user devices (PCs and wireless APs) connect to switches, enabling direct user access.

This structure ensures systematic communication, easier troubleshooting, and scalability for future network additions.

4.2 Network Components

Component	Description
Routers (4)	- 2 for ISP uplink- Located in the core layer- Redundant setup- Assigned public IPs from ISPs
Multilayer Switches (2)	- Positioned in the core- Support both routing and switching- Enable inter-VLAN communication
Distribution Switches	- Connect departments to the core- Handle VLAN-based routing
End-user PCs	- Located at the access layer- Connected to distribution switches
Access Points (APs)	- Provide wireless access- Placed in each department
DHCP Server (1)	- Allocates IPs dynamically to end-user devices
Server Room Devices	- Include DNS, HTTP, and other servers- Assigned static IPs- Used for services and storage

4.3 IP Addressing Scheme

Base Network: 192.168.0.0/22

First Floor

Department	Network Address	Subnet Mask	Host IP Range	Broadcast Address
Sales & Marketing	192.168.10.0	255.255.255.0 (/24)	192.168.10.1 - 192.168.10.254	192.168.10.255
HR & Logistics	192.168.20.0	255.255.255.0 (/24)	192.168.20.1 - 192.168.20.254	192.168.20.255

Second Floor

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

Third Floor

Department	Network Address	Subnet Mask	Host IP Range	Broadcast Address
ICT	192.168.50.0	255.255.255.0 (/24)	192.168.50.1 - 192.168.50.254	192.168.50.255
Server Room	192.168.60.0	255.255.255.0 (/24)	192.168.60.1 - 192.168.60.254	192.168.60.255

Core Router – Multilayer Switch Connections

Link	Network Address	Subnet Mask	IP Range	Broadcast Address
Core R1 - MLTSW1	10.10.10.0	255.255.255.252 (/30)	10.10.10.1 - 10.10.10.2	10.10.10.3
Core R1 - MLTSW2	10.10.10.4	255.255.255.252 (/30)	10.10.10.5 - 10.10.10.6	10.10.10.7
Core R2 - MLTSW1	10.10.10.8	255.255.255.252 (/30)	10.10.10.9 - 10.10.10.10	10.10.10.11
Core R2 - MLTSW2	10.10.10.12	255.255.255.252 (/30)	10.10.10.13 - 10.10.10.14	10.10.10.15

5. Results

5.1. ICMP PDU Check

The proof of device connectivity across networks uses ping testing through Cisco Packet Tracer.

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)

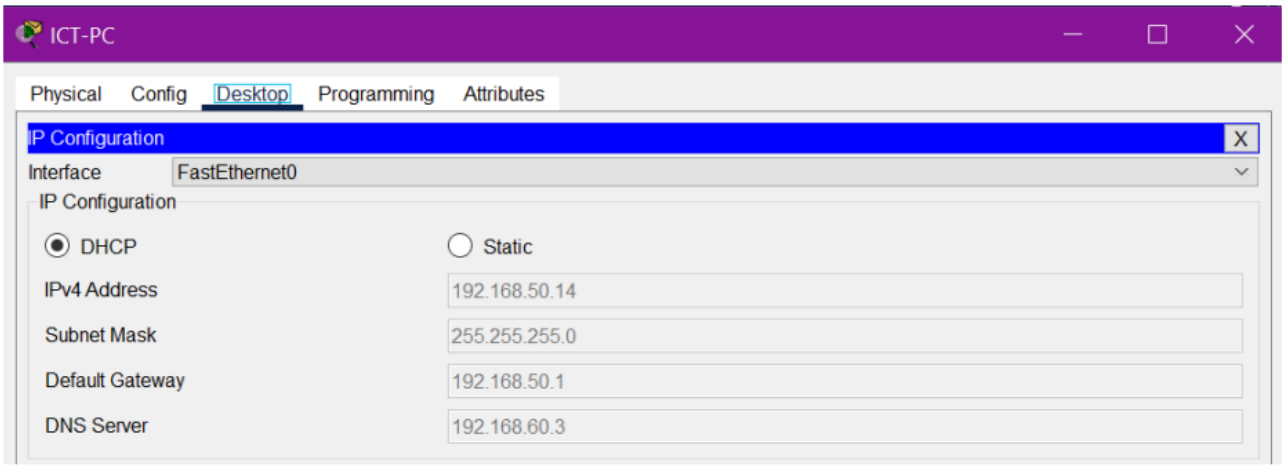
5.2. Traceroute Successful

The displayed packet routes help validate correct routing setup.

```
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.
```

5.3. DHCP IP Allocation

The devices correctly obtain dynamic Internet Protocol addresses from the Dynamic Host Configuration Protocol server.



5.4. Performance measure through ping time

```
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
```

6. Conclusion

The Company System Network Design project successfully delivered a robust, scalable, and secure network infrastructure tailored to support a modern trading floor support center. By implementing a hierarchical design with built-in redundancy, inter-VLAN routing, secure access control, and dynamic IP management, the system ensures both operational efficiency and future scalability.

Comprehensive testing using Cisco Packet Tracer validated all configurations, including routing protocols, DHCP functionality, NAT/PAT operations, and Quality of Service (QoS). The outcome is a resilient network that meets all project objectives—reliable communication, effective segmentation, strong security, and readiness for future technological integration.

This project not only demonstrates the practical application of network design principles but also emphasizes the importance of planning for growth, thorough testing, and security-first configurations in real-world networking scenarios.