A PROJECT REPORT

on

Company Network System Design

Submitted to

JK Cement Works

Submitted on

30/06/2025

Internship Domain: Networking and Security
Internship Duration : 1st May, 2025 - 30th June, 2025

BY

Pratistha Chakraborty

UNDER THE GUIDANCE OF

Mr. Mukesh Vasvani
(IT Head)

JK Cement Works

Nimbahera, Rajasthan - 312617
June 2025

Acknowledgements

I am profoundly grateful to **Mr. Mukesh Vaswani** of **JK Cement** for his expert guidance and continuous encouragement throughout to see that this project rights its target since its commencement to its completion.

Pratistha Chakraboty

JK CEMENT WORKS

One of India's top producers of grey cement and one of the world's top producers of white cement is JK Cement Ltd. Based on its superior products, customer focus, and technological leadership, the company has collaborated with India's multi-sectoral infrastructure demands for more than 50 years. In May 1975, JK Cement opened its flagship gray cement facility in Nimbahera, Rajasthan, marking the start of business operations. The firm is currently one of the leading cement producers in the nation, with an installed capacity of 24.34 million tons per annum (MnTPA) for grey cement. With a wall putty capacity of 1.33 MnTPA and a total white cement capacity of 1.12 MnTPA in India, JKCement is a top producer of white cement worldwide. JK White Cement products are sold in 36 countries worldwide, and the company has a robust international presence through its subsidiaries, JK Cement Works Fujairah FZC and JK White Cement (Africa) Ltd.

Vision: To be the preferred manufacturer of cement and cement-based products that partners in nation building, engages with its community and cares for all stakeholders.

Mission: JK Cement aims to deliver innovative products and solutions that meet the needs of its customers. Together with our exceptional people and strong stakeholder relationships, we commit to the highest standards of quality, productivity, sustainability and performance that drive shareholder value and long-term success.

JK Cement Works, Nimbahera

ABSTRACT

This report presents a comprehensive overview of the company's network system design, implemented using Cisco Packet Tracer. The primary objective of this project was to design a secure, scalable, and efficient network that interconnects multiple departments within the organization, including the IT Department, Security Department, Store Area, Dispatch Gate, Central Web Bridge, Kin Office, Truck Parking, Internal Shift Web Bridge, Packing Plant, Mines Office, and Crusher Office. The design ensures seamless communication and reliable data transfer across all sections while maintaining high standards of security and performance. Cisco Packet Tracer was used extensively to simulate, configure, and test the network setup before real-world deployment, enabling verification of routing, switching, and security configurations in a controlled environment.

Key configurations implemented in this network design include the use of Routing Information Protocol (RIP) for dynamic routing between departmental networks, facilitating efficient path selection and route updates. Dynamic Host Configuration Protocol (DHCP) was configured to automate IP address allocation, reducing administrative overhead and preventing IP conflicts. Secure Shell (SSH) was enabled on all major network devices to ensure encrypted remote access and management, enhancing overall network security. Port security features were configured on switches to prevent unauthorized devices from connecting to the network, mitigating risks of breaches and rogue devices. Additionally, multiple VLANs were created to logically segment the network, isolating traffic from different departments to improve security, manageability, and broadcast control. The design also includes the integration of three critical servers – an Active Directory (AD) server for centralized user authentication and management, a Darktrace server for real-time network monitoring and threat detection, and an RFID server for access control and attendance tracking – along with wireless access points in each department to provide seamless connectivity for laptops, IP phones, and mobile devices. This project demonstrates a holistic approach to enterprise network design, incorporating advanced routing, switching, server integration, and security configurations to meet the operational needs of the organization effectively.

Keywords: Cisco Packet Tracer, Dynamic Routing (RIP), VLANs, Port Security, Server

Content

List 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 secure, scalable, and efficient network infrastructure to support the operational requirements of a growing industrial environment. With the organization expanding its departments and integrating multiple operational units within a single interconnected system, the strategic significance of routing, switching, and security configurations takes center stage, playing a crucial role in ensuring seamless communication, reliable data transfer, and controlled access to resources. This project focuses on designing and implementing a robust network that connects various departments such as IT, Security, Dispatch, Store, Packing Plant, Mines Office, and Crusher Office, while integrating servers and wireless access points to enhance operational efficiency. The entire design and implementation process has been carried out using Cisco Packet Tracer to simulate, test, and validate network configurations before deployment.

1.2 Objectives

The primary objectives of the "Company System Network Design" initiative are clearly outlined to cater to the unique demands of the organization’s network infrastructure. The project aims to implement dynamic routing using Routing Information Protocol (RIP) for efficient inter-network communication, configure Dynamic Host Configuration Protocol (DHCP) for automated IP address allocation, and deploy Secure Shell (SSH) for secure remote device management. It seeks to implement port security to restrict unauthorized access, create multiple Virtual Local Area Networks (VLANs) to logically segment departmental traffic for improved security and performance, and integrate wireless access points to provide mobility across departments. Additionally, the project includes the deployment of three dedicated servers: an Active Directory server for centralized authentication, a Darktrace server for network monitoring and threat detection, and an RFID server for access control and attendance tracking. By achieving these objectives, the project establishes a secure, reliable, and future-ready network infrastructure that not only meets current operational requirements but also anticipates and accommodates the organization’s growth and technological advancements.

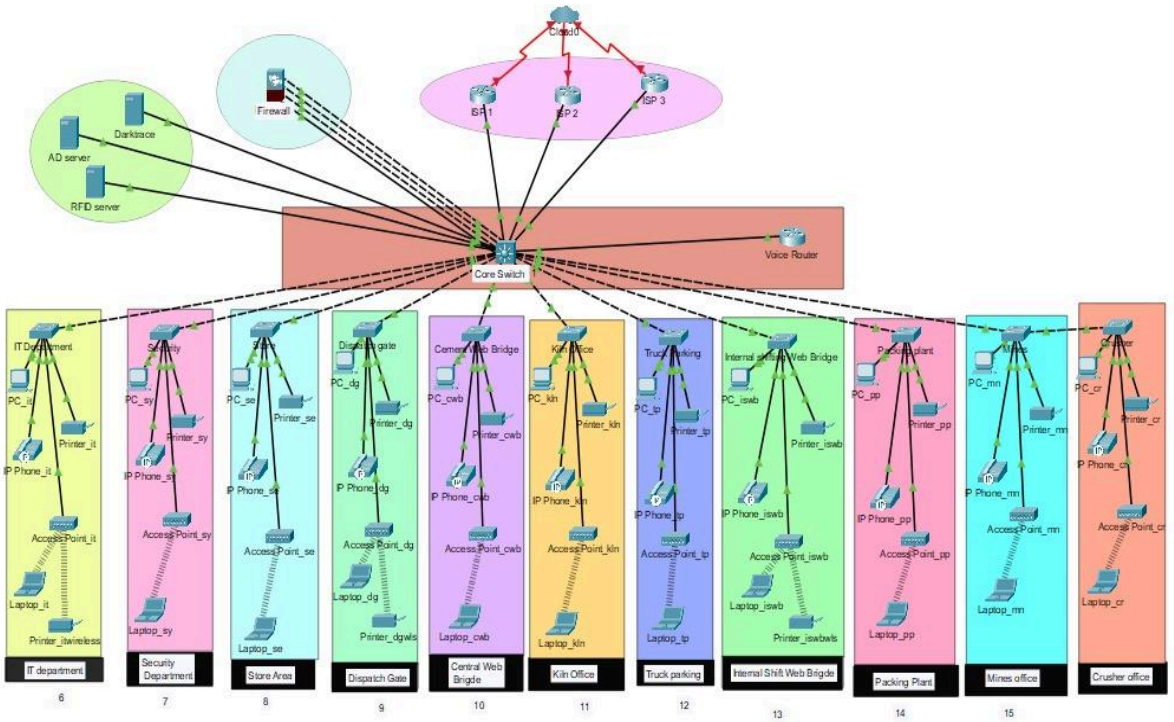
.

2. **Network Design**

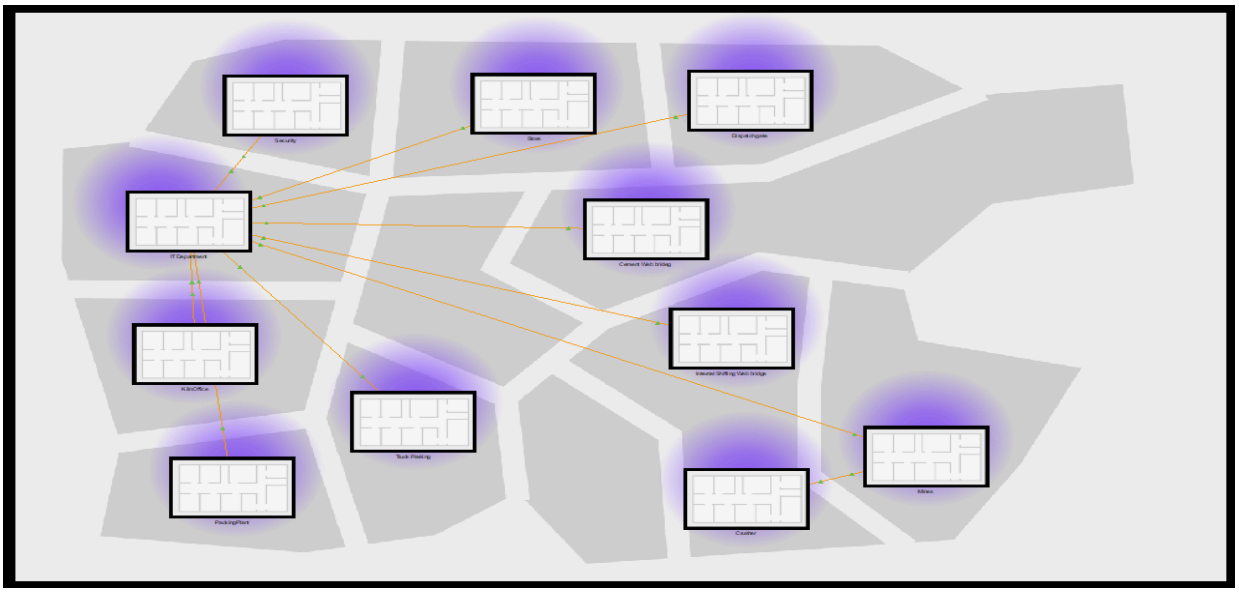
2.1 Topology

The network configuration simulated in Cisco Packet Tracer for the "Company System Network Design" project adheres to a hierarchical model, prioritizing security, scalability, and operational efficiency. The design consists of three logical layers: the core layer, distribution layer, and access layer. At the core layer, a central core switch is deployed to interconnect all departmental networks, servers, voice routers, firewall, and the internet via multiple ISPs, ensuring high-speed data routing and centralized management. The distribution layer comprises departmental switches that aggregate and manage network traffic from various departments such as IT, Security, Store, Dispatch Gate, Central Web Bridge, Kin Office, Truck Parking, Internal Shift Web Bridge, Packing Plant, Mines Office, and Crusher Office. Finally, the access layer includes end-user devices such as PCs, laptops, IP phones, printers, and wireless access points connected to departmental switches, enabling seamless connectivity and mobility across the organization. This topology ensures an organized, secure, and future-ready network layout, facilitating effective management, scalability, and simplified troubleshooting.

Logical Topology

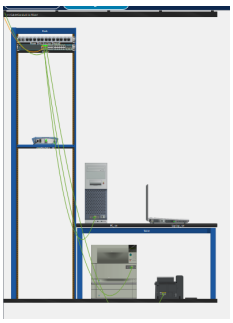


Physical Topology



JK Cement Plant Departments

IT Department - Server room



Other departments

2.2 Components

The network design for this project incorporates the following major devices and components:

1. **Core Switch (1):**
    - Positioned at the core layer.
    - Interconnects all departmental switches, servers, voice router, and firewall.
    - Provides centralized switching for efficient data transfer and management.
2. **Routers (4):**
    - Includes 3 ISP routers connecting the organization to the internet via multiple ISPs to ensure internet redundancy and reliability.
    - A voice router is also deployed for VoIP services and integration with IP phones across departments.
3. **Departmental Switches (Multiple):**
    - Act as distribution layer switches connecting specific departments to the core switch.
    - Facilitate intra-departmental and inter-departmental communication via VLAN configurations.
4. **Servers (3):**
    - **Active Directory (AD) Server**: Provides centralized authentication and user management.
    - **Darktrace Server**: Monitors network traffic and detects threats to enhance security.
    - **RFID Server**: Manages RFID-based access control and attendance tracking for operational areas.
5. **End-User Devices (PCs, Laptops, IP Phones, Printers):**
    - Deployed at the access layer within each department.
    - Connected to departmental switches for seamless access to network resources.
6. **Cisco Wireless Access Points (Multiple):**
    - Installed in each department to provide wireless connectivity for laptops and mobile devices.
    - Enhance user mobility and operational flexibility.

7. **Firewall (1):**
    - Positioned between the core switch and external ISPs.
    - Secures the network by monitoring and controlling incoming and outgoing traffic based on security policies.
8. **Voice Router (1):**
    - Integrated with the network to manage VoIP services.
    - Connects IP phones from various departments to external voice networks.

These components collectively establish a structured, secure, and highly functional network infrastructure tailored to the operational needs of the organization. The design ensures robust security using port security and SSH, efficient routing through RIP, automated IP allocation with DHCP, and logical segmentation using VLANs, aligning with the organization's current requirements while accommodating future growth and technological advancements.

3. IP Addressing Scheme

Base Network : 10.4.0.0/24

Department / Function	Network Address	Subnet Mask	Host Address Range	Broadcast Address
IT Department	10.4.11.0	255.255.255.0 (/24)	10.4.11.1 – 10.4.11.254	10.4.11.255
Security Department	10.4.12.0	255.255.255.0 (/24)	10.4.12.1 – 10.4.12.254	10.4.12.255
Store Department	10.4.13.0	255.255.255.0 (/24)	10.4.13.1 – 10.4.13.254	10.4.13.255
Dispatch Gate	10.4.14.0	255.255.255.0 (/24)	10.4.14.1 – 10.4.14.254	10.4.14.255
Cement Web Bridge	10.4.15.0	255.255.255.0 (/24)	10.4.15.1 – 10.4.15.254	10.4.15.255
Kiln Office	10.4.16.0	255.255.255.0 (/24)	10.4.16.1 – 10.4.16.254	10.4.16.255
Truck Parking	10.4.17.0	255.255.255.0 (/24)	10.4.17.1 – 10.4.17.254	10.4.17.255
Internal Shifting Web Bridg	10.4.18.0	255.255.255.0 (/24)	10.4.18.1 – 10.4.18.254	10.4.18.255
Packing Plant	10.4.19.0	255.255.255.0 (/24)	10.4.19.1 – 10.4.19.254	10.4.19.255
Mines Office	10.4.20.0	255.255.255.0 (/24)	10.4.20.1 – 10.4.20.254	10.4.20.255
Voice VLAN	10.4.22.0	255.255.255.0 (/24)	10.4.22.1 – 10.4.22.254	10.4.22.255
Wireless LAN Controller	10.4.23.0	255.255.255.0 (/24)	10.4.23.1 – 10.4.23.254	10.4.23.255
Management VLAN 201	10.4.201.0	255.255.255.0 (/24)	10.4.201.1 – 10.4.201.254	10.4.201.255
Management VLAN 202	10.4.202.0	255.255.255.0 (/24)	10.4.202.1 – 10.4.202.254	10.4.202.255
Inside VLAN to Firewall (20	10.4.204.0	255.255.255.0 (/24)	10.4.204.1 – 10.4.204.254	10.4.204.255

DHCP Scheme

VLAN ID	Department	DHCP Pool Name	Network Address	Subnet Mask	Excluded Address Range	DHCP Allocated Range	Default Gateway
11	IT Department	v11	10.4.11.0	255.255.255.0 (/24)	10.4.11.1 – 10.4.11.20	10.4.11.21 – 10.4.11.254	10.4.11.1
12	Security Department	v12	10.4.12.0	255.255.255.0 (/24)	10.4.12.1 – 10.4.12.20	10.4.12.21 – 10.4.12.254	10.4.12.1
13	Store	v13	10.4.13.0	255.255.255.0 (/24)	10.4.13.1 – 10.4.13.20	10.4.13.21 – 10.4.13.254	10.4.13.1
14	Dispatch Gate	v14	10.4.14.0	255.255.255.0 (/24)	10.4.14.1 – 10.4.14.20	10.4.14.21 – 10.4.14.254	10.4.14.1
15	Cement Web Bridge	v15	10.4.15.0	255.255.255.0 (/24)	10.4.15.1 – 10.4.15.20	10.4.15.21 – 10.4.15.254	10.4.15.1
16	Kiln Office	v16	10.4.16.0	255.255.255.0 (/24)	10.4.16.1 – 10.4.16.20	10.4.16.21 – 10.4.16.254	10.4.16.1
17	Truck Parking	v17	10.4.17.0	255.255.255.0 (/24)	10.4.17.1 – 10.4.17.20	10.4.17.21 – 10.4.17.254	10.4.17.1
18	Internal Shifting Web Bridge	v18	10.4.18.0	255.255.255.0 (/24)	10.4.18.1 – 10.4.18.20	10.4.18.21 – 10.4.18.254	10.4.18.1
19	Packing Plant	v19	10.4.19.0	255.255.255.0 (/24)	10.4.19.1 – 10.4.19.20	10.4.19.21 – 10.4.19.254	10.4.19.1
20	Mines	v20	10.4.20.0	255.255.255.0 (/24)	10.4.20.1 – 10.4.20.20	10.4.20.21 – 10.4.20.254	10.4.20.1
22	Voice VLAN	v22	10.4.22.0	255.255.255.0 (/24)	N/A	Full range available	10.4.22.1
23	Wireless LAN Controller	v23	10.4.23.0	255.255.255.0 (/24)	N/A	Full range available	10.4.23.1

4. VLAN Configuration

In the **Core_Switch**, multiple VLANs are configured to segment the network into logical broadcast domains based on departments and functions. Each VLAN interface (SVI) is assigned a unique IP address to enable inter-VLAN routing. VLANs such as **IT_department (VLAN11)**, **Security (VLAN12)**, **Store (VLAN13)**, and others are created to ensure efficient traffic management, enhanced security, and organized addressing. This approach facilitates network scalability and simplifies administration by isolating departmental traffic within their respective VLANs.

```
! Create VLAN in database (if needed)
vlan <VLAN_ID>
 name <VLAN_NAME>
exit

! Create SVI (Switched Virtual Interface) for routing
interface vlan <VLAN_ID>
 description <Department_or_Use_Case>
 ip address <IP_ADDRESS> <SUBNET_MASK>
 no shutdown
exit
```

Example:

```
interface Vlan11
 description IT_department
 mac-address 00e0.8fb0.6402
 ip address 10.4.11.1 255.255.255.0
```

5. Port Security:

In this network configuration, **port security is implemented on switch ports where printers are connected** within each department. This enhances security by **restricting access to a single device per port**, preventing unauthorized devices from connecting and misusing network resources. The configuration uses **sticky MAC address learning**, ensuring that the printer's MAC address is dynamically learned and secured on the port. The **violation mode is set to restrict**, which drops unauthorized frames and generates security notifications without shutting down the port entirely.

```
IT_department_sw1(config)#int fa0/4
IT_department_sw1(config-if)#switchport port-security
IT_department_sw1(config-if)#switchport port-security maximum 1
IT_department_sw1(config-if)#switchport port-security violation restrict
IT_department_sw1(config-if)#switchport port-security mac-address sticky
IT_department_sw1(config-if)#
```

6. Connectivity Test Analysis

>This connectivity test shows that **ISP-1 is able to reach the core switch interfaces (10.4.201.2 and .3)**, the **department switch can reach the firewall inside interface (10.4.204.2) and its gateway (10.4.204.1)**, the **core switch is able to reach the firewall inside interface**, and **Firewall-1 has successful connectivity with an internal device (10.4.11.11)**. Overall, it confirms proper routing and switching configuration across ISP, firewall, core switch, and department switches in the network.

```
ISP-1#ping 10.4.201.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.4.201.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/1/7 ms
ISP-1#ping 10.4.201.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.4.201.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/2/14 ms
ISP-1#ping 10.4.201.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.4.201.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
IT_department_sw1#ping 10.4.204.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.4.204.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
IT_department_sw1#ping 10.4.204.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.4.204.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
Core_Switch_1#ping 10.4.204.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.4.204.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
Firewall-1#ping 10.4.11.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.4.11.11, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

This connectivity test confirms that routing is working end-to-end, which in your configuration is achieved using RIP.

>This connectivity test shows that the **PC successfully pinged the IP address 10.4.12.21**, which indicates **proper network connectivity** between the source device and the destination device in the **10.4.12.0/24 network (Security VLAN)**. Although the **first ping request timed out**, the subsequent three replies were successful with low latency (1ms–10ms). The initial timeout could be due to **ARP resolution delay**, where the PC needed to resolve the MAC address of the destination before sending ICMP packets. Overall, this confirms that **routing, VLAN configuration, and interface status are functioning correctly** for this device.

Connectivity between IT department and Security department:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.4.12.21

Pinging 10.4.12.21 with 32 bytes of data:

Request timed out.
Reply from 10.4.12.21: bytes=32 time=10ms TTL=127
Reply from 10.4.12.21: bytes=32 time=1ms TTL=127
Reply from 10.4.12.21: bytes=32 time<1ms TTL=127

Ping statistics for 10.4.12.21:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 3ms
```

Similarly connectivity between IT department and Packing plant

```
C:\>ping 10.4.19.21

Pinging 10.4.19.21 with 32 bytes of data:

Request timed out.
Reply from 10.4.19.21: bytes=32 time<1ms TTL=127
Reply from 10.4.19.21: bytes=32 time<1ms TTL=127
Reply from 10.4.19.21: bytes=32 time<1ms TTL=127

Ping statistics for 10.4.19.21:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

7. Access Points:

In this network setup, each department is provided with its own dedicated access point to enable wireless connectivity for their devices, such as laptops and wireless printers. For example, in the IT department, the access point named “Access_Point_it” connects devices like Laptop_it and Printer_itwireless.

Each department’s access point is configured with a unique SSID (Service Set Identifier) to distinguish its wireless network, along with a WPA-PSK (Wi-Fi Protected Access Pre-Shared Key) password to ensure security. This configuration allows only authorized users of that specific department to connect to their designated wireless network, ensuring secure and organized wireless access across the entire organization.

8. Quality of Service (QoS):

On the ISP-1 router, QoS is implemented to prioritize critical traffic types. Two class maps, VOICE and VIDEO, are created to match RTP traffic commonly used for voice and video streams. A policy map named QOS-POLICY allocates 30% guaranteed bandwidth for voice and 20% for video, while all remaining traffic is handled using fair queuing under the default class. This policy is then applied to the FastEthernet0/0 interface, ensuring efficient bandwidth utilization and service quality for latency-sensitive applications such as VoIP and video conferencing.

```
enable
configure terminal

! Step 1: Create class maps for VOICE and VIDEO traffic
class-map VOICE
 match protocol rtp

class-map VIDEO
 match protocol rtp

! Step 2: Define the policy map and assign bandwidth priorities
policy-map QOS-POLICY
 class VOICE
  priority percent 30
 class VIDEO
  bandwidth percent 20
 class class-default
  fair-queue

! Step 3: Apply the policy to the desired interface
interface fa0/0
 bandwidth 10000
 service-policy output QOS-POLICY

end
write memory
```

8. Conclusion:

The successful pings between **ISP-1, Core Switch, Firewall, and department switches** indicate that **RIP version 2**, configured on the core switch, is correctly advertising and learning routes for all **10.x.x.x subnets**. This ensures that devices in different VLANs and networks can communicate with each other seamlessly, with proper routing updates exchanged between routers and switches to maintain end-to-end connectivity.

This project **successfully demonstrates the design, configuration, and implementation of a secure, scalable, and efficient enterprise network** for multiple departments. Core networking concepts were integrated, including **VLAN segmentation, inter-VLAN routing, DHCP configuration, RIP routing, port security, and Quality of Service (QoS) policies** to prioritize critical traffic.

Wireless connectivity was established for each department with dedicated **access points configured with unique SSIDs and WPA-PSK passwords**, ensuring secure, department-specific wireless access. Comprehensive connectivity tests validated robust communication between the ISP, firewall, core switches, and departmental switches.

Additionally, **port security** was implemented on switch interfaces to enhance network security by restricting unauthorized device access, while **DHCP ensured efficient IP address allocation** across VLANs.

Overall, this project provides a **strong foundation for enterprise network deployment**, emphasizing structured planning, secure configuration, and practical troubleshooting skills essential for **real-world networking environments**.