**Retail Chain Network Infrastructure**

**Name:** Huzaifa Nasir

**Roll No:** 22i-1053

**Section:** CS-A

Table of Contents

[Introduction 3](#_Toc183876317)

[Network Topology Overview 3](#_Toc183876318)

[Technologies Used 4](#_Toc183876319)

[Routing Protocols and Configuration 4](#_Toc183876320)

[RIP – Store 1 4](#_Toc183876321)

[Store 1 Configuration: 5](#_Toc183876322)

[Routing at Store 1: 5](#_Toc183876323)

[EIGRP– Store 2 and Store 4 7](#_Toc183876324)

[Store 2 and Store 4 Configuration: 7](#_Toc183876325)

[Routing at Store 2: 7](#_Toc183876326)

[Routing at Store 4: 9](#_Toc183876327)

[OSPF – Store 3 11](#_Toc183876328)

[Store 3 Configuration: 11](#_Toc183876329)

[Routing at Store 3: 11](#_Toc183876330)

[Redistribution at Headquarters Router 13](#_Toc183876331)

[DHCP Configuration for Stores and HQ 14](#_Toc183876332)

[Store and HQ Configuration: 14](#_Toc183876333)

[DHCP Configuration: 15](#_Toc183876334)

[Network Address Translation (NAT) at Store 1 16](#_Toc183876335)

[Store 1 Configuration: 17](#_Toc183876336)

[Firewall Configuration and Security 17](#_Toc183876337)

[Firewall Configuration: 18](#_Toc183876338)

[Challenges Faced 20](#_Toc183876339)

[Routing Protocol Compatibility and Redistribution: 20](#_Toc183876340)

[NAT Configuration: 21](#_Toc183876341)

[Firewall Configuration: 21](#_Toc183876342)

[Network Topology Diagram 21](#_Toc183876343)

[Network Components: 21](#_Toc183876344)

[Conclusion 22](#_Toc183876345)

# Introduction

The Retail Chain Network Design project involves creating a detailed network topology for a retail chain consisting of four stores and a headquarters (HQ). This network was designed and simulated using Cisco Packet Tracer. The design includes a variety of networking components such as routers, switches, servers, firewalls, and end devices, ensuring secure, reliable, and scalable connectivity between stores and HQ. The project focuses on the implementation of routing protocols, NAT (Network Address Translation), DHCP (Dynamic Host Configuration Protocol), and firewall rules for securing sensitive devices like POS terminals and CCTV cameras.

The network design has been structured to meet the following objectives:

* Efficient communication between the stores and HQ.
* Implementation of routing protocols to manage traffic between stores.
* Ensuring security for sensitive devices within the stores.
* DHCP services dynamically assign IP addresses.
* Use of NAT at specific points to hide internal IP addresses.
* Implementing firewalls to restrict unauthorized access.

This report details the network topology, the use of routing protocols at each store, the implementation of NAT and DHCP, and the configuration of firewalls to protect the network.

# Network Topology Overview

The network consists of the following components:

* **Four Stores**: Each store has two routers for redundancy, switches, access points, end devices (laptops, printers, POS terminals, CCTV cameras), and a DHCP server.
* **Headquarters (HQ)**: The central hub connects all stores and is responsible for routing traffic between the stores.
* **Routing Protocols**: Different routing protocols are used at each store:
  + Store 1 uses **RIP** (Routing Information Protocol).
  + Store 2 uses **EIGRP** (Enhanced Interior Gateway Routing Protocol).
  + Store 3 uses **OSPF** (Open Shortest Path First).
  + Store 4 uses **EIGRP** (Enhanced Interior Gateway Routing Protocol).
* **DHCP Servers**: Each store and the HQ have a DHCP server configured to dynamically assign IP addresses within their respective network.
* **Security and Connectivity**: The network uses firewalls to secure sensitive devices such as POS terminals and CCTV cameras. NAT is also implemented at Store 1 to protect the internal IP addresses.

# Technologies Used

* Cisco Packet Tracer: Used for network simulation, configuration, and testing.
* Routing Protocols:
  + RIP (Routing Information Protocol) for Store 1.
  + EIGRP (Enhanced Interior Gateway Routing Protocol) for Store 2 and Store 4.
  + OSPF (Open Shortest Path First) for Store 3.
* DHCP (Dynamic Host Configuration Protocol): Configured for dynamic IP assignment to end devices at stores and HQ.
* NAT (Network Address Translation): Applied at Store 1 to allow multiple internal devices to share a set of public IP addresses.
* Firewall Configuration: To secure sensitive devices like POS terminals and CCTV cameras within the network.
* IP Helper Address: Configured on routers to forward DHCP Discover packets across subnets.

# Routing Protocols and Configuration

Routing is the backbone of communication between the stores and HQ. Each store has two routers to ensure fault tolerance and redundancy. The routers at each store use different routing protocols to exchange routing information and ensure optimal traffic flow.

## RIP – Store 1

**RIP** is used in Store 1 as the routing protocol. It is a distance-vector protocol that updates the routing table by broadcasting the entire table to neighboring routers. RIP is simple to configure and works well in smaller networks.

### Store 1 Configuration:

* + **Routing Protocol**: RIP
  + **Routers**: Two routers at Store 1 exchange RIP updates to ensure communication between devices at Store 1 and the HQ.

Routing at Store 1:

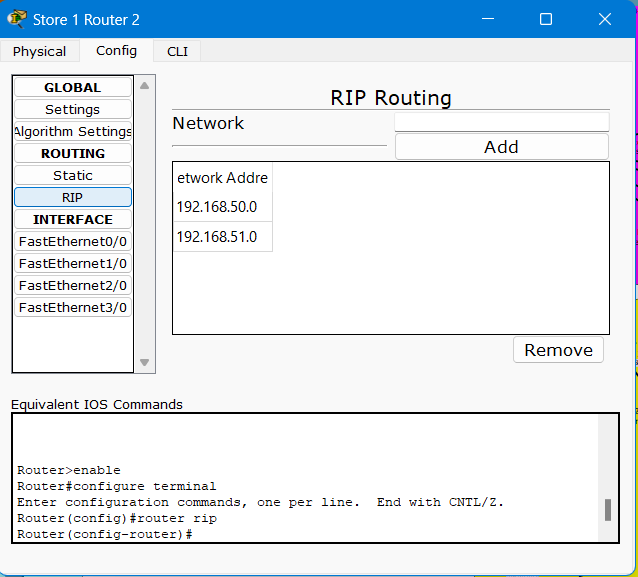
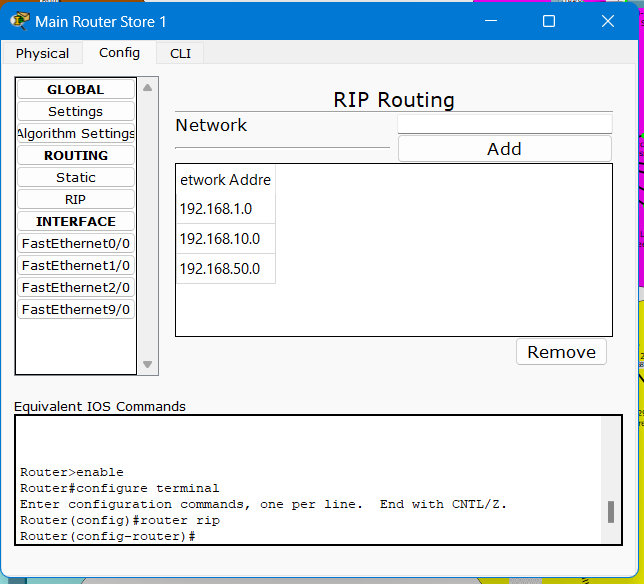
The routers at Store 1 are configured with RIP to exchange routing information and facilitate communication. The following images show the routing tables and configurations of the routers in Store 1, demonstrating the successful implementation of RIP.

Router(config)# router rip

Router(config-router)# network 192.168.1.0

Router(config-router)# network 192.168.10.0

Router(config-router)# network 192.168.50.0



## EIGRP– Store 2 and Store 4

**EIGRP** is used in Store 2 and Store 4. It is a hybrid routing protocol that combines the benefits of distance-vector and link-state protocols. EIGRP is highly efficient and scales well in larger networks, using a composite metric based on bandwidth, delay, reliability, and load.

### Store 2 and Store 4 Configuration:

* + **Routing Protocol**: EIGRP
  + **Routers**: Each store uses two routers configured with EIGRP to exchange routing information and ensure reliable communication between stores and HQ.

Routing at Store 2:

The routers in Store 2 use EIGRP to exchange routing information with the routers in Store 1 and the HQ. The following images demonstrate the EIGRP routing table and configurations.

Router(config)# router eigrp 1

Router(config-router)# network 192.168.20.0 0.0.0.255

Router(config-router)# network 192.168.11.0 0.0.0.255

Router(config-router)# network 192.168.2.0 0.0.0.255

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Routing at Store 4: Similarly, the routers in Store 4 use EIGRP to maintain communication with Store 3 and the HQ. The images below show the EIGRP routing table on both routers in Store 4, confirming that routing is configured correctly.

Router(config)# router eigrp 1

Router(config-router)# network 192.168.5.0 0.0.0.255

Router(config-router)# network 192.168.13.0 0.0.0.255

Router(config-router)# network 192.168.61.0 0.0.0.255

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

## OSPF – Store 3

**OSPF** is used in Store 3. It is a link-state routing protocol that uses cost as its metric, based on bandwidth. OSPF provides faster convergence and scalability compared to RIP, making it ideal for medium-to-large networks.

### Store 3 Configuration:

* + **Routing Protocol**: OSPF (Area 0, Area 3)
  + **Routers**: Two routers at Store 3 exchange OSPF link-state advertisements to maintain an updated view of the network topology.

Routing at Store 3:

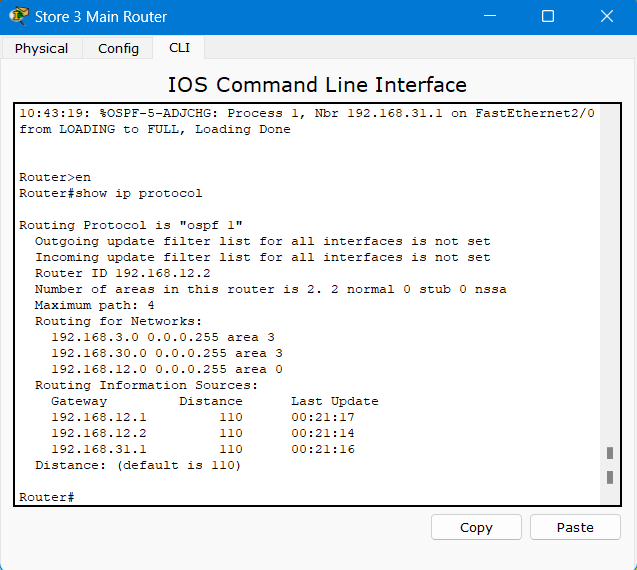
The routers in Store 3 are configured with OSPF to ensure seamless routing between the stores and the HQ. Below are images of the OSPF routing tables on both routers, confirming the successful implementation of OSPF.

Router(config)# router ospf 1

Router(config-router)# network 192.168.3.0 0.0.0.255 area 3

Router(config-router)# network 192.168.30.0 0.0.0.255 area 3

Router(config-router)# network 192.168.12.0 0.0.0.255 area 0



A screenshot of a computer

Description automatically generated

# Redistribution at Headquarters Router

Redistribution allows the headquarters router to share routing information between different routing protocols, enabling communication between stores using RIP, OSPF, and EIGRP.

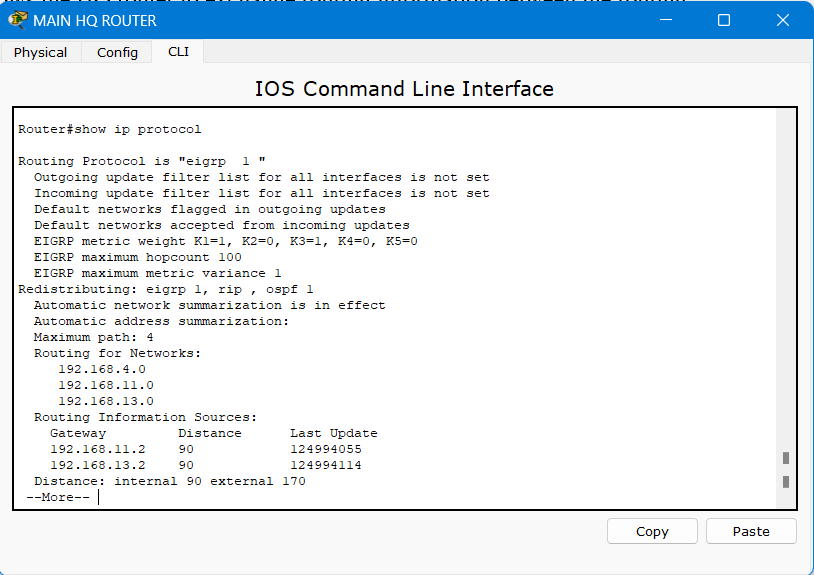
In this network design, redistribution was implemented at the headquarters (HQ) router to ensure seamless communication between stores using different routing protocols (RIP, OSPF, EIGRP). Redistribution allows the HQ router to exchange routing information between the routing protocols used in different stores, enabling devices in Store 1 (using RIP), Store 3 (using OSPF), and Stores 2 and 4 (using EIGRP) to communicate with one another through the HQ router.

To configure redistribution on the HQ router, the following commands were used:

HeadquartersRouter(config)# router ospf 1

HeadquartersRouter(config-router)# redistribute rip metric 10

HeadquartersRouter(config-router)# redistribute eigrp 100 metric 10



# DHCP Configuration for Stores and HQ

Each store and the HQ have their own DHCP servers configured to automatically assign IP addresses to devices within their respective networks. This ensures that devices can easily connect to the network without requiring manual IP address assignment.

## Store and HQ Configuration:

* + **DHCP Servers**: Each store has a DHCP server that provides IP addresses to devices within the store. The HQ also has a DHCP server that assigns IP addresses within the HQ network.
  + **IP Address Pools**: The IP address ranges for each store and the HQ are set according to their respective network addresses.

## DHCP Configuration:

The following images show the DHCP pool configuration for each store and the HQ, as well as successful IP address lease assignments to end devices.

A screenshot of a computer

Description automatically generated

A computer screen shot of a computer

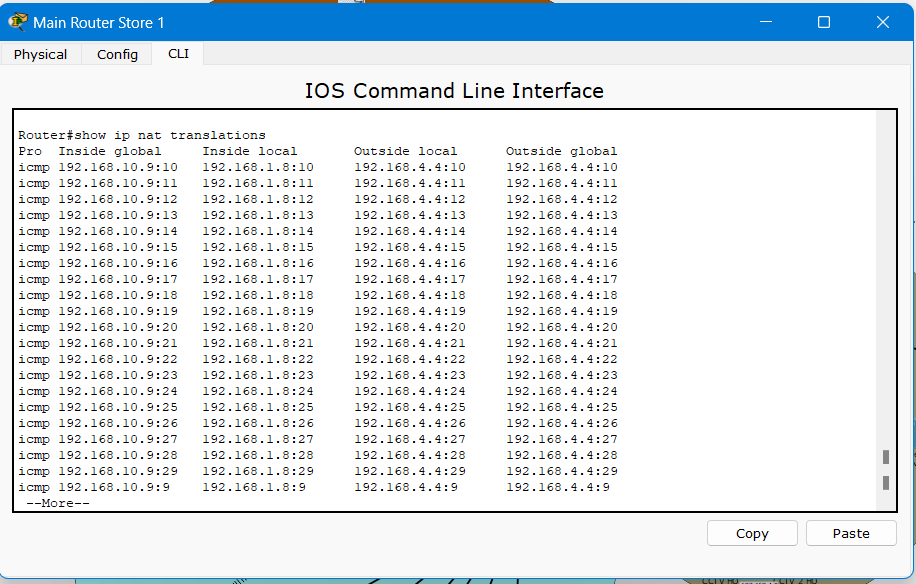
Description automatically generated

# Network Address Translation (NAT) at Store 1

NAT (Network Address Translation) is implemented at Store 1 to allow multiple internal devices to share a set of public IP addresses for communication with external networks. This provides an added layer of security by masking the internal IP addresses and making it difficult for external entities to directly target specific devices within the store network.

## Store 1 Configuration:

* + **NAT Type**: Dynamic NAT (using an IP address pool)
  + **Router Configuration**: the routers in Store 1 are configured to use Dynamic NAT, which translates internal private IP addresses to public IP addresses from a pre-configured pool. The pool of public IP addresses is used dynamically to map the internal devices as they need to access external resources.
  + **NAT Configuration at Store 1**: Dynamic NAT is set up on the router at Store 1 so that devices within the store can access external resources while maintaining the privacy of their internal IP addresses. Here are the general steps and configuration involved:



# Firewall Configuration and Security

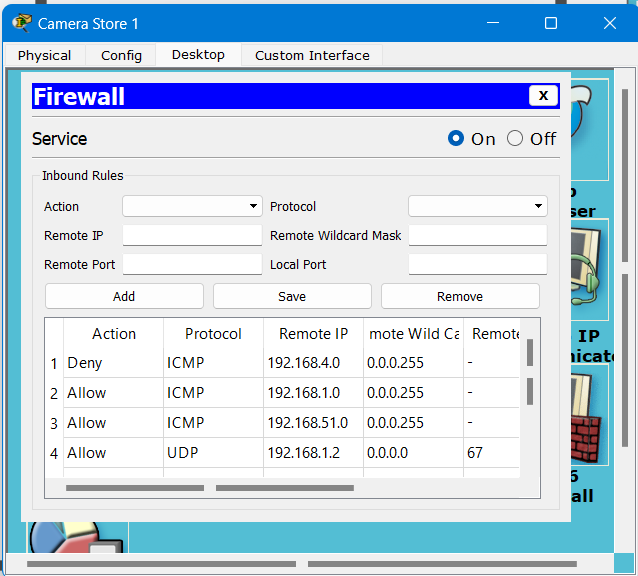
In this network, firewalls are implemented directly on the end devices such as the POS terminals and CCTV cameras. This ensures that these sensitive devices are protected from unauthorized access by blocking unwanted communication from devices outside of the store network.

## Firewall Configuration:

* **End Device Firewalls:** Each POS terminal and CCTV camera has a built-in firewall that restricts access to these devices. Only authorized devices within the same store network are allowed to communicate with these critical devices.
* **POS Terminal & CCTV Security**: The firewalls on these devices are configured to ensure that communication is only allowed between the authorized devices (e.g., employee laptops, manager laptops) within the store. Devices from other stores or unauthorized devices from the headquarters cannot access the POS terminals or CCTV cameras.

This approach enhances the security of sensitive devices without relying on router-based ACLs. It ensures that even if a device from outside the store network tries to access the POS terminal or CCTV camera, the firewall on the end device will block the attempt, thereby securing the store’s critical devices.

The following images demonstrate how firewalls have been implemented on the POS terminals and CCTV cameras to restrict access from unauthorized devices.



A screenshot of a computer

Description automatically generated

# Challenges Faced

## Routing Protocol Compatibility and Redistribution:

One of the biggest challenges faced during this project was ensuring proper communication between the different routing protocols used in the network—RIP, EIGRP, and OSPF. While each store used a different protocol, redistribution had to be configured at the headquarters router to ensure seamless communication between stores using different routing protocols. Implementing redistribution for each protocol (RIP, EIGRP, and OSPF) required careful attention to routing metrics and administrative distances to prevent routing loops or suboptimal paths. There were instances where incorrect redistribution caused routing inconsistencies, but after adjusting the redistribution metrics, I was able to resolve the issue and achieve optimal routing.

## NAT Configuration:

Configuring Network Address Translation (NAT) at Store 1 proved to be particularly challenging. Initially, I encountered issues with translating internal private IP addresses to the public IP pool. The key difficulty was in setting up the DynamicNAT configuration correctly, ensuring that devices behind the NAT (i.e., internal devices) were able to access external resources while maintaining privacy for their internal IP addresses.

## Firewall Configuration:

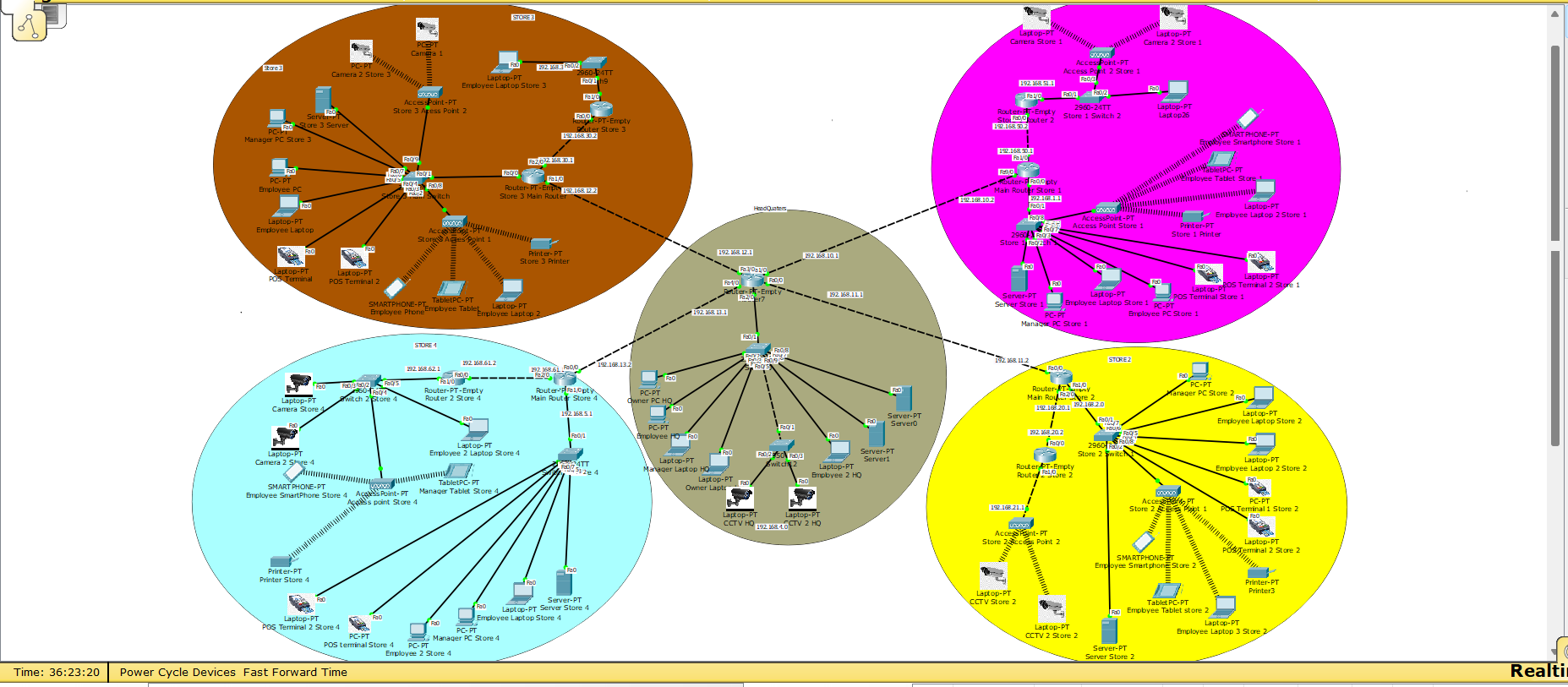
Implementing firewalls on sensitive devices like **POS terminals** and **CCTV cameras** posed another challenge, primarily because these devices are integral to the network's security. These devices needed to be isolated from external devices and unauthorized users, while allowing communication between authorized devices. The challenge arose due to the combination of **DHCP** and **UDP traffic**—firewalls on these devices had to allow DHCP requests, which are transmitted via **UDP**, and simultaneously block unwanted external connections. This complexity was exacerbated by the need for stateful packet inspection to ensure that return traffic was correctly allowed for UDP-based connections, especially for DHCP lease renewals. Configuring these firewalls required a deep understanding of both networking protocols and security principles to ensure that the POS and CCTV devices could function securely, without being compromised.

# Network Topology Diagram

The network topology diagram below provides a visual representation of the overall network design. It includes routers, DHCP servers, firewalls, access points, end devices, and the interconnections between stores and the HQ.

## Network Components:

* + **HQ** with routers and DHCP server.
  + **Store 1** with RIP routing, routers, access points, and servers.
  + **Store 2** with EIGRP routing, routers, access points, and servers.
  + **Store 3** with OSPF routing, routers, access points, and servers.
  + **Store 4** with EIGRP routing, routers, access points, and servers.



# Conclusion

The Retail Chain Network Design project successfully demonstrates the creation and configuration of a functional and secure network using Cisco Packet Tracer. By implementing different routing protocols (RIP, EIGRP, OSPF), configuring NAT for secure IP address translation, setting up DHCPservers for dynamic IP assignment, and using firewalls to protect sensitive devices, the network meets the requirements of a retail chain with multiple stores and a central HQ.

**Key aspects of the network include**:

* Routing using RIP, OSPF, and EIGRP at each store.
* DHCP servers in each store and HQ for automatic IP address assignment.
* NAT implementation at Store 1 to secure internal IP addresses.
* Firewall configurations to restrict access to sensitive devices.

This network is both secure and scalable, ensuring optimal performance for the retail chain.