# Centralized Railway Ticketing System Network

**A CASE STUDY REPORT**

***Submitted by***

**Abishek S R (RA2211003011292)**

**Mallela Gnanamrutha (RA2211003011294)**

**Mageshwar C S (RA2211003011297)**

**Deekshith P (RA2211003011309)**

***for the course***

**21CSC302J – COMPUTER NETWORKS**

***in partial fulfillment of the requirements for the degree of***

**BACHELOR OF TECHNOLOGY**


**DEPARTMENT OF COMPUTING TECHNOLOGIES**

**SCHOOL OF COMPUTING**

**FACULTY OF ENGINEERING AND TECHNOLOGY**

**SRM INSTITUTE OF SCIENCE AND TECHNOLOGY**

**KATTANKULATHUR - 603 203.**

# SRM INSTITUTE OF SCIENCE AND TECHNOLOGY
# KATTANKULATHUR – 603 203

## BONAFIDE CERTIFICATE

Certified that Computer Network A Case Study Report titled "**Centralized Railway Ticketing System**" is the bonafide work of "**Deekshith P" [RA2211003011309],** "**Abishek S R" [RA2211003011292],** "**Mageshwar C S" [RA2211003011297], Mallela Gnanamrutha (RA2211003011294)** who carried out the case study under my supervision. Certified further, that to the best of my knowledge the work reported herein does not form any other work

**SIGNATURE OF FACULTY NAME**

Dr. JEYASEKAR A.
Assistant Professor
Department of Computing Technologies

**Date : 12-11-2024**

# ABSTRACT

In today's interconnected world, robust and efficient network systems are the backbone of any large-scale operation. The railway industry, with its vast network of stations and ticketing counters, demands a highly reliable, secure, and scalable network to handle its centralized ticketing system. This project aims to design and simulate a comprehensive network for a "Centralized Railway Ticketing System" using Cisco Packet Tracer. The primary goal is to establish seamless communication between various nodes, ensuring real-time data exchange and high availability for uninterrupted ticketing services.

The proposed network architecture incorporates hierarchical design principles, including Core, Distribution, and Access layers. Each layer is equipped with redundancy mechanisms to minimize downtime and ensure failover in case of hardware or network failures. VLANs (Virtual Local Area Networks) are deployed to segment the network based on functional areas, such as ticketing counters, administrative offices, and server rooms, improving both performance and security. Inter-VLAN routing is configured to enable controlled communication between these segments.

Advanced IP addressing schemes, including subnetting and DHCP, are implemented to optimize IP resource allocation. Static and dynamic routing protocols, such as OSPF (Open Shortest Path First), are employed to ensure efficient and reliable data routing across the network. Security measures, including Access Control Lists (ACLs) and port security, are integrated to protect sensitive ticketing data from unauthorized access and potential cyber threats.

The network design is validated through rigorous testing, including connectivity checks, redundancy simulations, and performance evaluations. The simulation results demonstrate the effectiveness of the proposed architecture in providing a secure, efficient, and scalable solution for centralized railway ticketing. This project not only addresses the technical challenges of network design but also highlights the critical role of networking in supporting large-scale operational systems, ultimately contributing to the seamless functioning of the railway industry.

# Table of Contents



**TABLE OF FIGURES**

# 1. Introduction

## 1.1 Background

In the era of advanced digital transformation, transportation systems like railways require highly reliable and scalable network infrastructures to support ticketing, scheduling, and operational management across multiple locations. A centralized railway network must serve the needs of ticket counters, customer service offices, and administrative departments at various stations while ensuring seamless access to ticketing databases and real-time scheduling information. This project aims to design a network that is not only efficient and secure but also capable of handling the demands of future growth, as railway operations expand and the volume of passengers increases.

This project focuses on creating a centralized ticketing system network infrastructure that connects multiple railway stations through a single, unified network. By centralizing ticketing and administrative services, the railway network will provide each station with real-time access to ticket inventory, booking updates, and secure communication channels to manage operations effectively. The centralized design also supports mobile ticketing, online booking, and integration with external services like payment gateways and customer support.

The network must support a wide variety of devices, including ticket counters, administrative PCs, server rooms, and cloud services. The design must accommodate both internal station communications and external data connections to cloud servers, enabling reliable access to customer data, ticketing information, and administrative services. This requires the implementation of VLANs to segment the network, DHCP for dynamic IP management, inter-VLAN routing, and robust security protocols to ensure data protection and regulatory compliance.

Cisco Packet Tracer will be used to design and simulate this network, ensuring that it meets the critical technical requirements for scalability, security, and reliability while supporting a high level of operational efficiency across all connected railway stations.

---

## 1.2 Objectives

The primary objective of this project is to design a comprehensive, efficient, and secure centralized railway ticketing network that connects multiple railway stations and centralizes the management of ticketing, scheduling, and customer support services.

**Key objectives include:**

- **VLAN Configuration**: Segment the network by functions (Different ticketing counters) to optimize network performance and enhance security.
- **Dynamic IP Addressing**: Use a DHCP server to dynamically assign IP addresses to ticketing counters and administrative devices, simplifying network management.
- **Inter-VLAN Routing**: Implement inter-VLAN routing to allow communication across different VLANs, enabling seamless data flow between departments and stations.
- **Routing Protocols**: Use OSPF as the dynamic routing protocol for efficient data transfer across stations, ensuring real-time access to centralized databases.
- **Security**: Apply security best practices, such as SSH for secure remote management and port security to restrict unauthorized device connections.
- **Scalability**: Design the network to accommodate future expansions, allowing for the addition of more stations, ticketing counters, and network resources as railway operations grow.
- **Cloud Services Integration**: Establish connectivity to cloud-hosted services, including centralized ticket databases, through appropriate static and dynamic routing configurations.
- **Testing and Verification**: Conduct thorough testing and validation to ensure network functionality, connectivity across stations, and implementation of security protocols.

---

# 2.Network Design

## 2.1 Topology

The centralized railway ticketing network is designed using a three-layer hierarchical model, consisting of the **Core Layer**, **Distribution Layer**, and **Access Layer**. This structure allows for efficient data management, secure access, and seamless scalability across the various stations and service points within the network.

- **Core Layer**: The Core Layer houses the main data center, where high-speed core routers interconnect critical servers, such as the centralized ticketing server, database servers, and backup systems. These core routers provide reliable and secure communication between regional offices, ticket counters, and external interfaces for public access. The core routers also handle routing between internal network segments and external systems, such as cloud-hosted applications for mobile ticketing and self-service kiosks. The design of the core layer ensures centralized control, data consistency, and high availability, supporting the core functions of the ticketing system.
- **Distribution Layer**: The Distribution Layer connects the Core Layer to the Access Layer and is composed of Layer 3 switches strategically placed in regional offices. These switches are configured to manage inter-VLAN routing and traffic policies, ensuring data segmentation between different service areas (e.g., ticket counters, administration, and customer service) while allowing secure communication. The distribution layer is responsible for enforcing network policies, including access control lists (ACLs), to limit inter-departmental data flow and manage traffic between VLANs. This layer provides the necessary infrastructure to scale the network as additional stations or service points are added.
- **Access Layer**: The Access Layer connects end devices through Layer 2 switches located at individual stations and ticket counters. Each access switch manages dedicated VLANs for different operational areas, such as ticket counters, customer service desks, and administrative offices. For example, ticket counters are assigned to a specific VLAN to manage high-traffic transactions securely, while administration and customer service each have their own VLANs to control and isolate traffic. Self-service kiosks and mobile apps access the ticketing system through secure public interfaces, ensuring safe, controlled interaction with the centralized ticketing server. Access switches are configured with port security to prevent unauthorized devices from connecting to the network, providing an added layer of security at each service point.

This layered topology ensures the network is scalable, secure, and efficient, accommodating the growing operational needs of the railway system. It provides centralized management of ticketing, real-time data consistency, and secure access across all railway stations and customer service points.

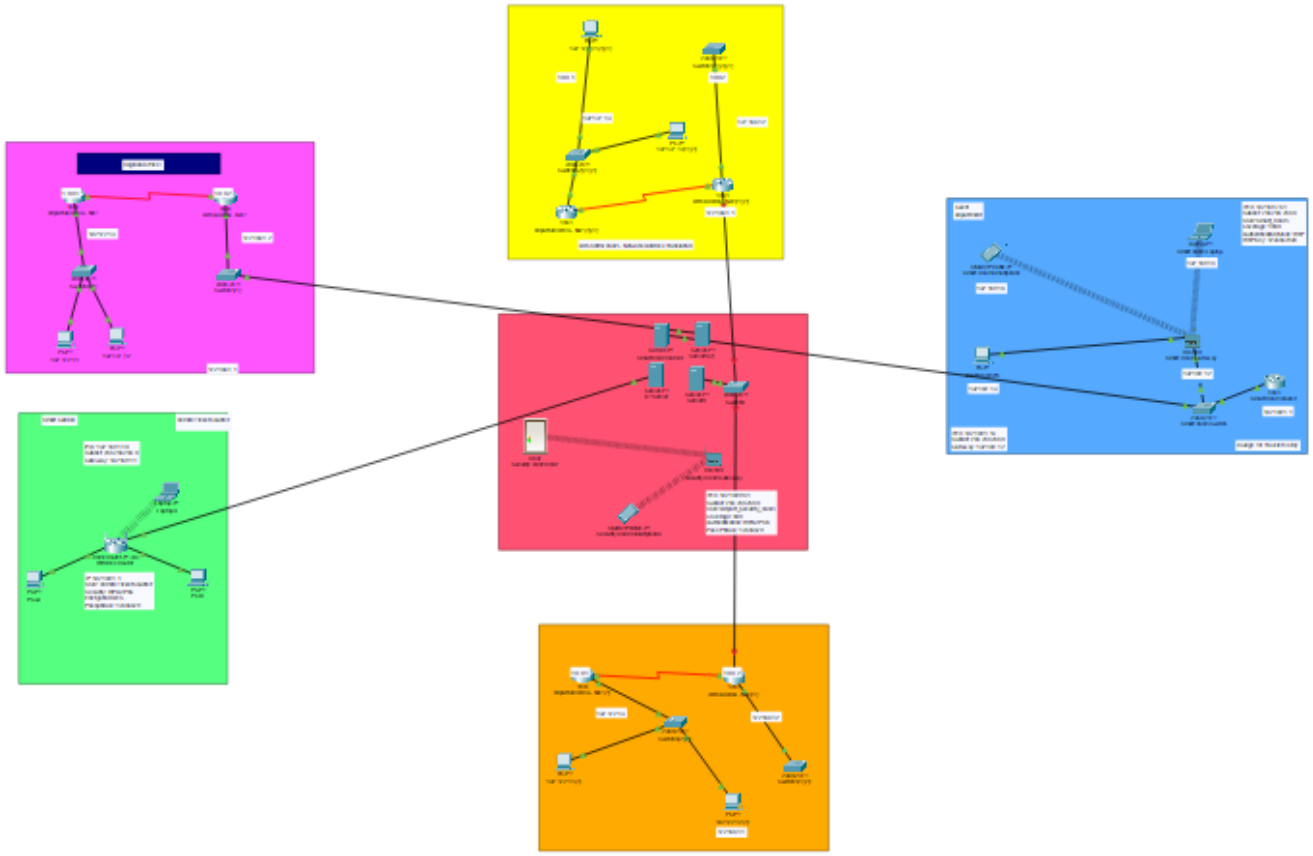

*Figure 1: Topology of full network*

## 2.2 Components

The components of the centralized railway ticketing network are designed to create a secure, scalable, and efficient infrastructure. These components facilitate seamless communication between railway stations, centralized servers, and external interfaces, supporting real-time ticketing and administrative functions. The main components include:

1. **Routers**:
   - **Core Routers**: Positioned in the data center, these core routers provide high-speed, central routing for all connected railway stations, regional offices, and remote ticket counters. They ensure reliable, secure communication with centralized servers and manage external

connectivity for kiosks and mobile apps.

- **Regional Office Routers**: Connect each regional office to the core network, handling local routing for connected stations and managing data traffic back to the data center.
- **Public Access Router**: Enables secure external connections to the ticketing system for self-service kiosks and mobile apps, implementing security measures like NAT (Network Address Translation) to safeguard internal resources.

2. **Switches**:

- **Layer 3 (L3) Switches**: Located at regional offices, these switches support inter-VLAN routing, allowing different departments (e.g., ticket counters, administration, and customer service) to communicate securely. Examples include switches assigned to the North and South regional offices.
- **Layer 2 (L2) Access Switches**: Positioned at ticket counters and service desks in individual railway stations, these switches provide connectivity for end devices and segregate traffic through VLANs. Examples include switches connecting ticket counter PCs, administrative PCs, and customer service desks.

3. **Servers**:

- **Centralized Ticketing Server**: Housed in the data center, this server is responsible for managing ticket inventory, bookings, and real-time updates across all stations.
- **Database Server**: Also in the data center, this server securely stores customer information, booking history, and scheduling data.
- **Backup Server**: Ensures data redundancy and disaster recovery by regularly backing up ticketing and database information.

4. **VLANs (Virtual Local Area Networks)**:

- **VLAN 100**: For Ticketing Server traffic (IP range: 192.168.100.0/24).
- **VLAN 110**: For Database Server traffic (IP range: 192.168.110.0/24).
- **VLAN 200**: Ticket Counters (IP range: 192.168.200.0/24).
- **VLAN 210**: Administration (IP range: 192.168.210.0/24).
- **VLAN 220**: Customer Service (IP range: 192.168.220.0/24).
- **VLAN 300**: Public Access (for kiosks and mobile apps with IP range: 192.168.300.0/24).

5. **End Devices**:

- **PCs at Ticket Counters**: Deployed at each ticket counter, connected to the network through dedicated VLANs to handle high-volume transactions securely.
- **Administrative PCs**: Located in regional offices and connected to the administration VLAN, these PCs support station management and reporting functions.

- **Customer Service PCs**: Connected to the customer service VLAN, these PCs provide assistance and manage customer inquiries related to ticketing and travel.

6. **Self-Service Kiosks and Mobile Apps**:

- **Public Interfaces**: Kiosks and mobile apps access the ticketing system through secure public interfaces, managed by the public access router. These devices are segregated into a public VLAN to prevent direct access to internal resources, ensuring controlled and secure interaction with the centralized ticketing system.

7. **IP Addressing and Subnets**:

- Each VLAN is assigned a distinct subnet to facilitate organized IP management and secure traffic flow. The subnets are configured to support scalability and efficient routing across multiple stations.

- **Example IP Ranges**:
  - Ticketing Server: 192.168.100.0/24
  - Ticket Counters: 192.168.200.0/24
  - Administration: 192.168.210.0/24
  - Public Access: 192.168.300.0/24

This organized layout enables secure and efficient communication across railway stations, regional offices, and public interfaces. Each VLAN and network component serves a specific purpose, ensuring that ticketing operations are centralized, accessible, and resilient, providing reliable service for railway customers and staff.

---

### 2.3 IP Addressing Scheme

The IP addressing scheme for the centralized railway ticketing network is organized by VLANs and location to ensure structured IP management and secure traffic segmentation. Each VLAN has a unique subnet, and additional subnets are designated for connections between the core routers and Layer 3 switches at regional offices.

**Base Network**: 192.168.0.0/16

**Data Center (Core Layer)**

| Component | Network Address | Subnet Mask | Host Address Range | Broadcast Address |
|---|---|---|---|---|
| Centralized Ticketing Server | 192.168.100.0 | 255.255.255.0/24 | 192.168.100.1 to 192.168.100.254 | 192.168.100.255 |

| Component | Network Address | Subnet Mask | Host Address Range | Broadcast Address |
|---|---|---|---|---|
| VLAN | | | | |
| Database Server VLAN | 192.168.110.0 | 255.255.255.0/24 | 192.168.110.1 to 192.168.110.254 | 192.168.110.255 |
| Backup Server VLAN | 192.168.120.0 | 255.255.255.0/24 | 192.168.120.1 to 192.168.120.254 | 192.168.120.255 |

**Regional Offices (Distribution Layer)**

Each regional office is connected to the core network and hosts local ticket counters, administration, and customer service departments. VLANs at each regional office segment network traffic based on operational requirements.

| Department | Network Address | Subnet Mask | Host Address Range | Broadcast Address |
|---|---|---|---|---|
| Ticket Counters (VLAN 200) | 192.168.200.0 | 255.255.255.0/24 | 192.168.200.1 to 192.168.200.254 | 192.168.200.255 |
| Administration (VLAN 210) | 192.168.210.0 | 255.255.255.0/24 | 192.168.210.1 to 192.168.210.254 | 192.168.210.255 |
| Customer Service (VLAN 220) | 192.168.220.0 | 255.255.255.0/24 | 192.168.220.1 to 192.168.220.254 | 192.168.220.255 |

**Remote Ticket Counters and Public Access (Access Layer)**

Remote ticket counters and self-service kiosks are part of the public-facing side of the network, allowing customer access to ticketing services through secure interfaces.

| Component | Network Address | Subnet Mask | Host Address Range | Broadcast Address |
|---|---|---|---|---|
| Public Access for Kiosks and Mobile Apps (VLAN 300) | 192.168.300.0 | 255.255.255.0/24 | 192.168.300.1 to 192.168.300.254 | 192.168.300.255 |

**Core Router and Layer 3 Switch Connections**

The core routers and Layer 3 switches at the data center and regional offices require dedicated subnets for

secure routing and redundancy.

| Link | Network Address | Subnet Mask | Host Address Range | Broadcast Address |
|---|---|---|---|---|
| Core Router 1 - Layer 3 Switch (Data Center) | 10.10.10.0 | 255.255.255.252/30 | 10.10.10.1 to 10.10.10.2 | 10.10.10.3 |
| Core Router 2 - Layer 3 Switch (Data Center) | 10.10.10.4 | 255.255.255.252/30 | 10.10.10.5 to 10.10.10.6 | 10.10.10.7 |
| Core Router - Regional Office 1 L3 Switch | 10.10.10.8 | 255.255.255.252/30 | 10.10.10.9 to 10.10.10.10 | 10.10.10.11 |
| Core Router - Regional Office 2 L3 Switch | 10.10.10.12 | 255.255.255.252/30 | 10.10.10.13 to 10.10.10.14 | 10.10.10.15 |

**Public IPs for External Access (ISP Connection)**

Public IP addresses are used for secure access to the centralized network from external sources, such as self-service kiosks and mobile applications.

| Public Link | Public Network Address | Subnet Mask | IP Range |
|---|---|---|---|
| Core Router to ISP | 103.133.254.0 | 255.255.255.252/30 | 103.133.254.1 to 103.133.254.2 |
| Backup ISP Link | 103.133.254.4 | 255.255.255.252/30 | 103.133.254.5 to 103.133.254.6 |

This IP addressing scheme allows efficient traffic management, security through segmented subnets, and structured routing across the centralized railway network, ensuring reliable communication between railway stations, the data center, and public access points.

---

# 3. Routing Configuration

## 3.1 Router Configuration

The network routing for the **Centralized Railway Ticketing System** utilizes a combination of VLAN, routing protocols, DHCP, and static and dynamic routing to ensure efficient and secure communication across the data center, regional offices, remote ticket counters, and public access kiosks.zz

#### VLAN Configuration

- **Define VLANs**: Each department and service area (ticket counters, administration, customer service, public kiosks, etc.) has a unique VLAN ID to manage traffic segmentation. VLAN IDs and subnets are configured on the core router to handle traffic segregation within the network.
- **Trunking Configuration**: Trunking is configured on interfaces connecting the core router to switches for regional offices and ticket counters, using **encapsulation dot1q**. This setup enables multiple VLANs to communicate over a single trunk link.

#### Routing Protocol (EIGRP)

- **Enable EIGRP**: EIGRP is configured on the core router for efficient dynamic routing across the network, enabling fast convergence and supporting VLSM (Variable Length Subnet Masking).
- **Advertise Networks**: All VLAN network IDs associated with each regional office and the data center are advertised under the EIGRP routing process, allowing automatic updates and minimizing routing table configurations.

#### DHCP Configuration

- **Dynamic IP Allocation**: DHCP pools are configured for each VLAN, with unique IP ranges, subnet masks, default gateways, and DNS settings. This configuration allows automatic IP address allocation to all end devices, including ticket counters, kiosks, and administrative PCs.

#### IP Address Assignment

- **Interface IPs**: Each VLAN interface (sub-interface) is assigned a unique IP address within its respective subnet, providing default gateway functionality for devices on each VLAN.
- **Encapsulation dot1q**: Trunk links use dot1q encapsulation, enabling tagged VLAN traffic over single links for inter-VLAN communication on the core router.

#### Branch Connectivity (Static Routing)

- **Static Route Configuration**: Static routes are configured on the core router to connect regional offices and branch routers, providing dedicated, direct paths for remote site connectivity.
- **Verification and Troubleshooting**: Ensure connectivity and reachability for all VLANs from the core to regional and branch routers, finalizing the setup for network-wide connectivity.

## 3.2 Static and Dynamic Routing (EIGRP)

A hybrid routing strategy is used in this project. **Static routes** handle critical connections between the core and branch routers, while **dynamic routing (EIGRP)** manages internal VLANs and regional connections.

**Static Routing**:

- Static routes are configured for direct paths to centralized DHCP, database servers, and other critical resources in the data center. This configuration provides predictable, stable paths for essential services, reducing latency.

**Dynamic Routing with EIGRP**:

- **EIGRP** is implemented on the core and branch routers to adapt routing paths based on network topology changes. This enables the network to self-adjust, supporting future expansions and fault tolerance.

---

# 5. Inter-VLAN Routing

The **Inter-VLAN Routing** configuration in our centralized railway network enables efficient communication between various VLANs set up for ticketing counters, administrative offices, customer service, and public access kiosks. This routing is accomplished through **Layer 3 (L3) switching** in both the main and branch routers, allowing different network segments to communicate securely and effectively.

### 1.1 Layer 3 Switching in Core Router

In the data center, **Layer 3 switching** is implemented on the core router to manage inter-VLAN routing for primary VLANs. Each VLAN represents a distinct network segment (e.g., ticket counters, administration), providing secure and segmented traffic flow.

**Inter-VLAN Configuration in the Core Router:**

plaintext
Copy code

```
interface vlan 100
 ip address 192.168.100.1 255.255.255.0
 no shutdown

interface vlan 110
 ip address 192.168.110.1 255.255.255.0
 no shutdown

interface vlan 120
 ip address 192.168.120.1 255.255.255.0
 no shutdown

interface vlan 200
 ip address 192.168.200.1 255.255.255.0
 no shutdown

interface vlan 210
 ip address 192.168.210.1 255.255.255.0
 no shutdown

interface vlan 220
 ip address 192.168.220.1 255.255.255.0
 no shutdown

interface vlan 300
 ip address 192.168.300.1 255.255.255.0
 no shutdown

exit
write memory
```

Each interface above is assigned an IP address that acts as the **default gateway** for devices within that VLAN. For example, **VLAN 200** (Ticket Counters) has the gateway IP 192.168.200.1. This allows ticket counter devices to communicate with other VLANs through the core router.

### 1.2 Layer 3 Switching in Regional Office Router

In each regional office, Layer 3 switching is configured on the branch router to manage inter-VLAN routing locally. This configuration enables efficient communication between local segments at each regional office and allows routing back to the main data center.

**Inter-VLAN Configuration in Branch Router:**

plaintext

Copy code

```
interface vlan 400
 ip address 192.168.400.1 255.255.255.0
 no shutdown

interface vlan 410
 ip address 192.168.410.1 255.255.255.0
 no shutdown
```

In this setup:

- **VLAN 400** may be assigned to local ticket counters, while **VLAN 410** could be for regional administrative offices.

### 1.3 PC Configuration via DHCP

To simplify IP management, **DHCP** is used to dynamically assign IP addresses to devices within each VLAN, such as ticket counter PCs, administrative workstations, and customer service devices. DHCP is configured on the core router for main VLANs, and each VLAN has a dedicated DHCP pool with specific IP ranges.

Example DHCP configuration for **VLAN 200 (Ticket Counters)**:

plaintext

Copy code

```
ip dhcp pool Ticket_Counter_Pool
 network 192.168.200.0 255.255.255.0
 default-router 192.168.200.1
 dns-server 8.8.8.8
```

This configuration assigns addresses from 192.168.200.0/24 to devices in VLAN 200, with 192.168.200.1 as the default gateway. Similar DHCP pools are created for other VLANs to ensure automatic IP allocation within each segment.

### 1.4 Subnetting

**Subnetting** plays a crucial role in organizing and efficiently managing IP addresses across the network. The base network (192.168.0.0/16) is subnetted to provide each VLAN with a unique range, allowing separate address spaces for different departments.

For example:

- **VLAN 100 (Centralized Ticketing Server)** uses the subnet 192.168.100.0/24.
- **VLAN 200 (Ticket Counters)** uses the subnet 192.168.200.0/24.
- **VLAN 300 (Public Access)** uses the subnet 192.168.300.0/24.

By assigning distinct subnets, each VLAN can be isolated, improving security and facilitating organized IP management. This structured approach also supports scalability, allowing additional stations or departments to be easily added by assigning new subnets within the 192.168.0.0/16 range.

---

## 6. Security Measures

To enhance security and optimize traffic management in the Centralized Railway Ticketing System, VLAN segmentation has been implemented across the network. VLANs allow for logical grouping of network devices based on function, department, or security level, providing isolation between different network segments. By assigning separate VLANs for servers, user devices, and administrative systems, we can control access and minimize the risk of unauthorized access between different parts of the network.

In addition to VLANs, dot1q encapsulation is used on trunk links between network switches to carry multiple VLANs across a single physical link. This method ensures that traffic from each VLAN remains segregated, preventing cross-VLAN access and reducing the potential for network disruptions caused by broadcast storms or malicious activity. By tagging frames with VLAN IDs, dot1q encapsulation supports traffic isolation, improving the security of the network and maintaining efficient data flow.

The use of VLANs and dot1q encapsulation enables granular network access control, allowing administrators to enforce security policies and limit the impact of potential threats. In the context of the Centralized Railway Ticketing System, this approach ensures that critical data, such as customer payment information and booking records, remains secure within its designated network segment. By preventing unauthorized access and containing security incidents within specific VLANs, the system's overall security posture is significantly enhanced, providing a safer and more reliable service for both users and administrators.

# 7. Testing and Validation

### 3.3 Simulation

For testing the Centralized Railway Ticketing System's network design, **Cisco Packet Tracer** was used as the primary simulation tool. Packet Tracer offers a virtual environment for designing, configuring, and testing network setups, allowing us to simulate real-world network operations. The simulation process included the following steps:

- **Network Topology Design:** The network design was created within Packet Tracer, including servers, workstations, routers, switches, and firewalls, ensuring the topology met the requirements of the ticketing system. The network was designed to support seamless ticket bookings, secure payment transactions, and efficient data flow across multiple user interfaces.
- **Configuration Implementation:** Once the network topology was established, configurations were applied to various devices such as routers, switches, and firewalls based on the system's security and communication requirements. Using Packet Tracer's user-friendly interface, devices were configured with IP addressing, VLANs, routing protocols (OSPF), and other necessary settings.
- **Traffic Simulation:** Packet Tracer facilitated the simulation of traffic across the network, enabling the verification of connectivity between devices. Various traffic patterns were simulated to ensure that data flowed as expected, especially during high traffic times, such as ticket booking periods, ensuring a smooth user experience.
    - **Verification of Redundancy and Failover:** Redundancy at every layer of the network was tested, including multiple routers and multilayer switches. Failover mechanisms were verified to ensure the system would maintain functionality in case of hardware failure or network disruptions.
    - **DHCP and IP Address Allocation:** The **Dynamic Host Configuration Protocol (DHCP)** functionality was tested to ensure devices within the network received IP addresses dynamically from the DHCP server. Devices in critical areas, such as the server room, were configured with static IP addresses for more consistent management.

### 3.4 Troubleshooting

During the testing phase, several troubleshooting steps were implemented to address common network issues and ensure smooth operations:

- **Device Connectivity:** Connectivity across VLANs and inter-departmental communication were thoroughly tested. Inter-VLAN routing configurations were reviewed to ensure that devices in different VLANs could communicate with each other and that no unauthorized access was allowed between departments.
- **DHCP Issues:** DHCP functionality was verified to ensure devices received the correct IP addresses dynamically. Any issues related to unreachable DHCP servers were resolved, and static IP configurations for key servers were confirmed.
- **Routing Configuration:** The **Open Shortest Path First (OSPF)** routing protocol was implemented across routers and multilayer switches. The routing tables were verified for accuracy, and inter-departmental communication was tested to ensure that the network handled traffic effectively.
- **Access Control Issues:** Access Control Lists (ACLs) were reviewed to ensure they allowed necessary traffic while blocking unauthorized access. ACLs were implemented to restrict access to critical areas of the network, such as the server room and administrative systems, ensuring data security.
- **Port Security:** Port security configurations on key switches, especially those used by sensitive departments like the Finance team, were tested. Each switchport was configured to allow only one device per port, preventing unauthorized devices from connecting to the network and ensuring secure access control.

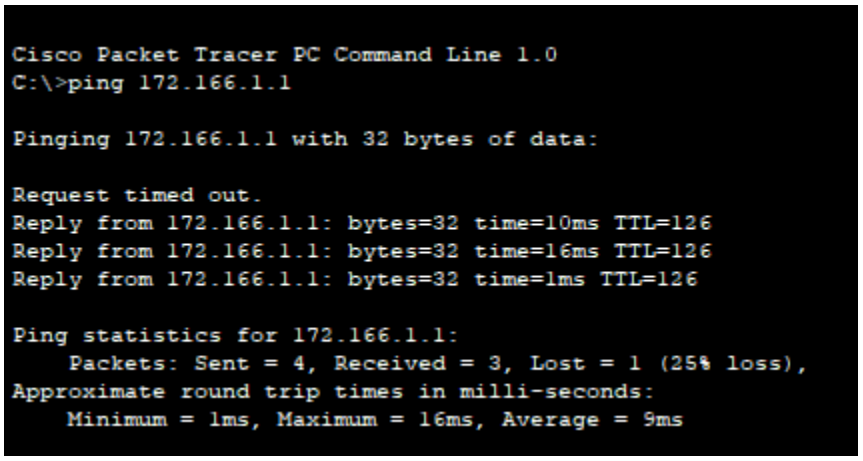


*Figure 2: Successful Ping Test*

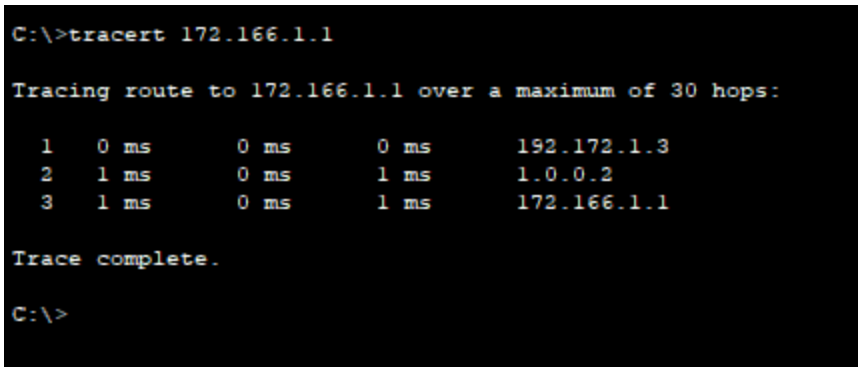


*Figure 3: Successful traceroute test*

By thoroughly simulating and troubleshooting the network, we ensured that the Centralized Railway Ticketing System's infrastructure was robust, secure, and capable of handling the expected network traffic efficiently.

# 8. Results and Evaluation

### 4.3 Performance Metrics

The performance of the **Centralized Railway Ticketing System** network was thoroughly evaluated using key performance metrics to ensure the network operated optimally. These metrics included:

- **Network Latency:** Latency was measured to assess the time delay for data to travel across the network. Low latency was critical to ensure fast ticket booking and transaction processing for users.
- **Throughput:** Throughput was tested to determine the network's capacity to handle high traffic volumes, especially during peak booking periods. Ensuring sufficient throughput helped maintain the system's responsiveness.
- **Redundancy Testing:** The network was tested for redundancy, particularly for failover mechanisms, to ensure continued availability of services during hardware or link failures.
- **DHCP Response Time:** DHCP servers were tested for speed in assigning IP addresses to devices across different VLANs, ensuring quick connectivity for users.
- **Inter-VLAN Routing Performance:** The performance of routing between VLANs was measured to ensure smooth communication between different departments and user segments.
- **Security:** Security tests were conducted to ensure proper segmentation and access controls were in place, preventing unauthorized access and data breaches.
- **Quality of Service (QoS):** QoS configurations were evaluated to prioritize critical traffic, such as payment transactions, over less critical data, ensuring a seamless user experience.
- **NAT/PAT Functionality:** Network Address Translation (NAT) and Port Address Translation (PAT) functionality were tested to ensure correct handling of external communication and address translation for users.

```
C:\>ping 192.168.7.2

Pinging 192.168.7.2 with 32 bytes of data:

Reply from 192.168.7.2: bytes=32 time<1ms TTL=127
Reply from 192.168.7.2: bytes=32 time<1ms TTL=127
Reply from 192.168.7.2: bytes=32 time<1ms TTL=127
Reply from 192.168.7.2: bytes=32 time=9ms TTL=127

Ping statistics for 192.168.7.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 9ms, Average = 2ms
```

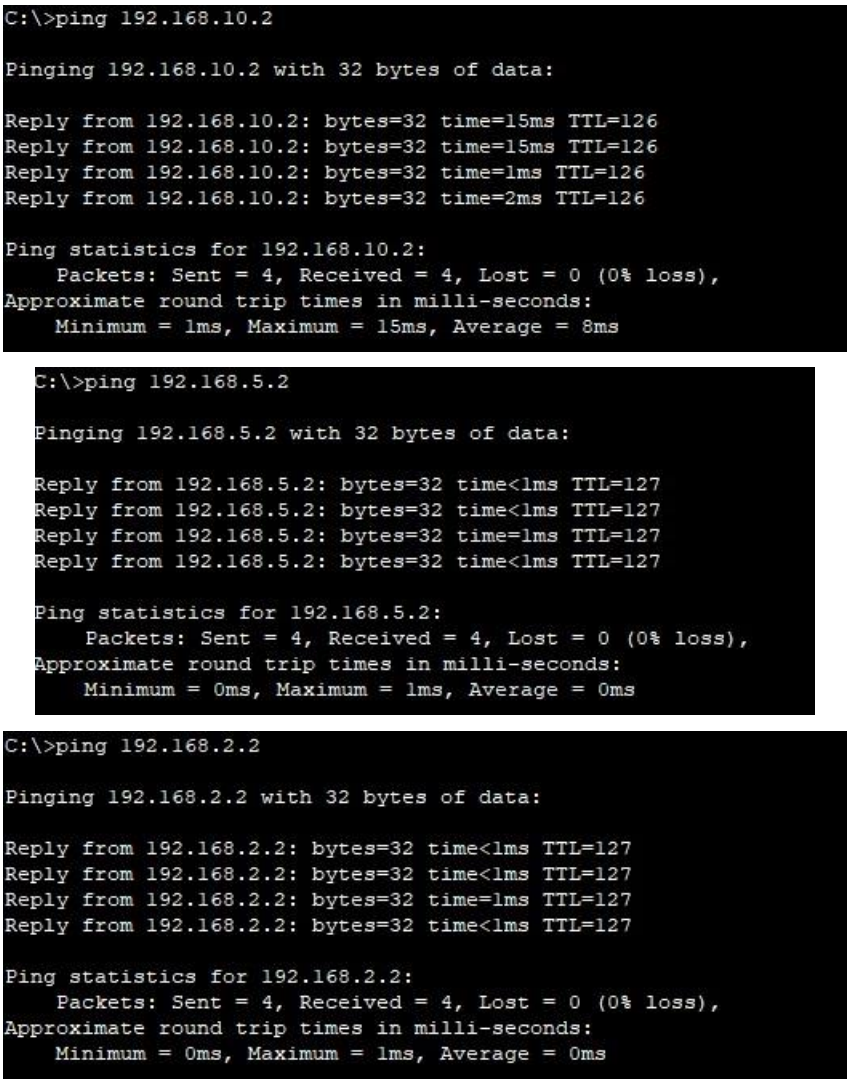


*Figure 4: Performance Measure Through Ping Time*

---

## 5. Conclusion

### 5.3 Summary

In summary, the **Centralized Railway Ticketing System** project successfully designed and implemented a scalable, secure, and efficient network architecture to handle the operational needs of the railway system. The network design utilized a **three-layer hierarchical model**, incorporating core routers, Layer 3 and Layer 2 switches, and dedicated DHCP servers to manage inter-departmental communication and VLAN segmentation. Each department was assigned a unique VLAN to ensure effective traffic management and enhanced security.

Routing configurations were implemented using **OSPF** for internal communication, while static routing was used for external services like cloud-based payment gateways. **Router on a Stick** was employed for inter-VLAN routing, enabling seamless communication between different network segments. Additionally, **IEEE 802.1Q encapsulation** was used on trunk links to segment traffic, enforce security, and prevent unauthorized access between VLANs. This setup also helped mitigate the risk of broadcast storms, ensuring stable network performance.

### 5.4 Lessons Learned

Throughout the project, several key lessons were learned, which helped improve the overall design and implementation of the network:

- **Redundancy and Network Segmentation:** Ensuring proper VLAN segmentation for different departments improved traffic management and security, making the network more efficient and easier to manage.
- **Subnetting and Addressing:** Careful planning of IP addressing and subnetting was critical to avoid conflicts and optimize address allocation for a growing user base.
- **Redundancy and High Availability:** Adding more redundancy, especially at the core layer, would further enhance network reliability and resilience against hardware failures.
- **Router on a Stick for Inter-VLAN Routing:** While effective, Router on a Stick required meticulous configuration of trunking and encapsulation to maintain smooth communication between VLANs.
- **Security Measures:** Implementing robust security practices, such as **SSH** for secure remote access and **port security**, was vital to protect the network from unauthorized access and potential breaches.
- **Scalability Considerations:** Ensuring the design was scalable for future growth, both in terms of users and network capacity, was essential for accommodating the system's long-term needs.
- **Network Management and Monitoring:** The importance of continuous monitoring and proactive management was highlighted to ensure optimal performance and swiftly address any emerging issues.

This project laid a strong foundation for the **Centralized Railway Ticketing System**, ensuring that it is secure, reliable, and capable of supporting future growth as the system evolves.

# 1 References


- Cisco Systems, Inc. (2020). Cisco Networking Basics: A Comprehensive Guide to Networking Fundamentals. Cisco Press.

- Tan, K. (2021). Network Design and Implementation: A Guide to Best Practices. Wiley & Sons.

- RFC 2453. (1998). Routing Information Protocol version 2 (RIPv2). Retrieved from: https://www.rfc-editor.org/rfc/rfc2453

- Cisco Systems, Inc. (2019). Configuring VLANs and Inter-VLAN Routing in Cisco Packet Tracer. Cisco Networking Academy.

- Baker, P. (2018). Designing Enterprise Networks: Principles and Best Practices. Pearson Education.

- Cai, D., & Li, Y. (2020). Implementing Secure Network Infrastructure: A Practical Guide to Security Protocols and Strategies. Springer.

- Cisco Systems, Inc. (2022). Configuring DHCP on Cisco Routers and Switches. Cisco Documentation. Retrieved from: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_dhcp/configuration/xe-3s/iad-xe-3s-book/

- Hughes, C., & Stepanek, M. (2019). Understanding and Implementing Network Security Solutions. McGraw-Hill Education.

# 2 Appendices

**Abbreviations**:

DHCP - Dynamic Host Configuration Protocol

IP - Internet Protocol

VLAN - Virtual Local Area Network

Encapsulation dot1q

RIP V2

Subnetting