CHAPTER 1

INTRODUCTION

1.1 OBJECTIVE

This project focuses on developing a robust and efficient network infrastructure for a multi-floor hotel, designed to meet the demands of modern connectivity and secure data management across various departments. The network covers three floors, each with distinct departments: Reception, Store, and Logistics on the first floor; Finance, HR, and Sales on the second; and IT and Admin on the third. Each department is allocated a unique VLAN and IP subnet, ensuring data separation and efficient traffic management. Routers located in the IT department's server room connect each floor, with OSPF used for dynamic routing and reliable inter-departmental communication.

To enhance control, scalability, and security, the network incorporates Software-Defined Networking (SDN), which enables centralized management through an SDN controller. The controller automates configurations for VLAN assignments, DHCP, and routing paths, significantly reducing manual configurations and enabling real-time adjustments based on network conditions. Security is prioritized with policies like port security on specific devices, enforced dynamically through the controller to restrict unauthorized access.

The project also includes wireless networks on each floor for seamless connectivity of laptops and mobile devices, while wired access is configured for department printers and other essential devices. By integrating SDN, this network design combines traditional networking with modern SDN capabilities, offering streamlined management, enhanced performance, and improved security for hotel operations.

The proposed network spans three floors, each dedicated to specific hotel departments, and integrates various elements such as VLAN segmentation, dynamic IP allocation through DHCP, and OSPF routing for efficient data flow. The core of the network is controlled by an SDN controller, enabling centralized handling of VLAN assignments, routing, IP management, and security policies. This integration of SDN's programmability with conventional networking principles ensures a flexible and secure environment, capable of responding to real-time changes in network traffic and maintaining optimal performance. The result is a cutting-edge network solution that supports seamless connectivity, enhanced security, and improved operational efficiency, creating an optimal environment for both guests and hotel staff.

The hotel's network infrastructure is designed with security and reliability as top priorities. Through features like automated port security and dynamic device authentication, the SDN framework enhances network protection by controlling which devices gain access and responding swiftly to potential threats. These capabilities are particularly critical in safeguarding sensitive areas such as the IT department and guest data systems. Additionally, the integration of centralized SSH access facilitates secure remote management, enabling IT staff to maintain network stability and make configuration changes without being physically present. The outcome is a highly responsive and adaptive network that supports an array of devices—from laptops and smartphones to smart room technology—creating an environment that meets the connectivity expectations of modern guests and the operational needs of hotel staff.

In summary, this SDN-based network design introduces a transformative approach to managing hotel IT infrastructure. It blends the reliability of traditional networking with the innovation of software-defined systems, ensuring scalability, performance optimization, and superior security. This project lays the foundation for a forward-thinking, adaptable network architecture that can evolve as new technologies emerge, keeping the hotel at the forefront of hospitality technology and guest satisfaction.

CHAPTER 2

LITERATURE SURVEY

1. **Intelligent Traffic Engineering in Software-Defined Vehicular Networking Based on Multi-Path Routing (2020)**

Author: Ahed Abugabah, Ahmad Ali Alzubi, Osama Alfarraj, Mohammed Al-Maitah, Waleed S. Alnumay

Paper work:

The traffic engineering (TE) approach in software-defined vehicular networking (SDVN) represents a comprehensive solution to modern vehicular network challenges. At its core, this system implements a modified wave routing algorithm that enables dynamic multi-path routing capabilities, significantly enhancing network efficiency and reliability. The architecture leverages SDVN's centralized control structure, which separates the control and data planes, allowing for more flexible and programmable network management. Through this design, the system can perform real-time traffic monitoring and implement adaptive routing strategies based on current network conditions. The modified TE method notably reduces the computational complexity of path formation and reconfiguration time, making it more responsive to rapidly changing vehicular network demands. Additionally, the dynamic path reconfiguration algorithm ensures optimal resource utilization by continuously adjusting routes based on traffic patterns and network load. This integrated approach results in improved network performance, reduced latency, and enhanced overall reliability, making it particularly suitable for the demanding requirements of modern vehicular networks. The system's ability to balance traffic loads and avoid congestion while maintaining efficient resource utilization demonstrates its effectiveness in addressing the complex challenges of vehicular networking environments.

2. **SDN-enabled Traffic Engineering and Advanced Blackhole Filtering at the IXP (2021)**

Author: Marco Chiesa, Christoph Dietzel, Gianni Antichi, Marc Bruyere

Paper work:

Software-Defined Networking (SDN) implementation at Internet Exchange Points (IXPs) represents a transformative approach to managing and securing internet traffic exchange. This innovative architecture integrates SDN principles into IXP operations, where multiple Internet Service Providers (ISPs) and Content Delivery Networks (CDNs) interconnect to exchange traffic. The implementation enables sophisticated traffic engineering capabilities through a centralized control plane, allowing for dynamic and programmable network management. By leveraging SDN's flexibility, IXPs can implement advanced traffic management strategies, including real-time load balancing and intelligent path selection, significantly improving network efficiency and reducing latency.

A key feature of this implementation is the enhanced security framework, particularly in the realm of blackhole filtering. This security mechanism effectively mitigates Distributed Denial of Service (DDoS) attacks by dynamically identifying and dropping malicious traffic patterns. The SDN-based approach allows for more granular control over security policies and faster response times to emerging threats. Furthermore, the system provides improved visibility into traffic patterns and anomalies, enabling proactive security measures and network optimization.

The architecture addresses several traditional IXP limitations by introducing programmable network elements and centralized control. This modernization enables more efficient resource utilization and enhanced scalability, crucial for handling the growing demands of internet traffic exchange. The implementation also facilitates better integration with existing infrastructure while providing a foundation for future services and capabilities. Through this comprehensive approach, the SDN-enabled IXP architecture not only improves current operations but also establishes a framework for the evolution of internet exchange infrastructure, supporting the increasing demands of modern network connectivity while maintaining robust security measures.

3. Secure SDN-Based Multi-Vehicle Platoon Formation in Smart Cities

Author: Mohammad Aazam, Sherali Zeadally, Kim-Kwang Raymond Choo

Paper work:

"Secure SDN-Based Multi-Vehicle Platoon Formation in Smart Cities" addresses a critical intersection of emerging technologies in transportation, networking, and urban development. Vehicle platooning, a concept where multiple vehicles travel in close formation to improve efficiency and safety, is gaining traction as a key component of smart city transportation systems. This study explores how Software-Defined Networking (SDN) can be leveraged to enhance the security and effectiveness of these platoons within the complex ecosystem of a smart city.
In the context of smart cities, vehicle platooning presents unique challenges and opportunities. The dynamic nature of urban traffic, the need for real-time communication, and the critical importance of security in automated vehicle systems all contribute to the complexity of implementing effective platooning solutions. By introducing SDN principles to this environment, researchers aim to create a more flexible, manageable, and secure framework for coordinating vehicle platoons.

The SDN-based approach allows for centralized control and management of the network infrastructure supporting vehicle platoons. This centralization enables more efficient resource allocation, dynamic adjustment of network parameters, and improved visibility into the overall system state. In the context of security, this architecture provides several advantages. It allows for uniform security policy implementation across the entire platoon network, rapid response to detected threats or anomalies, and the ability to isolate compromised vehicles or network segments quickly.

Security aspects addressed in this research likely include authentication mechanisms to ensure only authorized vehicles can join or interact with a platoon, encryption protocols to protect the sensitive data exchanged between vehicles and infrastructure, and intrusion detection systems tailored to the unique characteristics of vehicular networks. The study may also explore how SDN can facilitate secure vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication, which are crucial for maintaining platoon integrity and responding to changing traffic conditions.

CHAPTER 3

EXISTING SYSTEM

The project described in *"Intelligent Traffic Engineering in Software-Defined Vehicular Networking Based on Multi-Path Routing"* focuses on enhancing traffic management within vehicular networks through a novel approach that integrates Software-Defined Networking (SDN) with traditional Vehicular Ad Hoc Networks (VANETs). This integration forms Software-Defined Vehicular Networking (SDVN), an architecture designed to address the challenges of high mobility and frequent route reconfigurations that are typical in vehicular environments. The SDVN architecture is structured with three levels: the infrastructure layer for network devices, the management layer that provides centralized control via an SDN controller, and an application layer that manages traffic flow and optimizes resource allocation. By utilizing a centralized SDN controller, this design enables dynamic reconfiguration of routes based on real-time conditions, greatly enhancing the efficiency and responsiveness of the network. A key innovation of this project is the use of a modified wave routing algorithm for multi-path routing, which allows for multiple paths to be formed, reducing traffic congestion and increasing data transmission reliability.

Dynamic path reconfiguration further optimizes traffic flow by adjusting routes to avoid congested or overloaded paths, ensuring stable connections and reducing delays. This SDVN-based traffic engineering approach provides significant improvements over traditional VANETs by efficiently managing network resources, balancing loads across multiple paths, and supporting the growing demands of intelligent transportation systems (ITS) and smart city infrastructure.

3.1 LIMITATIONS

1. **Scalability Challenges**: As the number of vehicles and devices in a smart city increases, the centralized SDN controller may face scalability issues. The controller must handle an ever-growing volume of data and manage numerous dynamic connections, which could lead to performance bottlenecks.
2. **Dependence on Network Infrastructure**: The effectiveness of the SDVN architecture relies heavily on the availability and reliability of the underlying network infrastructure, including roadside units and communication links. In areas with inadequate infrastructure, the benefits of SDVN may be diminished.
3. **Latency in Route Reconfiguration**: Although the project aims to achieve real-time dynamic path reconfiguration, there may still be latency in the decision-making process and the implementation of new routes. This delay could lead to temporary inefficiencies or increased congestion during critical situations.
4. **Security Vulnerabilities**: Centralized control in SDN can create single points of failure and may make the network more susceptible to cyber-attacks. Ensuring the security of the SDN controller and communication channels is paramount, but it also adds complexity to the system.
5. **Complexity of Implementation**: Integrating SDN with existing VANET infrastructures may require significant changes to current systems and protocols. This complexity can lead to increased deployment costs and longer implementation times, potentially hindering widespread adoption.

CHAPTER 4

PROPOSED SYSTEM

Our proposed system is a comprehensive, SDN-based network infrastructure tailored for a multi-floor hotel environment, designed to address the specific needs of efficient management, scalability, security, and seamless inter-departmental communication. This network spans three floors, with each floor hosting specific departments. Departments on the first floor include Reception, Store, and Logistics; the second floor Finance, HR, and Sales; and the third floor is home to IT and Admin. Each department is assigned a distinct VLAN and IP subnet to ensure network segmentation, security, and efficient traffic flow.

At the core of our system is an SDN controller that centralizes the management of all network configurations, including VLAN assignments, IP addressing, routing policies, and security controls. This controller provides real-time oversight and control of network resources, allowing dynamic adjustments to configurations as new devices connect or conditions change within the network. By leveraging SDN, our system enables dynamic VLAN allocation, automated routing with OSPF, and centralized IP address management, simplifying network administration and minimizing manual configuration needs.

Wireless connectivity is available on each floor for mobile devices such as laptops and phones, while wired connections support fixed assets like printers in each department. Security is further enhanced through port security configurations managed by the SDN controller, restricting unauthorized devices from accessing sensitive parts of the network

The SDN controller dynamically balances network load, optimizes traffic flow, and mitigates potential congestion by adjusting routing paths in real-time. Overall, this proposed system offers a future-ready, highly adaptable network solution that enhances operational efficiency, improves security, and meets the dynamic demands of hotel operations.

Enhanced security features include real-time monitoring and automated threat response, empowering the network to detect and respond to potential breaches or unauthorized access attempts. This capability is crucial for protecting sensitive data in departments such as Finance and HR, where data integrity and confidentiality are paramount. Centralized SSH access further streamlines secure remote management for IT personnel, enabling quick and secure updates, troubleshooting, and network oversight from any location.

Overall, the integration of SDN technology into the hotel's network infrastructure results in an intelligent, adaptive, and secure system that supports the hotel's day-to-day operations while being prepared for future technological advancements. This approach not only meets current connectivity and management requirements but sets a strong foundation for the implementation of future smart hotel features, such as IoT

device management and enhanced guest services. The modified TE method notably reduces the computational complexity of path formation and reconfiguration time, making it more responsive to rapidly changing vehicular network demands. Additionally, the dynamic path reconfiguration algorithm ensures optimal resource utilization by continuously adjusting routes based on traffic patterns and network load. This integrated approach results in improved network performance, reduced latency, and enhanced overall reliability, making it particularly suitable for the demanding requirements of modern vehicular networks.

4.1 ARCHITECTURE DIAGRAM

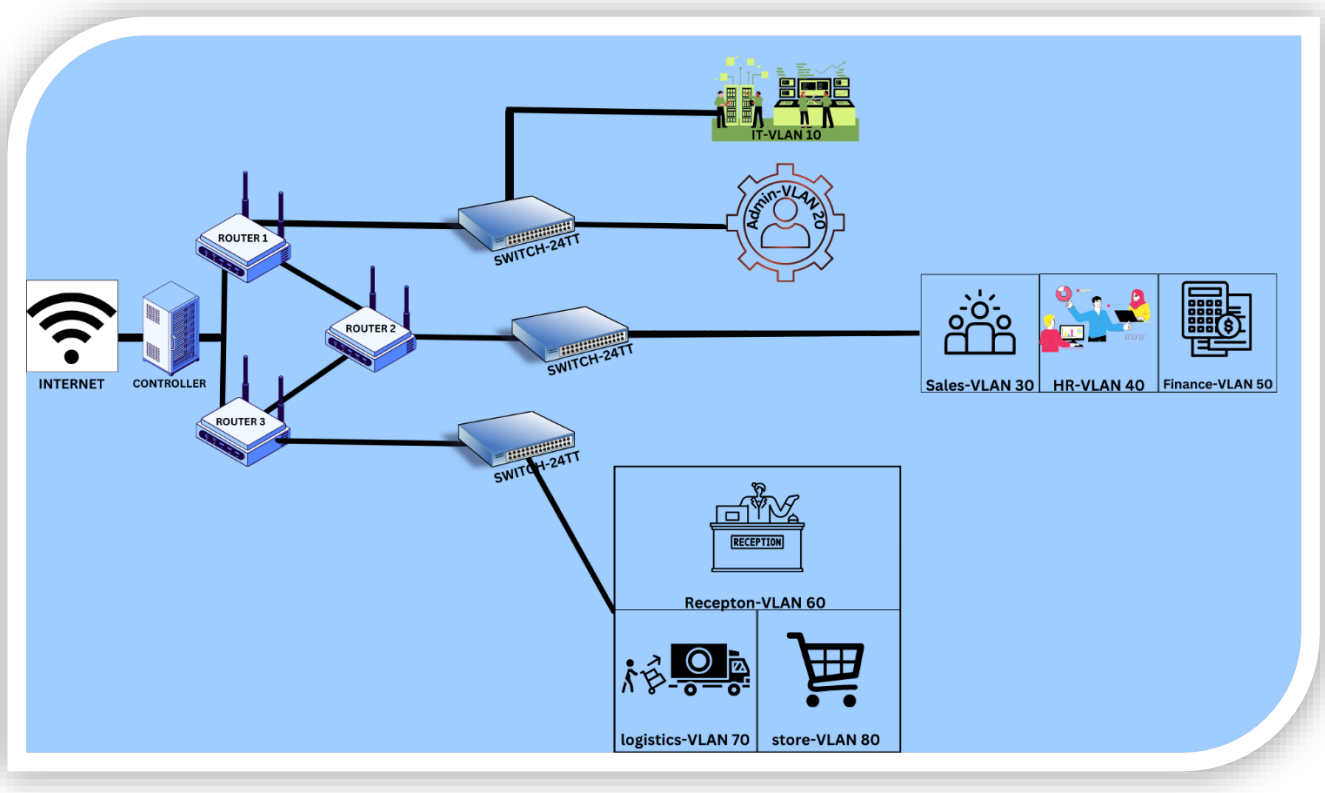

Figure 1

This diagram depicts a network topology with a Software Defined Networking (SDN) controller, routers, switches, and VLANs. Here's a breakdown:

Components:

- Internet: The gateway to the external world.
- SDN Controller: A centralized point that manages and controls the network, providing automation, programmability, and orchestration capabilities. It sits between the Internet and the routers.
- Routers (Router 1, Router 2, Router 3): Connect different network segments, manage traffic flow, and perform routing functions.
- Switches (SWITCH-24TT): Connect devices within a local network segment, forwarding traffic based on MAC addresses.
- VLANs: Virtual Local Area Networks, used to segment a physical network into smaller, logical networks for security, broadcast domain control, and improved performance.

VLAN Designations:

- IT-VLAN 10: A network segment for IT-related devices or users.
- Admin-VLAN 20: A network segment for administrative personnel or systems.
- Sales-VLAN 30: A network segment for the sales department.

- HR-VLAN 40: A network segment for the human resources department.
- Finance-VLAN 50: A network segment for the finance department.
- Reception-VLAN 60: A network segment for the reception area.
- Logistics-VLAN 70: A network segment for logistics operations.
- Store-VLAN 80: A network segment for the store or retail area.

How it Works:

1. Internet Connection: Devices on the network can access the internet through the SDN controller, which acts as a central point for managing traffic flow.
2. Router Connectivity: Each router connects to the SDN controller and to specific switches.
3. Switch Connections: Each switch is connected to different VLANs, allowing devices on those VLANs to communicate with each other but isolating them from other VLANs.
4. VLAN Segmentation: Devices within each VLAN are grouped logically based on their purpose. For example, devices in the "Sales-VLAN 30" can communicate within that VLAN, but they are isolated from devices in "HR-VLAN 40."
5. SDN Control: The SDN controller orchestrates traffic flow and policy enforcement across

This diagram depicts a network setup with various VLANs. The core network consists of three routers and three switches connected via ethernet cables. The internet connection is established through router 1. The network is segmented into several VLANs using switches, including IT-VLAN 10, Admin-VLAN 20, Sales-VLAN 30, HR-VLAN 40, Finance-VLAN 50, Reception-VLAN 60, logistics-VLAN 70, and store-VLAN 80. Each VLAN serves a specific purpose and is associated with different devices, for example, Reception-VLAN 60 connects to a reception desk while Finance-VLAN 50 connects to a computer with a calculator. This kind of network setup allows for better security, isolation, and control over different parts of the network.

At the core of the network are three routers and three switches interconnected via Ethernet cables, with Router 1 serving as the primary gateway to the Internet. The network is segmented into various VLANs, including IT-VLAN 10, Admin-VLAN 20, Sales-VLAN 30, HR-VLAN 40, Finance-VLAN 50, Reception-VLAN 60, Logistics-VLAN 70, and Store-VLAN 80, each tailored to specific departmental needs. This segmentation allows for improved security by isolating traffic, reducing broadcast domains, and optimizing overall network performance. The VLAN setup not only simplifies network management but also provides scalability for future growth, ensuring that the organization can adapt to changing requirements while maintaining a secure and efficient network environment.

Switch**es** are critical components in the network architecture, serving as the backbone for interconnecting devices within each VLAN. In this setup, three switches facilitate communication between various devices, such as computers, printers, and servers, ensuring efficient data transfer. Each switch operates at Layer 2 of the OSI model, using MAC addresses to forward data frames only to the intended recipients within the same VLAN, thereby minimizing unnecessary traffic and enhancing overall network performance. The switches also support VLAN tagging, which allows for the segmentation of network traffic, ensuring that devices within different VLANs remain isolated from one another. This capability not only improves security by limiting broadcast domains but also simplifies network management by allowing administrators to configure and monitor traffic flow more effectively. Overall, the switches play a vital role in maintaining a robust, efficient, and secure network infrastructure.

4.2 ALGORITHM

The Algorithms to focus on would be OSPF (Open Shortest Path First) for routing and DHCP (Dynamic Host Configuration Protocol) for IP address management.

OSPF (Open Shortest Path First)

OSPF is designed to efficiently manage the routing of packets in IP networks. It uses Dijkstra's algorithm to calculate the shortest path for data packets to travel across a network.

OSPF Works:

- **Link-State Advertisements (LSAs)**: Routers using OSPF periodically send out LSAs to inform other routers about the state of their links (interfaces). Each router builds a link-state database from these advertisements, reflecting the entire network topology.
- **Routing Decisions**: When a packet needs to be routed, OSPF uses the link-state database to determine the shortest path to the destination based on cost metrics (like bandwidth).
- **Areas**: OSPF supports hierarchical network design by dividing networks into areas. This helps optimize routing efficiency and reduces the overhead of LSAs.

Application in the Project:

- **Location**: OSPF is configured on each of the three routers connecting the different floors of the hotel.
- **Purpose**:
    - It enables inter-VLAN routing, allowing devices in different VLANs (e.g., Reception, Store, Finance) to communicate with each other effectively.
    - As the hotel network grows (e.g., adding more floors or departments), OSPF will dynamically adjust the routing paths without manual reconfiguration.

DHCP (Dynamic Host Configuration Protocol)

DHCP Works:

- **Lease Process**: When a device (DHCP client) connects to the network, it sends a DHCPDISCOVER message. The DHCP server responds with a DHCPOFFER message that contains an available IP address and lease duration.
- **Acknowledgment**: The client requests the offered address with a DHCPREQUEST message, and the server confirms with a DHCPACK message.
- **Lease Time**: DHCP leases the IP address for a specified duration, after which the client must renew the lease to continue using the address.

Application in the Project:

- **Location**: Each router in project acts as a DHCP server for its respective VLANs.
- **Purpose**: Automatically assigns IP addresses to devices (like laptops, phones, and printers) within their respective VLANs (e.g., Reception, Finance). Simplifies network management, allowing devices to join the network without manual IP configuration. This is particularly important in a dynamic environment like a hotel, where devices frequently connect and disconnect.

CHAPTER 5

IMPLEMENTATION:

1. Setting Up the SDN Controller

First, we will need to select and set up an SDN (Software-Defined Networking) controller. Ryu is an excellent choice for this project due to its user-friendly interface, extensive documentation, and active community support. To begin, you'll download and install Ryu on a server or a dedicated machine that will serve as your controller. The installation process involves setting up the necessary dependencies and ensuring that the environment is correctly configured to run Ryu applications. After installation, you will create a simple Ryu application that manages VLAN configurations and enables inter-switch communication. This application will be responsible for processing incoming traffic and making real-time decisions about how that traffic is handled across the network. The basic structure of the application includes event handlers for switch features, flow management, and mechanisms to dynamically update flow entries based on network conditions. Additionally, you may want to implement logging features to monitor the application's performance and track any anomalies in traffic patterns.

2. Establishing OpenFlow Switches

In this project, we will replace traditional Layer 3 switches with OpenFlow switches, which can be controlled programmatically via the SDN controller. OpenFlow allows for more granular control over network traffic, enabling dynamic adjustments to be made in real-time. To simulate this environment, we can use Mininet, a powerful network emulator that allows us to create a virtual network topology. You'll set up Mininet to mirror the hotel's physical structure, establishing a tree topology with OpenFlow-enabled switches corresponding to each floor of the hotel. This setup will allow for efficient traffic management and isolation between different departments. When configuring Mininet, you will specify that it should connect to the Ryu SDN controller, ensuring that all switches in your simulated network are under its control. This connection enables the controller to push flow rules to the switches, facilitating optimal traffic routing and management based on the defined policies.

3. Dynamic VLAN Management

With the SDN controller and OpenFlow switches in place, the next step is to implement dynamic VLAN management. This feature allows the network to adapt to changing conditions and user needs, providing a flexible and responsive infrastructure. In your Ryu application, you will add functionality to manage VLANs based on traffic patterns and user behavior. For example, if you notice an increase in traffic from a particular department, such as Sales or Finance, the application can dynamically create a new VLAN or adjust existing VLAN configurations to better distribute network resources. This can involve reallocating bandwidth, modifying traffic priorities, or even merging VLANs temporarily to handle peak loads. Such responsiveness improves the overall performance and reliability of the network, ensuring that critical applications remain accessible even during high-demand periods. Additionally, you can implement monitoring tools that provide real-time visibility into VLAN usage, allowing for proactive adjustments as needed.

4. Implementing Network Policies and Security

Next, we'll define network policies within the SDN framework to ensure that the network operates efficiently and securely. These policies might include rules for traffic prioritization, access control, and security measures tailored to the organization's specific needs. For instance, you can set up Quality of Service (QoS) rules to prioritize critical applications used by the Finance department while limiting bandwidth for less critical traffic, such as guest internet access. This prioritization ensures that essential services receive the necessary resources

to function optimally. You'll also configure security policies to restrict access to sensitive data, which is crucial for compliance and data protection

5.1 CODE:

VLAN and DHCP Configuration:

Router Configuration: Below are the commands to configure the routers and set up DHCP pools.

- **Router 1 (First Floor)**:

```
Router1> enable
Router1# configure terminal
Router1(config)# vlan 80
Router1(config-vlan)# name Reception
Router1(config-vlan)# exit
Router1(config)# vlan 70
Router1(config-vlan)# name Store
Router1(config-vlan)# exit
Router1(config)# vlan 60
Router1(config-vlan)# name Logistics
Router1(config-vlan)# exit

Router1(config)# ip dhcp pool Reception
Router1(dhcp-config)# network 192.168.8.0 255.255.255.0
Router1(dhcp-config)# default-router 192.168.8.1
Router1(dhcp-config)# exit

Router1(config)# ip dhcp pool Store
Router1(dhcp-config)# network 192.168.7.0 255.255.255.0
Router1(dhcp-config)# default-router 192.168.7.1
Router1(dhcp-config)# exit

Router1(config)# ip dhcp pool Logistics
Router1(dhcp-config)# network 192.168.6.0 255.255.255.0
Router1(dhcp-config)# default-router 192.168.6.1
```

Router1(dhcp-config)# exit

- **Router 2 (Second Floor)**:

Router2> enable

Router2# configure terminal

Router2(config)# vlan 50

Router2(config-vlan)# name Finance

Router2(config-vlan)# exit

Router2(config)# vlan 40

Router2(config-vlan)# name HR

Router2(config-vlan)# exit

Router2(config)# vlan 30

Router2(config-vlan)# name Sales

Router2(config-vlan)# exit

Router2(config)# ip dhcp pool Finance

Router2(dhcp-config)# network 192.168.5.0 255.255.255.0

Router2(dhcp-config)# default-router 192.168.5.1

Router2(dhcp-config)# exit

Router2(config)# ip dhcp pool HR

Router2(dhcp-config)# network 192.168.4.0 255.255.255.0

Router2(dhcp-config)# default-router 192.168.4.1

Router2(dhcp-config)# exit

Router2(config)# ip dhcp pool Sales

Router2(dhcp-config)# network 192.168.3.0 255.255.255.0

Router2(dhcp-config)# default-router 192.168.3.1

Router2(dhcp-config)# exit

- **Router 3 (Third Floor)**:

bash

Copy code

```
Router3> enable
Router3# configure terminal
Router3(config)# vlan 20
Router3(config-vlan)# name Admin
Router3(config-vlan)# exit
Router3(config)# vlan 10
Router3(config-vlan)# name IT
Router3(config-vlan)# exit

Router3(config)# ip dhcp pool Admin
Router3(dhcp-config)# network 192.168.2.0 255.255.255.0
Router3(dhcp-config)# default-router 192.168.2.1
Router3(dhcp-config)# exit
Router3(config)# ip dhcp pool IT
Router3(dhcp-config)# network 192.168.1.0 255.255.255.0
Router3(dhcp-config)# default-router 192.168.1.1
Router3(dhcp-config)# exit
```

Port Security Configuration on Switches

Switch 3 (IT Department):

```
Switch3> enable
Switch3# configure terminal
Switch3(config)# interface fa0/1
Switch3(config-if)# switchport mode access
Switch3(config-if)# switchport port-security
Switch3(config-if)# switchport port-security maximum 1
Switch3(config-if)# switchport port-security violation shutdown
Switch3(config-if)# switchport port-security mac-address sticky
```

5.2 OUTPUT:

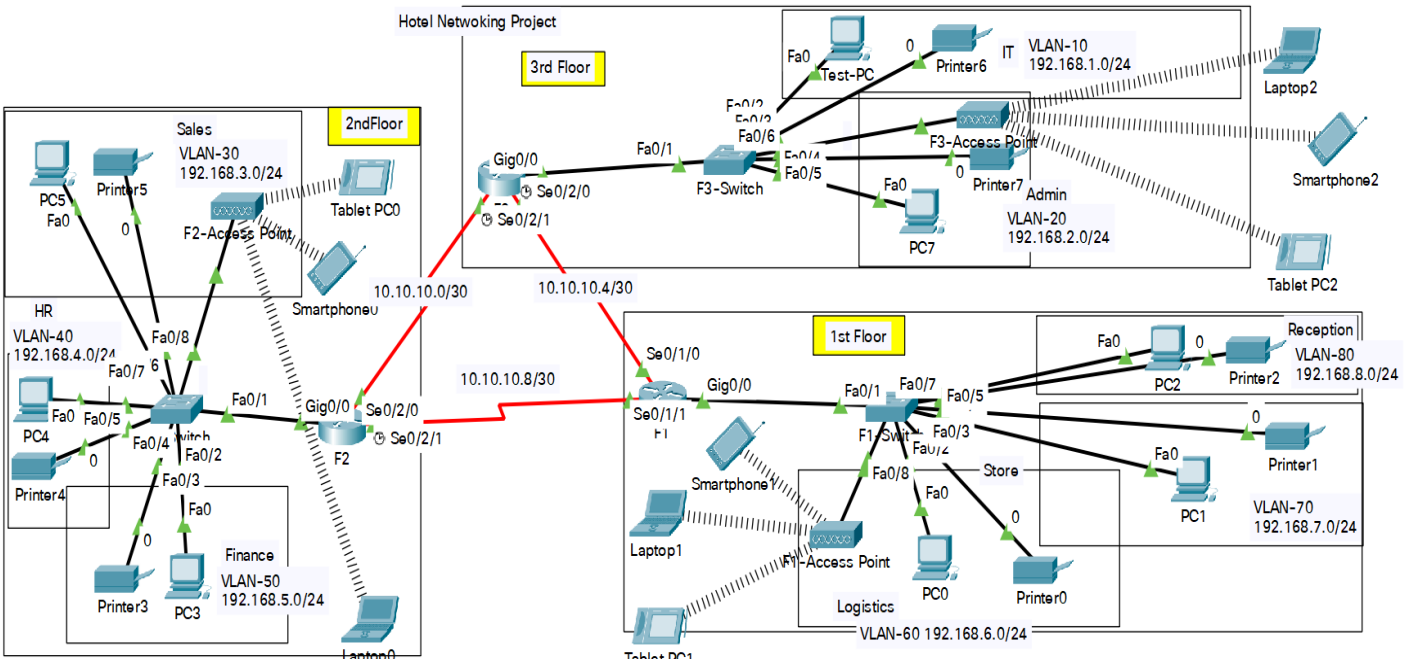

Figure 2

VLAN Segmentation

The network is segmented into distinct VLANs, each serving specific departments or functions within the organization. This segmentation enhances security by isolating traffic and reducing broadcast domains. The VLANs included in this setup are:

- **IT-VLAN 10**: Dedicated to the IT department, connecting servers, workstations, and network management devices.
- **Admin-VLAN 20**: Supports administrative functions, connecting office equipment, and administrative staff workstations.
- **Sales-VLAN 30**: Designed for the sales team, connecting sales representatives' devices and CRM systems.
- **HR-VLAN 40**: Allocated for the Human Resources department, connecting employee management systems and HR personnel.
- **Finance-VLAN 50**: Dedicated to the finance team, connecting computers with accounting software and financial tools, including calculators.
- **Reception-VLAN 60**: Connects devices at the reception desk, including telephones and visitor management systems.
- **Logistics-VLAN 70**: Supports logistics operations, connecting devices related to inventory management and shipping.
- **Store-VLAN 80**: Designed for retail operations, connecting point-of-sale systems and inventory devices.

CHAPTER 6

6.1 CONCLUSION

Software-Defined Networking (SDN) into the hotel network project demonstrates a significant advancement in network management by enhancing flexibility, security, and efficiency. By leveraging an SDN controller like Ryu, the project allows for dynamic management of VLANs, streamlined configuration, and improved traffic flow across the hotel's various departments. The use of virtualized environments with tools such as Mininet not only facilitates testing and validation of the network design but also provides a platform for real-time monitoring of network performance. Looking to the future, further enhancements could include the implementation of advanced security protocols to safeguard sensitive data, the exploration of machine learning algorithms to optimize network performance and predict traffic patterns, and the integration of IoT devices for improved guest experiences. Additionally, expanding the project to incorporate multi-site management capabilities could pave the way for a more interconnected and intelligent hotel network infrastructure, further elevating operational efficiencies and guest satisfaction.

the implementation of a Software-Defined Networking (SDN) architecture using Ryu as the controller and OpenFlow switches represents a transformative approach to managing modern network infrastructures. This project highlights the critical advantages of SDN, including enhanced flexibility, scalability, and improved resource management. By replacing traditional Layer 3 switches with OpenFlow switches, we have enabled a level of programmability that allows for real-time traffic management and dynamic VLAN configurations tailored to the specific needs of various departments within the organization.

The establishment of a virtual network topology using Mininet not only simulates the physical layout of the hotel but also provides a controlled environment for testing and validating network policies and configurations. The ability to dynamically manage VLANs based on traffic patterns ensures that the network can adapt to changing demands, optimizing performance and reliability. This responsiveness is particularly vital in environments where user behavior can fluctuate significantly, such as in a hotel setting where different departments may experience varying levels of traffic at different times.

Moreover, the implementation of robust network policies and security measures further enhances the overall integrity of the network. By prioritizing critical applications through Quality of Service (QoS) rules and establishing access control lists (ACLs), we can safeguard sensitive data while ensuring that essential services remain operational during peak usage periods. The integration of security features, such as intrusion detection systems, serves to proactively monitor for potential threats, thereby reinforcing the organization's commitment to maintaining a secure and resilient network environment.

As organizations continue to evolve and embrace digital transformation, the adoption of SDN technologies like Ryu and OpenFlow will be instrumental in meeting the challenges of modern networking. The insights gained from this project underscore the importance of flexibility, security, and efficient resource management in creating a network infrastructure that not only supports current operational needs but is also prepared for future growth and innovation. By leveraging the capabilities of SDN, organizations can foster an agile and responsive network that enhances user experiences, drives productivity, and ultimately contributes to achieving strategic business objectives.

6.2 FUTURE WORK

Dynamic VLAN Management: Implement dynamic VLAN assignment based on user roles or device types. This can enhance security and simplify management by automatically placing devices in the appropriate VLAN. **Integration of AI for Traffic Analysis**: Utilize artificial intelligence to analyze network traffic patterns and optimize routing decisions in real-time, improving overall network performance and efficiency. **Enhanced Security Protocols**: Develop and implement advanced security measures, such as machine learning-based intrusion detection systems, to proactively identify and mitigate potential threats within the network. **Multi-Cloud Networking Solutions**: Explore solutions for seamless integration and management of multi-cloud environments, ensuring consistent policies and performance across different cloud providers. **Network Function Virtualization (NFV)**: Investigate the use of NFV to virtualize network functions, allowing for more flexible and scalable network architectures that can adapt to changing demands. **User Experience Monitoring**: Implement tools to monitor user experience across the network, providing insights into application performance and user satisfaction, which can guide future improvements. **Interoperability Testing**: Conduct extensive testing of interoperability between different SDN controllers and network devices to ensure compatibility and performance across diverse environments. **Green Networking Initiatives**: Research and develop strategies for reducing the energy consumption of network devices and infrastructure, contributing to sustainability goals. **Edge Computing Integration**: Explore the integration of edge computing solutions to process data closer to the source, reducing latency and improving response times for critical applications. **Training and Certification Programs**: Establish training programs for network administrators and engineers to enhance their skills in SDN, VLAN management, and emerging networking technologies, ensuring the workforce is prepared for future challenges. **Automated Network Recovery**: Develop automated systems for network recovery and failover to ensure high availability and resilience. This could involve implementing self-healing mechanisms that detect failures and automatically reroute traffic **Advanced Analytics and Reporting**: Implement advanced analytics tools that provide deeper insights into network performance, user behavior, and resource utilization. This could include predictive analytics to forecast future network trends and demands. **Integration with IoT Devices**: Explore the integration of IoT (Internet of Things) devices into the SDN architecture, focusing on managing the unique challenges posed by IoT traffic patterns, security, and scalability. **User -Centric Network Design**: Investigate user-centric network design approaches that prioritize end-user experience and application performance. This could involve gathering user feedback and using it to inform network configurations and policies.