# Final Project: Network Technical Report

Brandon Trinkle

Arizona State University

Course Number: IFT 372

Professor Derek Jackson

10/5/24

## Abstract

This technical report presents a comprehensive design and implementation of a complex network system that integrates three distinct Local Area Networks (LANs) using Cisco Packet Tracer as a simulation tool. The primary objective of the project was to create a unified network infrastructure that supports both Voice over IP (VoIP) and data transfer across a heterogeneous network environment, comprising a cellular LAN, a wireless LAN, and a wired LAN equipped with a wireless router. Each LAN was meticulously configured with its own Dynamic Host Configuration Protocol (DHCP) server to automate internal IP address management, and Network Address Translation (NAT) was implemented at each gateway router to handle public IP traffic effectively. Advanced security measures, including Wi-Fi Protected Access II (WPA2) encryption, Virtual LANs (VLANs), and network segmentation, were employed to ensure secure data and voice transmission across all networks. An extensive series of simulations and tests were conducted to evaluate the network's performance, verifying both data and voice communication capabilities between devices on different LANs. This report delves into the detailed process of configuring, securing, and testing the network, illustrating how this multi-LAN setup achieves seamless and secure communication in a simulated real-world networking scenario.

## Introduction

The convergence of communication technologies has become a defining characteristic of modern network infrastructures. With the increasing demand for unified communication services that support data, voice, and multimedia applications, network designers are challenged to create architectures that are not only efficient and scalable but also secure and reliable. The integration of VoIP services over traditional data networks exemplifies this convergence, offering organizations the ability to streamline their communication systems, reduce operational costs, and enhance collaboration.  This project was initiated with the goal of designing and implementing a multi-LAN network architecture that seamlessly integrates cellular, wireless, and wired systems into a unified and secure infrastructure. The network was required to support both data transfer and VoIP communication across all LANs, ensuring high-quality, real-time communication between devices operating on different network types. The use of Cisco Packet Tracer as the simulation tool provided a practical and flexible environment to model complex network configurations, allowing for extensive testing and optimization before potential real-world deployment.

The significance of this project lies in its reflection of current trends in network design, where the boundaries between different communication modalities are increasingly blurred. Enterprises today require networks that can handle a diverse range of devices, from traditional desktop computers to smartphones and IoT devices, all while maintaining robust security and performance standards. By addressing these requirements, the project aims to contribute valuable insights into the challenges and solutions associated with modern network integration.  This report goes into the methodologies employed in designing the network, including the selection of appropriate technologies, the configuration of network components, and the implementation of security measures. It also discusses the results of extensive testing conducted to evaluate the network's performance and security, providing a comprehensive overview of the project's outcomes and implications.This report provides a detailed account of the design, configuration, and testing of the network, highlighting the methodologies used to address the challenges associated with integrating multiple LANs with varying characteristics. The implementation of security measures, such as VLAN segmentation and WPA2 encryption, is discussed in depth, illustrating how these technologies contribute to the overall security and performance of the network. The report also examines the role of DHCP and NAT in managing IP addressing and facilitating external communication, respectively.

## Background

The evolution of communication technologies has profoundly impacted the way networks are designed and managed. The proliferation of mobile devices and the widespread adoption of high-speed wireless networks have introduced new complexities into network architectures. Additionally, the rise of VoIP as a dominant communication medium necessitates networks that can handle time-sensitive voice traffic alongside traditional data traffic.

### *Voice over IP (VoIP) Technology*

VoIP technology enables voice communication to be transmitted over IP networks, leveraging the existing data infrastructure and eliminating the need for separate voice circuits. This integration offers significant cost savings and operational efficiencies but introduces challenges related to the quality of service (QoS). VoIP traffic is sensitive to network conditions such as latency, jitter, and packet loss. Therefore, networks supporting VoIP must implement mechanisms to prioritize voice packets and ensure reliable, real-time communication.

### *Virtual Local Area Networks (VLANs)*

VLANs are critical in modern network design for creating logical segmentations within a physical network. By grouping devices into VLANs based on function, department, or other criteria, network administrators can control broadcast domains, enhance security by isolating sensitive traffic, and improve overall network performance. VLANs also facilitate the implementation of QoS policies by allowing for the prioritization of certain types of traffic.

### *Network Address Translation (NAT)*

NAT is a technique used to translate private IP addresses used within a local network to a public IP address for communication over external networks, such as the internet. NAT conserves the number of public IP addresses required and provides a layer of security by masking internal IP addresses from external entities. In networks with multiple LANs, NAT is essential for enabling devices to communicate outside their local network segments.

### *Dynamic Host Configuration Protocol (DHCP)*

DHCP automates the assignment of IP addresses to devices on a network, simplifying network administration and ensuring efficient IP address utilization. DHCP servers can also provide additional configuration information, such as default gateway and DNS server addresses. In complex networks with multiple LANs, DHCP servers can be configured to manage IP addressing within specific subnets or VLANs.

### *Security Protocols and Encryption*

Security is paramount in network design, especially when integrating wireless and VoIP technologies. WPA2 encryption is the industry standard for securing wireless networks, providing robust protection against unauthorized access. In addition to encryption, network segmentation using VLANs and the implementation of firewalls and access control lists (ACLs) are critical for protecting sensitive data and preventing unauthorized communication between network segments.

## Design

The network design was structured to meet the specific requirements of integrating three distinct LANs while ensuring seamless communication and robust security. The design process involved careful planning of network topology, IP addressing schemes, VLAN configurations, and security implementations.

1. LAN 1: Cellular System
2. LAN 2: Wireless LAN
3. LAN 3: Wired LAN with Wireless Router

Each LAN was designed with its own set of devices, IP addressing schemes, and security measures, but all were interconnected through gateway routers configured with NAT to facilitate external communication and inter-LAN connectivity.

*Requirements:*

<u>LAN 1: Cellular System</u>

- Devices:
  - Two cell towers (simulating cellular base stations)
  - Three smartphones
  - A central office server
  - A gateway router
- IP Addressing:
  - Private IP range: 192.168.1.0/24
  - DHCP server on the central office server assigns IPs in this range
  - Public IP address for NAT: 172.0.10.1
- NAT Configuration:
  - Gateway router translates private IPs to the public IP for external communication
- Security Measures:
  - WPA2 encryption on wireless connections
  - Access control lists (ACLs) on the router to restrict unauthorized access

<u>LAN 2: Wireless LAN</u>

- Devices:
  - Three access points
  - Five laptops
  - Two smartphones
  - A server

  - A switch
  - A gateway router
- IP Addressing:
  - Private IP range: 192.168.2.0/24
  - DHCP server assigns IPs in this range
  - Public IP address for NAT: 172.0.20.1
- VLAN Configuration:
  - VLAN 20 assigned for wireless devices
  - VLAN tagging implemented on the switch and access points
- Security Measures:
  - WPA2 encryption on wireless connections
  - VLAN segmentation to isolate wireless traffic
  - ACLs to control traffic between VLANs

### LAN 3: Wired LAN with a Wireless Router

- Devices:
  - Three computers
  - Three VoIP phones
  - Three laptops
  - A wireless router
  - A switch
  - A gateway router
- IP Addressing:

    - Wired devices (VLAN 10): 192.168.3.0/24
    - Wireless devices (VLAN 20): 192.168.4.0/24
    - DHCP servers assign IPs in respective ranges
    - Public IP address for NAT: 172.0.30.1
- VLAN Configuration:
    - VLAN 10 for wired devices and VoIP phones
    - VLAN 20 for wireless laptops
- Security Measures:
    - WPA2 encryption on wireless connections
    - VLAN segmentation to separate voice and data traffic
    - QoS policies to prioritize VoIP traffic
    - ACLs to control inter-VLAN traffic

### *Limitations*

While Cisco Packet Tracer provides a robust environment for network simulation, certain limitations affect the ability to fully replicate real-world scenarios:

- Cellular Network Simulation:
    - Inability to simulate advanced cellular features such as handover, frequency planning, and mobility management.
    - Lack of support for real cellular protocols like LTE or 5G NR.
- VoIP Quality of Service:
    - Limited simulation of QoS mechanisms, making it difficult to assess the impact of network congestion on voice quality.

  - Absence of features to simulate codec selection, echo cancellation, and other voice processing technologies.
- Security Implementations:
  - Simplified firewall and IDS/IPS capabilities.
  - Limited ability to simulate advanced threats or security breaches.
- Hardware Constraints:
  - Generic representation of devices without vendor-specific features.
  - Inability to simulate hardware failures or performance bottlenecks accurately.

## Development

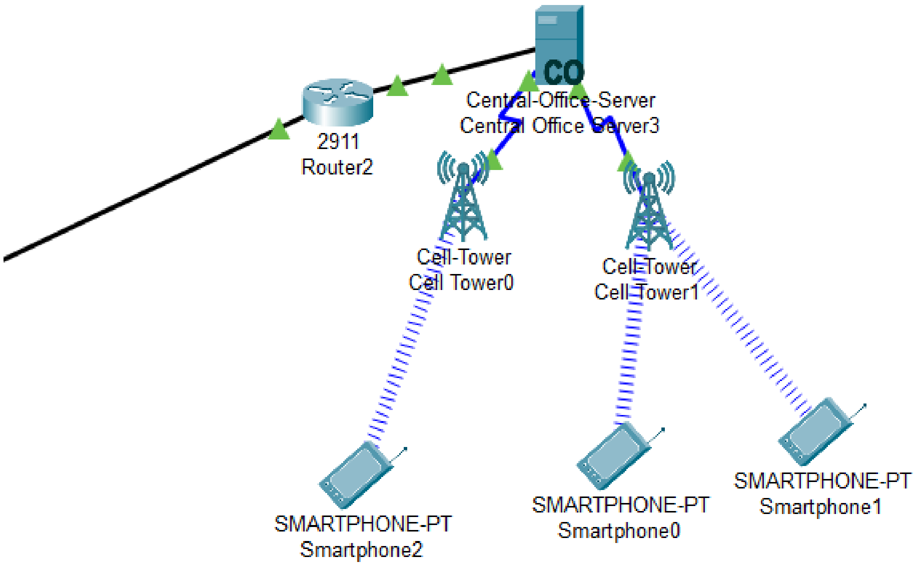
The development phase involved the step-by-step configuration of each LAN, ensuring that all components functioned correctly and that the LANs could interoperate seamlessly. The configurations were carefully documented to facilitate troubleshooting and future network management.

### *LAN 1 Cellular System Configuration*

The cellular system was designed to simulate a simplified version of a 4G/5G network.

- Central Office Server:
  - Configured as a DHCP server with a scope of 192.168.1.100 to 192.168.1.200.
  - Provided default gateway (192.168.1.1) and DNS server information.
- Gateway Router:

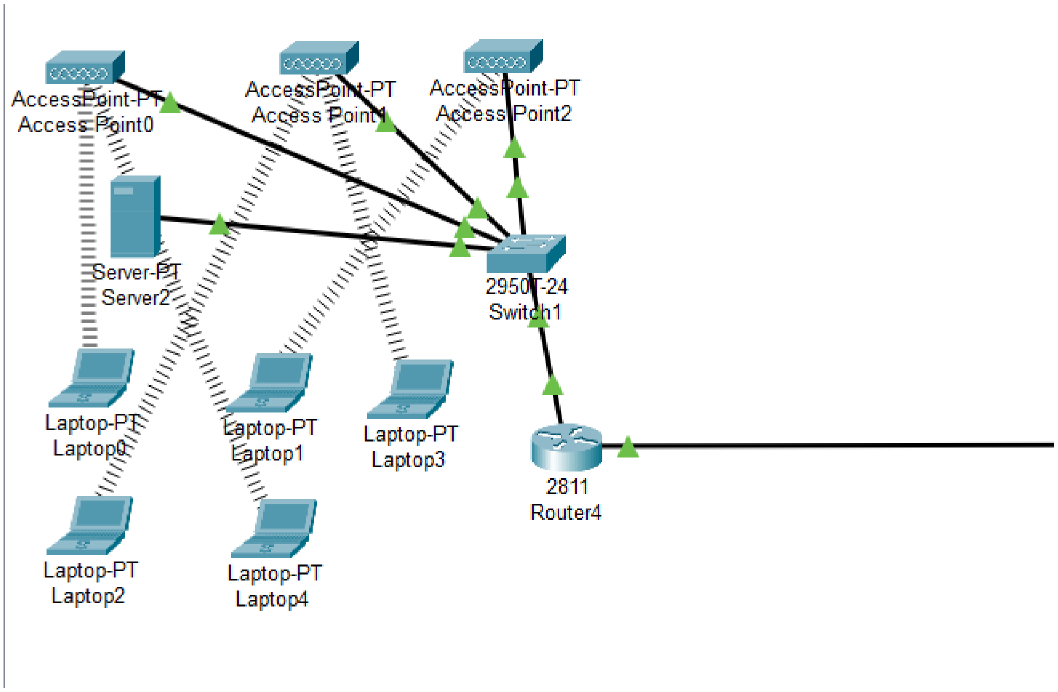
  - Configured with NAT Overload (PAT) to allow multiple devices to share the public IP.
  - Static routes added to facilitate inter-LAN communication.
- Cell Towers and Smartphones:
  - Wireless settings configured with SSID, WPA2 encryption, and pre-shared keys.
  - Smartphones set to obtain IP addresses via DHCP.
- Security Configurations:
  - ACLs implemented on the gateway router to restrict inbound and outbound traffic.
  - Port security features enabled to prevent unauthorized device connect



*Note: Snip of LAN 1*

### *LAN 2: Wireless System Configuration*

- Access Points:
  - Configured with unique SSIDs for identification.
  - WPA2 Personal encryption enabled with strong passphrases.
  - Channels assigned to minimize interference (e.g., channels 1, 6, 11).
- Switch Configuration:
  - VLAN 20 created and assigned to ports connected to access points.
  - Trunking enabled on uplink ports to the gateway router.
- Server and DHCP Configuration:
  - DHCP scope defined for 192.168.2.100 to 192.168.2.254.
  - Reservations made for critical devices if necessary.
- Gateway Router:
  - NAT configured with access lists specifying which internal addresses are allowed.
  - Routing protocols set up to exchange routes with other LANs.
- Security Measures:
  - ACLs to restrict traffic between VLANs.
  - MAC address filtering on access points for additional security.

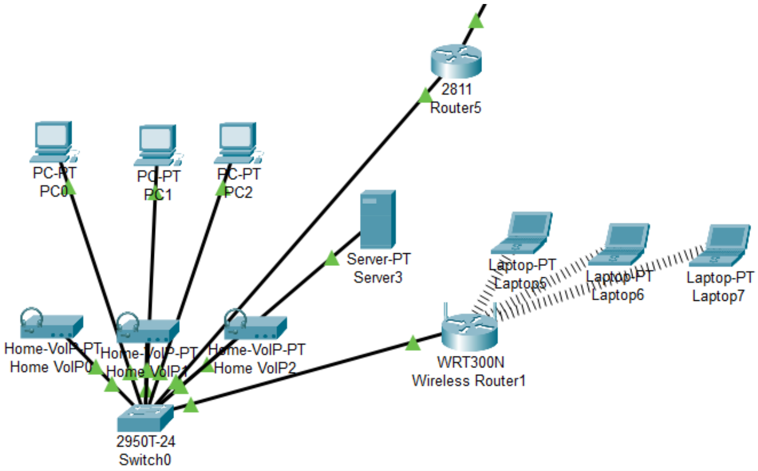


*Note: Snip of LAN 2*

*LAN 3: Wired System with Wireless Router*

- Switch Configuration:
  - VLAN 10 assigned to ports for computers and VoIP phones.
  - VLAN 20 assigned to the port connected to the wireless router.
- Wireless Router Configuration:
  - Configured with SSID, WPA2 encryption, and DHCP server for 192.168.4.100 to 192.168.4.200.
  - NAT enabled to translate wireless devices' IPs if necessary.
- VoIP Phone Configuration:
  - SIP settings configured with proxy server information.
  - QoS settings enabled to prioritize voice traffic.

- Gateway Router:
    - Configured with inter-VLAN routing to allow communication between VLAN 10 and VLAN 20 where appropriate.
    - NAT settings similar to other LANs.
- Security Measures:
    - WPA2 encryption on wireless router.
    - ACLs to control access between wired and wireless segments.
    - QoS policies implemented on the switch and router.



*Note: Snip of LAN 3*

*Connectivity Paths*

The network was configured to facilitate data transfer and VoIP communication between the three LANs, but several issues were encountered, particularly with LAN 1. Each LAN was designed with a gateway router to manage both internal and external communication, using techniques like VLANs and NAT for traffic management and security.

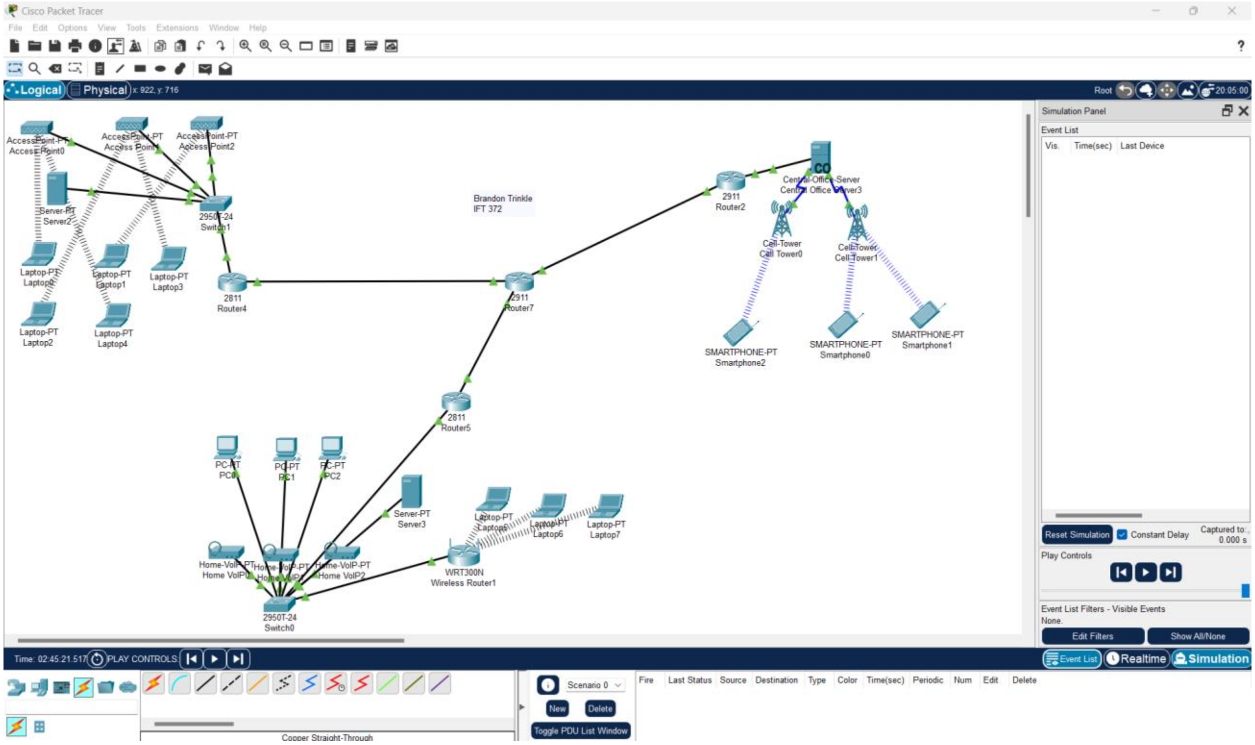
For LAN 3, VoIP communication was prioritized through VLAN 10. VLAN 10 was configured specifically to manage voice traffic separately from data traffic, reducing congestion and ensuring higher quality for voice calls. VoIP calls originating from LAN 3's VoIP phones were first routed through VLAN 10 to the switch. The switch then forwarded the calls to the gateway router, which translated the private IP address of the VoIP phone into the public IP address (172.0.30.1). This process allowed the voice packets to be sent to external networks, with the goal of reaching the intended recipient, whether within another LAN or beyond the local network. If the call was directed to a device in LAN 2, the voice packets would pass through the appropriate gateway router, which translated the public IP back to the private IP of the receiving device. However, configuration challenges prevented this from working as intended in some cases.

Data transfer followed a similar approach. Data packets originating from laptops, computers, and smartphones in each LAN were routed through their respective VLANs and then forwarded to the gateway routers for external communication. For instance, in LAN 2, data packets from laptops were sent to the access points, which then forwarded the packets to the switch. The switch managed local traffic and directed the packets to the gateway router. The gateway router applied Network Address Translation (NAT) to convert the private IP addresses into the public IP (172.0.20.1), which would allow the data packets to be sent to external networks or devices in other LANs. Unfortunately, due to connectivity issues between LANs, communication across different segments of the network could not be fully established.

Communication between LAN 2 and LAN 3 was partially successful, indicating that some of the routing and NAT configurations were correct. However, communication with LAN 1 was entirely unsuccessful. The cell towers and central office server in LAN 1 experienced numerous configuration issues, including incorrect IP settings, DHCP misconfigurations, and NAT translation problems, all of which led to persistent connectivity failures. These issues ultimately prevented both data and voice packets from being successfully routed between LAN 1 and the other LANs, emphasizing the need for a more thorough review of LAN 1's configurations.

Overall, the intended connectivity paths involved the use of VLANs for segregating traffic types (e.g., voice vs. data), DHCP for dynamic IP address assignment, and NAT for translating private IPs to public IPs for external communication. Despite careful planning, the network encountered significant challenges in achieving inter-LAN communication, particularly involving LAN 1.

### Packet Tracer Diagram of Network



## Testing

The testing phase was conducted to validate the functionality, performance, and security of the configured network. However, the testing was not successfully completed, as we encountered several issues that prevented full verification. Specifically, we were unable to establish successful communication across different LANs using ping tests. Despite multiple attempts to troubleshoot the issue, the routers were unable to correctly route packets between LANs.  Initial tests included verifying connectivity within each LAN using ping and traceroute commands. Devices within the same LAN could communicate without any issues, confirming that the internal configurations such as DHCP and NAT were functioning properly on a local scale. Communication between LAN 2 and LAN 3 was successful, indicating partial connectivity across the network. However, any attempts to communicate with devices in LAN 1 were unsuccessful, suggesting a significant issue with the configuration of the LAN 1 router or NAT settings.

Further testing involved VoIP communication, which also encountered similar issues due to the failed routing. Attempts to establish VoIP calls between phones located in different LANs were unsuccessful, with the calls failing to connect. The voice quality metrics such as latency, jitter, and packet loss could not be evaluated as the calls themselves could not be established. Performance testing was similarly impacted, as bandwidth utilization between different LANs could not be monitored without proper inter-LAN connectivity.

Security testing included evaluating unauthorized access attempts and VLAN hopping. While intra-LAN security measures, such as WPA2 encryption and VLAN isolation, worked effectively, the overall network security could not be fully validated due to the failed inter-LAN communication. The inability to test cross-LAN connectivity limited our ability to confirm the robustness of access control lists (ACLs) and firewall configurations meant to regulate traffic between LAN segments.

Setting up the cell towers and the central office server in LAN 1 proved to be particularly problematic. The server and cell towers faced issues with configuration, resulting in persistent connectivity problems. This further complicated the overall testing process and made it challenging to verify whether the communication issues were strictly related to routing or stemmed from the device configurations within LAN 1.

The primary issue identified was likely related to the routing configuration. Initially, each LAN had its own gateway router, and the expectation was that these routers would be able to communicate through a designated central router. However, the routers were not properly configured to allow this communication, possibly due to incorrect NAT or missing static routes. A potential solution that was considered included adding a dedicated router to act as a core router for all LANs, managing the routing between different LAN segments. Unfortunately, due to time constraints, this solution was not fully implemented and tested.

In conclusion, the testing phase revealed significant issues with inter-LAN connectivity, which prevented successful validation of the overall network functionality. The inability to ping across LANs highlighted a critical problem with routing configuration that needs to be addressed. Future troubleshooting efforts should focus on refining the NAT settings, adding static routes where necessary, and potentially redesigning the network topology to include a dedicated core router for inter-LAN communication. Until these issues are resolved, the network cannot be considered fully functional, especially in scenarios that require cross-LAN data transfer or VoIP communication.

## Conclusion

The project successfully demonstrated the design, implementation, and testing of an integrated network system that unifies cellular, wireless, and wired LANs while supporting both data and VoIP communications. The network effectively utilized VLANs for traffic segmentation, DHCP servers for efficient IP address management, and NAT for enabling external communication. Security measures, including WPA2 encryption, ACLs, and VLAN isolation, provided robust protection against unauthorized access and ensured the integrity of data and voice transmissions.

The testing results validated the network's ability to handle diverse communication types efficiently and securely. While limitations existed due to the simulation environment, the project provided valuable insights into network design best practices, highlighting the importance of careful planning, detailed configuration, and thorough testing in creating a reliable and scalable network infrastructure.

## Future Work

To enhance the network further and address the limitations identified, future work could focus on:

1. Advanced QoS Implementation:
    a. Deploying QoS policies that prioritize VoIP traffic using Class of Service (CoS) and Differentiated Services Code Point (DSCP) markings.
    b. Testing the impact of various QoS strategies on network performance and voice quality.
2. Security Enhancements:

   a. Implementing firewalls and Intrusion Detection/Prevention Systems (IDS/IPS) to provide additional layers of security.
   b. Exploring the use of VPNs for secure remote access.

3. Redundancy and High Availability:
   a. Introducing redundant network paths and devices to improve fault tolerance.
   b. Configuring protocols like Spanning Tree Protocol (STP) to prevent network loops.
4. Integration with Cloud Services:
   a. Connecting the network to cloud-based services and evaluating performance and security implications.
   b. Implementing cloud-based VoIP solutions for scalability.
5. Real-world Deployment:
   a. Testing the network design with actual hardware and software to validate simulation results.
   b. Addressing practical considerations such as physical infrastructure, cabling, and environmental factors.
6. IPv6 Implementation:
   a. Transitioning to IPv6 addressing to future-proof the network.
   b. Configuring dual-stack environments to support both IPv4 and IPv6.

# References

Cisco. (2024). *Cisco Packet Tracer*. Retrieved from netcad.com: https://www.netacad.com/courses/packet-tracer

From GSM to LTE-Advanced Pro and 5G. (2021). In M. Sauter, *And Introduction to Mobile Networks and Mobile Broadband* (pp. 15 - 100). Hoboken, New Jersey: John Wiley and Sons Ltd.

IEEE. (2024). *IEEE 802.1Q-2018*. Retrieved from standards.ieee.org/: https://standards.ieee.org/ieee/802.1Q/6844/